Andre lands arbeid med digitale sårbarheter

Innholdsfortegnelse

1. Innledning

1.1. Oppdrag

Digitalt sårbarhetsutvalg (Lysneutvalget) har, på vegne av Regjeringen, blant annet som oppgave å beskrive hvordan relevante allierte, og andre sammenlignbare land, arbeider med å redusere sin digitale sårbarhet. Utvalget skal ha særlig vekt på virkemidler som har overføringsverdi til norske forhold. Utvalget ønsker at deler av arbeidet utføres av en ekstern konsulent. Oppdraget består i at BDO skal bistå utvalget med å utarbeide en slik rapport. Rapporten skal skrives som en prosatekst egnet til å gjengi i en norsk offentlig utredning (NOU). Informasjonen skal sorteres etter land.

Følgende forhold skal beskrives:

- Hvordan jobber landet med å forebygge digitale sårbarheter på nasjonalt nivå?
- Hvis landet har en informasjonssikkerhetsstrategi/IKT-sikkerhetsstrategi/cyberstrategi, hva er hovedtrekkene i denne?
- Hvordan er IKT-hendelseshåndering organisert?
- Hvordan fører myndighetene tilsyn med og regulerer IKT-sikkerhet?
- Hvordan sikrer landet at det har tilstrekkelig kompetanse, forskning og utdanning på IKT-sikkerhetsområdet?
- Hvordan jobber myndighetene med å sikre innbyggernes personvern i det digitale rom?

Spørsmålene skal besvares for følgende land:

- USA
- Canada
- Tyskland
- Storbritannia
- Nederland
- Sverige
- Finland
- Estland

Utvalget av land er begrunnet i:

- at disse har tilnærmet samme verdigrunnlag som Norge, og
- at deres reguleringer og arbeid med informasjonssikkerhet skjer i et verdiperspektiv der menneskerettighetene, herunder personvern, demokrati og rettsstatsprinsipper danner rammene for politikkutforming på området.

I den utstrekning Lysneutvalget ønsker det, skal BDO også delta i andre aktiviteter som inngår i prosjektet.

1.2. Gjennomføringen av oppdraget

Oppdraget er utført av BDOs rådgivingsavdeling. Arbeidet er således å anse som et rådgivningsoppdrag. Rapporten bygger på den informasjon vi har innhentet gjennom åpne

kilder, og vurderingene er begrenset til denne informasjonen. BDO vil presisere at vi ikke kan påta oss ansvar for fullstendigheten eller riktigheten i det grunnlagsmaterialet som har vært utgangspunkt for vurderingene.

BDO har forsøkt å verifisere omtalene av andre lands arbeid med digitale sårbarheter gjennom kontakt med de respektive landenes ansvarlige myndigheter. Det har i varierende grad kommet tilbakemeldinger på disse landomtalene. Det er mottatt tilbakemeldinger med tekstlige innspill fra USA, UK, Tyskland og Nederland. I tillegg er kapittelet om Sveriges arbeid på område i sin helhet utarbeidet av svenske myndigheter.

I de tilfeller der landinformasjonen ikke er blitt verifisert av offisielle kontaktpunkter i de respektive landene, tas det forbehold om at det kan forekomme faktiske feil og mangler. Det tas også forbehold om at det kan forekomme faglige uenigheter mellom offisielle kontaktpunkter i de utvalgte landene, hvilket kan medføre at redegjørelsene har faktiske feil og mangler også i de tilfeller der omtalen er blitt verifisert av Justis- og beredskapsdepartementets (JD) offisielle kontaktpunkter. Dersom vi har mottatt uriktige eller ufullstendige opplysninger, har BDO ikke hatt anledning til å avdekke dette ut over overordnede rimelighetsvurderinger.

Arbeidet er gjennomført innenfor en begrenset tidsramme og tidsperiode, og omfanget og fullstendigheten av våre analyser og beskrivelser av andre lands arbeid med digitale sårbarheter må ses i lys av dette. BDO kan ikke gå god for at alle relevante forhold er avdekket eller analysert.

BDO er ikke ansvarlig for ev. feil eller mangler i denne rapporten. BDO er heller ikke ansvarlig for de resultater som følger av bruken av denne rapporten. BDOs vurderinger er basert på våre konsulenters beste faglige skjønn.

Oslo, 09.09.2015

BDO AS

Karl-Ludvig Mauland
Partner

Dagfinn Buset
Prosjektleder

2. Presiseringer og avgrensninger av oppdraget

Det er gjennomført et oppstartsmøte og tre prosjektmøter mellom Lysneutvalget og BDO. I disse er det gjort følgende presiseringer og avgrensninger i forhold til oppdraget:

- BDO skal utarbeide følgende:
    - Et sammendrag som kan innarbeides i utvalgets utredning, og som trekker ut essensen og drøfter hvordan andre land arbeider med digitale sårbarheter opp mot de problemstillinger som utvalget har ønsket besvart.
    - Et vedlegg med mer utfyllende landomtaler. Hva gjelder vektingen av de ulike spørsmålene som ønskes besvart, vil dette måtte variere fra land til land. Vedlegget skrives på engelsk for å sikre nødvendig verifikasjon fra de respektive landenes myndigheter.

- BDO skal ta utgangspunkt i de aktuelle landenes eksisterende nasjonale strategier, samt annen åpent tilgjengelig relevant informasjon.

- Spørsmålene skal drøftes i et overordnet perspektiv og dermed belyse større trender i landenes arbeid med digitale sårbarheter. BDO skal trekker frem de gode eksemplene og vektlegge omtale av det som synes å ha størst overføringsverdi til norske forhold.

- Landomtalene utarbeides ved å sette sammen offentlig tilgjengelig informasjon. Da dette kan medføre at nyanser og viktige elementer av landenes arbeid med å reduseres digitale sårbarheter ikke omtales, har Lysneutvalget formidlet utkast til landomtalene til de respektive myndigheter i de utvalgte landene. Omtalen er formidlet via JDs kontaktpunkter. Landomtalene skrives på engelsk, med unntak av omtalen av Sverige som skrives på svensk.

- BDO kan legge mindre vekt på personvernproblemstillingen, da utvalgssekretariatet og utvalget har kompetanse til å ivareta dette selv.

- Omtalene av Nederland, Storbritannia, Tyskland og USA prioriteres.

3. Andre lands arbeid med digitale sårbarheter

3.1. Innledning

Utfordringene ved samfunnets stadig større grad av digitalisering er grenseoverskridende og mange. Nasjonale myndigheter i de fleste land det er naturlig å sammenligne Norge med, anerkjenner at den digitale utviklingen medfører nærmest grenseløse positive muligheter, så vel som en rekke sikkerhetsutfordringer som må håndteres.

Det har i tråd med utvalgets mandat vært naturlig å se til hvordan land som er sammenlignbare med Norge, arbeider på nasjonalt nivå for å møte disse utfordringene. Det er derfor gjort en gjennomgang av diverse offentlige dokumenter og nasjonale strategier i følgende land: USA, Canada, Tyskland, Nederland, Storbritannia, Sverige, Finland og Estland. I tillegg er landenes myndigheter forespurt om å gjøre en vurdering av utvalgets utredning, og invitert til å komme med sine innspill.

3.2. Hovedområder

Digitale sårbarheter, som en del av den digitale utviklingen, har vært gjenstand for diskusjon i mange år. Det er likevel først de siste 15 årene at nasjonale myndigheter har løftet dette høyt på den politiske agendaen. Siden 2010 har samtlige av de landene som er sett på i denne rapporten utviklet egne nasjonale strategier for informasjonssikkerhet, IKT-sikkerhet eller cybersikkerhet.

De siste fem årene har myndighetene i flere av disse landene vært svært tydelige i det offentlig rom på at dette er et høyt prioritert område. Amerikanske myndigheter har uttalt at cybertrusselen er den største nasjonale sikkerhetsutfordringen. I Storbritannia er cybertrusselen kategorisert som en «*tier 1 threat*». Allerede i 2011 gikk *UK Cabinet Office* høylytt ut i sin rapport «*The cost of cybercrime*»[1] og fastslo at nasjonen tapte 27 milliarder Pund årlig som følge av manglende cybersikkerhet.

De digitale utfordringene er grenseoverskridende. I 2013 lanserte den Europeiske Union (EU) en egen strategi – *EU Cyber Security Strategy*. Strategien angir klare prioriteringer for EUs internasjonale politikk for det digitale rom, grunnleggende rettigheter som også skal gjelde i det digitale samfunn, og et fritt og åpent Internett[2]. Videre har EU Kommisjonen fremlagt et forslag til europaparlaments- og rådsdirektiv om tiltak for å sikre et felles høyt nivå for nettverks- og informasjonssikkerhet i hele Unionen, «*Network and information security directive*»[3].

Med det formål å identifisere relevante aspekter som kan ha overføringsverdi til norske forhold, er det sett til andre lands gjennomførte og pågående arbeid for å håndter digitale utfordringer. BDO har gått i dybden på områdene myndighetenes organisering og ansvar, nasjonale strategier, hendelseshåndtering, FoU og regulering. I tillegg er det gitt en generell og overordnet beskrivelse av landenes arbeid med personvern. Det presiseres at

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[2] http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm
[3] http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive

personvern er et sentral hensyn i informasjonssikkerhetssammenheng, som i stor grad integreres i landenes øvrige arbeid på området.

3.2.1. Nasjonale myndigheters organisering og ansvar

Samtlige land anser cybertrusselen som en alvorlig sikkerhetsutfordring. Den økende risikoerkjennelsen har medført at arbeid med cybersikkerhet er plassert høyt på den politiske agendaen i alle de utvalgte landene.

Alle landende legger særlig fokus på å organisere cybersikkerhetsarbeidet på en måte som sikrer at det forebyggende sikkerhetsarbeidet blir sett i sammenheng med kriminalitetsbekjempelse, beredskap og hendelseshåndtering. Samtidig er det en gjennomgående økende bevissthet om at det er nødvendig å inkludere alle relevante aktører i cybersikkerhetsarbeidet. Dette gjenspeiles bl.a. ved at myndighetene i USA har etablert en såkalt "whole of government" -tilnærming til cybersikkerhet (samme tilnærming som i kontra-terrorarbeidet). I praksis betyr dette at alle offentlige organer samvirker på tvers av ansvarslinjer for å nå et felles mål om å redusere sikkerhetsrisikoen. En slik tilnærming fordrer strenge krav til etablering av funksjonelle samarbeidsstrukturer der alle relevante aktører deltar. Flere land erkjenner dog at myndighetsorganenes mandater og kompetanse ofte er overlappende, og at manglende samarbeid og samvirke kan føre til at det oppstår «blindsoner». En følge av dette kan være at sentrale tiltak stagnerer eller ikke gjennomføres.

Behovet for helhetlig tilnærming har i mange tilfeller ført til omfattende organisatoriske endringer. I Nederland medførte dette at Justis- og sikkerhetsdepartementet[4] ble utnevnt som overordnet ansvarlig for informasjonssikkerhet. Koordineringen av sikkerhetsarbeidet ivaretas der av «*National Coordinator for Counterterrorism and Security*» (NCTV), som er underlagt det nederlandske Justis- og sikkerhetsdepartementet. Opprettelsen av NCTV skjedde gjennom en sammenslåing av det tidligere «*National Safety and Security Department*», «*National Coordinator for Counterterrorism (NCTb)*» og «*Government Computer Emergency Response Team (GOVCERT.NL)*». Det interessante med denne organisatoriske strukturen er at sikkerhets- og etterretningstjenesten innenlands og kontra-terrorarbeidet samordnes med cybersikkerhetsarbeidet. Som en del av NCTV ble det i 2012 etablert et *National Cyber Security Centre (NCSC)*. Senteret fungerer som bindeledd mellom de ulike ansvarlige organer innen cybersikkerhet, og skal dermed sikre koordinering av de ulike aktivitetene.

Alle de åtte landene uttrykker at de har en helhetlig tilnærming til cybersikkerhetsarbeidet sitt. Konkretiseringen av helhetstilnærmingen varier noe. De fleste av landene satser på samarbeid mellom offentlige og private virksomheter («*public-private cooperation*»[5]). Denne samarbeidsformen springer ut av et behov for informasjonsdeling både for å forebygge uønskede hendelser og for å begrense skadene når slike hendelser likevel inntreffer. Det offentlige har ikke tilstrekkelig kapasitet til å ivareta befolkningens behov for sikkerhet alene; dette kan bare ivaretas gjennom samarbeid og felles innsats fra alle relevante aktører. Særlig Nederland, USA og Storbritannia har derfor

[4] http://www.government.nl/ministries/venj

[5] Det er valgt å ikke oversette dette til «offentlig-privat-samarbeid» i og med at dette har en spissere definisjon i norsk sammenheng; som en ordning der det offentlige og private deler på finansieringen av et prosjekt.

fokusert på å forbedre cybersikkerheten gjennom å etablere strukturer for informasjonsdelingen og samarbeid mellom offentlig og privat sektor. *The National Cybersecurity and Communications Integration Center (NCCIC)* i USA har som oppdrag å sikre at relevant informasjon knyttet til risikobildet, hendelser og analyser blir beskyttet og delt. NCCIC deler informasjon mellom offentlige og private virksomheter, og er også et 24/7 senter som utgjør et samlepunkt for føderale myndigheter, etterretningstjenestene og politimyndighetene. US-CERT er en del av NCCIC.

I de tre ovennevnte landene er det også skapt markedsincentiver for innovasjon og utvikling av sikkerhetsløsninger, samt lagt grunnlaget for implementeringen av overordnede cybersikkerhetsstandarder. Erfaringer fra hvordan disse landene inkluderer offentlige og private virksomheter, sikkerhetsindustrien, akademia, organisasjoner og øvrige institusjoner både i utviklingen av sine cybersikkerhetsstrategier og gjennomføringen av tiltak, har stor overføringsverdi til norske forhold. Dette er noe Norge bør omtale og inkludere ved neste revisjon av den nasjonale strategien for informasjonssikkerhet.

De fleste landene har en nasjonal sikkerhetsstrategi som cybersikkerhetsstrategien blir forankret i. Dette understøtter prioriteringen av cybersikkerhet, og bidrar til strukturering av oppfølgingsarbeidet.

Ivaretakelse av personvern er et sentralt prinsipp som legges til grunn i alle landenes arbeid med cybersikkerhet. Det synes imidlertid å være noe uklare grenser knyttet til dette, all den tid flere land driver masseovervåkning av IKT og samtidig samarbeider tett om deling av etterretningsopplysninger. I denne sammenheng vises det til landenes balansering/avveining mellom personverninteresser og utforming av informasjonssikkerhetsstrategier som krever overvåking/etterretning. Videre vises det til proporsjonalitetskravet i artikkel 8 i den europeiske menneskerettskonvensjonen (EMK), som gjelder vern om privatliv og er grunnlaget for en felles personvernlovgivning ved direktiv 95/EF i EU- og EØS-statene. Ulik grad og dybde av masseovervåkning kan innrettes på ulike måter for å ivareta personvernhensyn, «*privacy by design*» og annen personvernfremmende bruk av teknologi som forvalter enkeltindividers identitet på mer forsvarlige måter. Det er imidlertid et spørsmål om i hvilken grad dette er gjort, eller ikke.

De offentlige budsjettene til organer med ansvar for cybersikkerhet har økt betydelig i de senere årene. Dette reflekterer en økende bekymring for IKT-risikobildet, samt en større vilje til å demme opp for denne utviklingen. Landene satser på både oppbygging av offensive og defensive kapasiteter knyttet til cybersikkerhet. Det kan imidlertid stilles spørsmål ved hvor målrettede disse satsningene har vært, og er. Det er i dag ingen land som har overordnede nasjonale indikatorer for måling av IKT-sikkerhet. Det er derfor vanskelig, om ikke umulig, å fastslå om gitte nasjonale strategier, budsjettsatsninger og øvrige virkemidler faktisk gir en tilfredsstillende sikkerhets- og beredskapsmessige effekt eller ikke.

Det er et gjennomgående trekk at Justis-/Innenriksdepartementene og Forsvarsdepartementene har sentrale roller i alle de åtte aktuelle landene. Videre er det tydelig at alle har et stadig større fokus på de sikkerhetspolitiske aspektene av

cybersikkerhetsarbeidet. Som et resultat utvikler flere land et eget «cyber diplomati» som en del av utenrikstjenestene. Her er USA et foregangsland.

Det er også klare fordeler ved å se det sivile og det militære cybersikkerhetsarbeidet i sammenheng. Eksempelvis har Canada, Storbritannia og Tyskland organer med brede mandater hvor formålet er å sikre kritisk infrastruktur og kritiske samfunnsfunksjoner, uavhengig av om dette er sivilt eller militært.

Den sterke forankringen av cybersikkerhetsarbeidet på øverste myndighetsnivå i *Cabinet Office* i Storbritannia, og den tydelige rollen til *Office of Cyber Security and Information Assurance*[6] (OCSIA), har trolig vært en viktig premiss for at Storbritannia synes å koordinere cybersikkerhetsarbeidet på en svært tilfredsstillende måte[7]. Britiske myndighetsorganer med cybersikkerhetsansvar utmerker seg som svært godt koordinerte. Også Nederland har en moden organisering av cybersikkerhetsarbeidet, og synes å ha etablert hensiktsmessige strukturer for å jobbe systematisk med kvalitetsforbedringer. Særlig to prosesser i Nederland kan ha overføringsverdi til norske forhold;[8] arbeidet med den årlige «Cyber Security Assessment»[9], og prosessen for å identifisere kritiske sektorer der cybersikkerhet bør prioriteres spesielt.

3.2.2. Nasjonale strategier

OECDs «*Guidelines for the security of information systems and networks: Towards a culture of security*»[10] var på mange måter startskuddet for utarbeidelsen av nasjonale strategier for informasjonssikkerhet.[11] De fleste sammenlignbare land har som følge av den digitale utviklingen og utviklingen i risikobildet i flere omganger revidert sine nasjonale strategier på dette området. I de senere år er bl.a. ENISAs «*Good practice guide on national cyber security strategies*» brukt som utgangspunkt i flere lands strategier.[12]

Informasjonssikkerhet prioriteres høyt på den politiske agendaen, og fremheves som en nødvendig forutsetning for opprettholdelse av samfunnets funksjonsdyktighet, nasjonal sikkerhet og økonomisk vekst. Det er økende erkjennelse av at manglende risikohåndtering knyttet til digitale sårbarheter kan true vitale nasjonale interesser og føre med seg enorme økonomiske tap. Dette har ført til økt fokus på organisering av informasjonssikkerhetsarbeidet, samt etablering av hensiktsmessige systemer for risikohåndtering på nasjonalt nivå. Begge aspekter har bidratt til a øke graden av nødvendig samordning og koordinering, samtidig som de har utfordret de tradisjonelle ansvarslinjer og organisasjonsstrukturer både i offentlig og privat sektor. Eksempelvis har USA gjennomført en omfattende evaluering av sitt strategiske arbeid, med det formål at det skal bli mest mulig målrettet.

---

[6] www.gov.uk/government/groups/office-of-cyber-securityand-information-assurance
[7] https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance
8 Basert på generell kommentar til Lysneutvalgets arbeid fra Nederlandske sikkerhetsmyndigheter
9 https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/trend-reports/cyber-security-assessment-netherlands-2014.html
[10] http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm
[11] Benevnelsen informasjonssikkerhet brukes her synonymt med cybersikkerhet. På engelsk benevnes de nasjonale strategiene for informasjonssikkerhet «National cyber security strategy».
[12] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

Det er et gjennomgående trekk at landene har en helhetlige tilnærming til informasjonssikkerhet i sine nasjonale strategier. Strategiene omfatter tiltak rettet mot både enkeltindivider, offentlige og private virksomheters egenbeskyttelse, og det samlede statlige virkemiddelapparatet. Samtidig blir behovet for operative og strategiske samarbeidsmekanismer på tvers av myndighetsorganer, og mellom alle relevante aktører i offentlig og privat sektor, fremholdt som helt nødvendig for å redusere digitale sårbarheter og IKT-kriminalitet på en effektiv og målrettet måte. Dette gjelder både nasjonalt og internasjonalt.

Særlig USA, Storbritannia og Nederland synes å ha gode konsepter for informasjonsdeling og samarbeid i sine strategier. Eksempelvis fremhever Storbritannia behovet for regionale samarbeids- og informasjonsdelingsmekanismer, noe som trolig har stor overføringsverdi til Norge. Det eksisterer i dag en rekke regionale næringsklynger rundt om i Norge der samarbeid innen informasjonssikkerhet trolig kan integreres. Videre fremhever flere land, deriblant USA og Tyskland, særlig behovet for økt innovasjon knyttet til sikkerhetsløsninger som følge av stadig strengere krav til effektivitet og mobilitet. Dette oppnås først og fremst gjennom godt samarbeid og strukturert informasjonsdeling.

Ettersom sikkerhetsutfordringene er grenseoverskridende, blir også behovet for internasjonalt samarbeid understreket i samtlige strategier. Her vises det til USAs internasjonale cybersikkerhetsstrategi,[13] som antas å ha stor overføringsverdi hva gjelder utviklingen av norsk utenrikspolitikk innen cybersikkerhet (bl.a. i tilknytning til prosesser rundt internasjonal regulering av Internett).

Nedenfor følger en oversikt over hvilke temaer som er felles for de åtte landenes nasjonale strategier:

- Styring og ledelse
- Samarbeids- og informasjonsdelingsmekanismer
- Hendelseshåndtering
- IKT-kriminalitet
- Sikkerhetskultur og bevisstgjøring
- Kunnskapsutvikling og innovasjon
- Sikkerhetsutdanning
- Rammeverk og standarder
- Menneskerettigheter og personvern

3.2.3. Hendelseshåndtering

Alle de åtte landene har ett eller flere nasjonale responsmiljøer for håndtering av IKT-hendelser. Samtlige har også nasjonale CERT-er, (*Computer Emergency Response Team*), men organiseringen er noe ulik, både hva gjelder ansvarsområder og plasseringen i forhold til myndighetsstrukturene. Landene poengterer i sine nasjonale strategier at CERT-arbeidet er en avgjørende del av den strategiske tilnærmingen til håndtering av IKT-

[13] https://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf

hendelser på nasjonalt nivå. I tillegg fremheves det av flere at hendelseshåndtering og IKT-sikkerhet er et virksomhetsansvar.

Nederland har en helhetlig og målrettet tilnærming til hendelseshåndtering. Landet har valgt å samle hovedtyngden av sin IKT-sikkerhetsekspertise og hendelseshåndtering på nasjonalt nivå i et nasjonalt cybersikkerhetssenter (NCSC). Dette inkluderer både et nasjonalt rapporteringspunkt, CERT-funksjonen fra den tidligere GOVCERT-NL, koordineringsansvar ved IKT-hendelser, monitoring og informasjonsdeling. NCSC opererer i tillegg et offentlig varslingssystem rettet mot mindre virksomheter og befolkningen forøvrig.

I 2011 etablerte også Tyskland sitt «*Nationales Cyber – Abwehrzentrum*» (Nasjonale cyber responssenter). Formålet med senteret er også her å optimalisere samarbeidet mellom de statlige myndighetene.

USA har en noe annerledes tilnærming, hvor de nasjonale kapasitetene på IKT-sikkerhet er spredt mellom flere aktører, herunder US-CERT, en egen ICS-CERT (CERT for SCADA-systemer), en nasjonal task-force for etterforskning i det digitale rom (NCIJTF) i regi av FBI, *US Cyber Command* under Forsvarsdepartementet, the *Intelligence Community – Incident Response Center (IC-IRC)*, *National Security Agency/Central Security Services Threat Operations Center (NTOC)*, *DoD Defense Cyber Crime Center (DC3)*, og nylig etablerte *Cyber Threat Intelligence Integration Center (CTIIC)*. Samtidig er ambisjonen at IKT-hendelseshåndtering skal være en samlet innsats mellom disse aktørene, koordinert gjennom *National Cyber Security and Communications Integration Center (NCCIC)*. NCCIS skal blant annet ha et oppdatert situasjonsbilde, drive IKT-hendelseshåndtering og styring, samt være et nasjonal knutepunkt for føderale myndigheter, etterretningssamfunnet og politimyndigheter. US-CERT og ICS-CERT er en integrert del av NCCIC.

De ulike organene i den amerikanske satsingen på IKT-sikkerhet utfyller det flersidige bildet i et stort land med en kompleks organisering. Mens DHS, gjennom *National Cyber Security and Communications Integration Center (NCCIC)*, proaktivt skal håndtere digital risiko og sørge for informasjonsdeling om digitale sårbarheter, har *The National Cyber Investigative Joint Task Force (NCIJTF)*, som består av 19 etterretningsbyråer og rettshåndhevende myndigheter, fokuset på å trygge internett gjennom aktivt å jakte på trusselaktører.

For IKT-hendelseshåndtering i Storbritannia, har man på nasjonalt nivå delt ansvaret mellom GovCERT.uk og CERT-UK. Sistnevnte ble grunnlagt i 2014, og var en viktig satsing som oppfølging av den nasjonale cybersikkerhetsstrategien. CERT-UK har fokus på å ha et oppdatert situasjonsbilde, hendelseshåndtering på nasjonalt nivå, samt å støtte virksomheter med samfunnskritisk infrastruktur. GovCertUK har på sin side ansvaret for å koordinere hendelseshåndtering og tiltak for myndighetsorganer.

I juni 2014 lanserte britiske myndigheter satsingen «*Cyber Essentials*», en sertifiseringsordning som støttes av industrien og som skal stimulere til utbredt bruk av grunnleggende sikkerhetskontroller for å beskytte organisasjoner mot mindre avanserte IKT-hendelser. Sertifiseringen kommer med et merke som benyttes av bedrifter til å

demonstrere sitt sikkerhetsnivå til kunder og investorer, og som forsikringsselskaper kan ta i betraktning når de vurderer IKT-sikkerhetsnivået og påfølgende beregne forsikringspremier til bedrifter. Som et annet initiativ har *The Council for Registered Ethical Security Testers (CREST)* nylig innført en godkjenningsordning for selskaper som jobber med IKT-sikkerhet i Storbritannia. Ordningen har blitt godkjent av GCHQ og CPNI og fokuserer på aktuelle standarder for hendelseshåndtering justert til å passe alle sektorer og industrier. Dette er tiltak som har stor overføringsverdi til Norge.

3.2.4. Informasjonsdeling og offentlig-privat samarbeid

Det er enighet om viktigheten av å dele informasjon, både i det forebyggende sikkerhetsarbeidet og ved hendelseshåndtering, i et flertall av de nasjonale myndighetene som BDO har sett på. Dette understrekes i både i de nasjonale strategiene og annet informasjonsmateriell fra disse myndighetene. Mekanismer og plattformer for å dele informasjon er tett integrert med hendelseshåndteringsmiljøene, herunder USAs *National Cyber Security and Communications Integration Center (NCCIC)*, Nederlands *National Cyber Security Center* og Storbritannias *CERT-UK*.

I Storbritannia er det også igangsatt et fellesinitiativ mellom myndighetene og industrien hva angår informasjonsdeling og samarbeid for å møte de digitale truslene, kalt *Cyber-Security Information Sharing Partnership (CISP)*. Allerede ved utgivelsen av den nasjonale strategien i 2011 ble det gjort klart at myndighetenes tilnærming til cybersikkerhet er risikobasert, og at arbeidet må gjøres i partnerskap med private aktører. Dette primært på grunnlag av at det digitale rom er et område hvor myndighetene erkjenner sine begrensinger og at de ikke kan nå målene alene.

President Obamas «Executive order 13691» angir et rammeverk for utvidet informasjonsdeling, og promoterer informasjonsdeling både innad i privat sektor og mellom private virksomheter og myndighetene i USA.

Offentlig-privat samarbeid er også løftet som et satsingsområde i flere av de andre landene. Det legges generelt stor vekt på at deling av informasjon mellom offentlige og private aktører er et viktig premiss for at samfunnet skal kunne møte utfordringene som følger den digitale utviklingen. Allerede to år etter utgivelsen av sin første nasjonale strategi, reviderte Nederland denne. I 2013-versjonen var rundt 130 nye aktører, fra både offentlig og privat sektor, involvert i forarbeidet.

3.2.5. Forskning og utvikling

Alle landene har over tid fokusert på og prioritert forskning- og utviklingsarbeid i sine nasjonale strategier. De vektlegger alle viktigheten av FoU-området, da særlig med tanke på sårbarhetsreduksjon, men også hva gjelder effektiv utnyttelse av samfunnets samlede informasjonsteknologi. I de fleste nasjonale strategiene er FoU-begrepet nært knyttet til myndighetenes og næringslivets behov for informasjonssikkerhet. Enkelte av landene kobler også begrepet opp mot befolkningens behov for økt sikkerhetsbevissthet (og kunnskap).

Et annet fellestrekk er at FoU-innsatsen er et samarbeidsprosjekt mellom myndigheter, akademiske miljøer og privat sektor. Imidlertid er selve finansieringen av

utdanningsprogrammer og lignende i liten grad beskrevet i strategiene. Et unntak er Tyskland, hvor Utdannings- og forskningsdepartementet tilsynelatende har finansiert en rekke større forskningsprosjekter de siste årene.

Måten å operasjonaliserer FoU-begrepet i strategiene varierer. Generelt vektlegger samtlige av landende behovet for spesialiserte utdannings- og forskningsprogrammer, særlig på universitetsnivået. De fleste har også igangsatt særskilte strategier og initiativ, som skal sikre tilgang på en stabil og kvalifisert arbeidskraft. USA og Storbritannia fremhever spesielt hvordan deres sikkerhets- og etterretningstjenester har et særskilt samarbeid med utvalgte universiteter.

Den bredeste tilnærmingen til FoU-begrepet finner man i Finland, Storbritannia, Nederland og delvis i Estland. Disse vektlegger at IKT-sikkerhet må være en del av det generelle utdanningsløpet allerede fra barneskolenivå, og videre oppover.

3.2.6. Regulering

Det er gjennomgående at landene vurderer at de lover og regler vi i dag har i den fysiske verden, også gjelder i den digitale verden. Samtidig erkjennes det at det kan være utfordrende å finne de riktige regulatoriske virkemidlene og å oppdatere lovverket slik at det blir anvendbart i den «nye virkeligheten».

Det er vanlig at informasjonssikkerhet reguleres i sektorspesifikke regelverk. Således blir for eksempel kraftsektorens informasjonssikkerhetsarbeid regulert gjennom det lovverket som gjelder for kraftsektoren. Det er også vanlig at ulike lovformål innenfor informasjonssikkerhetsarbeidet reguleres hver for seg. Dette gjelder for eksempel straffebestemmelser mot datakriminalitet, ivaretakelse av personvern og opphavsrettigheter, bestemmelser om sikkerhetsgradering og beskyttelse av statshemmeligheter, osv. Det er også vanlig med en lovfesting av ansvar og oppgaver til sentrale myndighetsorganer. Eksempelvis er mandat og oppgaver til både BSI i Tyskland og DHS i USA gitt i egne spesiallover. Det er foreløpig uvanlig med en overordnet cybersikkerhetslov. Det pågår imidlertid regelverksarbeid knyttet til dette i flere land. Eksempelvis søker Obama-administrasjonen å få vedtatt en slik overordnet cyberlov.

Selv om det ikke er vanlig med en overordnet lov for cybersikkerhet, legges et økende antall standarder til grunn for informasjonssikkerhetsarbeid. Mange av disse standardene er overlappende i det at de regulerer implementeringen av et styringssystem for informasjonssikkerhet, med mål om et mer strukturert og systematisk arbeid for å bedre kvaliteten på informasjonssikkerheten generelt og implementeringen av risikoreduserende tiltak spesielt. Et svært godt eksempel på en slik standard er «*Framework for Improving Critical Infrastructure Cybersecurity*»,[14] utgitt av *National Institute of Standards and Technology (NIST)* i USA, og det helhetlige veiledningsmaterialet i cybersikkerhet utarbeidet av britiske *GCHQ, CPNI* og *Department for Business Innovation and Skills (BIS)*[15], Sistnevnte inkluderer bl.a. en lett tilgjengelig og svært anerkjente veileder kjent som «*10 Steps to Cybersecurity*».

[14] http://www.nist.gov/cyberframework/
[15] https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

President Obama utstedte i 2013 ordre (EO) 13636 *«Improving Critical Infrastructure Cybersecurity»*, og *Presidential Policy Directive-21 (PPD) «Critical Infrastructure Security and Resilience»*. Disse dokumentene henstilte føderale myndigheter til å iverksette tiltak for å styrke sikkerheten og robustheten i kritisk infrastruktur mot økende trusler, gjennom et oppdatert og overordnet nasjonalt rammeverk som anerkjenner IKTs økte rolle i å sikre fysiske verdier. Sammen angir disse to dokumentene retning mot en *«whole of community»* tilnærming til risikostyring, sikkerhet og robusthet. Ordren (EO 13636) gav også *«the National Institute of Standards and Technology» (NIST)* i oppdrag å utvikle det ovennevnte rammeverk for cybersikkerhet, basert på sammenstilling av standarder og beste praksis i bransjen. Denne ordren henstilte også DHS til å etablere et frivillig program for cybersikkerhet i kritisk infrastruktur, til å fungere som en føderal koordineringsenheten for cybersikkerhetsressurser, og støtte økt digital motstandsdyktighet ved å fremme bruk av rammeverket. Programmet skal legge til rette for en felles tilnærming til risikostyring, sikkerhet og robusthet.

Utarbeidelse av standarder for cybersikkerhet synes å være styrt av markedsinsentiver. Eksempelvis er alle myndighetsorganer i Storbritannia forpliktet til å kreve at leverandører som skal behandle sensitiv informasjon overholder gitte standarder for informasjonssikkerhet.[16] Videre pågår det en diskusjon i USA angående erstatningsansvar ved uaktsomhet knyttet til informasjonssikkerhet, som følge av hendelser som har hatt store økonomiske konsekvenser. Manglende juridisk forankring av spesifikke sikkerhetskrav kan imidlertid gjøre dette vanskelig å gjennomføre.

Det kan vurderes nærmere lovfesting av ansvar og roller knyttet til cybersikkerhet i norsk lovgivning. Dette eksemplifisert gjennom erfaringene fra bl.a. IMSI-catcher saken, som viste at uklare ansvarslinjer kan føre til at sentrale oppgaver faller mellom to stoler.

De fleste land har et informasjonssikkerhetsregleverk som regulerer klassifisering av skjermingsverdig informasjon, tilsvarende det norske graderingssystemet i sikkerhetsloven. Det er imidlertid ikke fullt ut samsvar mellom antall graderingsnivåer, hvilket kan skape utfordringer med hensyn til deling av skjermingsverdig informasjon mellom nasjoner.

Cyberhendelser går ofte på tvers av organisatoriske og geografiske grenser. Dette skaper utfordringer, i og med at nasjonale myndigheter ofte definerer hendelsene ut fra sitt eget perspektiv. Det vil si at en hendelse kan bli vurdert forskjellig avhengig av hvorvidt den oppdages av en etterretningsorganisasjon, en sikkerhetstjeneste, eller politiet. Ulike fullmakter og begrensinger i jurisdiksjon kan da skape ytterligere utfordringer i forhold til håndteringen.

3.2.7. Personvern

Ivaretakelse av innbyggernes frihet og personvern er av alle landene anerkjent som et viktig premiss for arbeidet med IKT-sikkerhet. EU-medlemsland må også forholde seg til det overnasjonale regelverket på området, herunder *«Directive on Personal Data»*, *«the Data Retention Directive»*, og *«the Privacy and Electronic Communications Directive»*.

[16] www.gov.uk/government/publications/cyber-essentialsscheme-overview

Storbritannia, Tyskland, Finland, Estland og Nederland har i tillegg egne nasjonale lovverk for beskyttelse av data og personvern. Tilsvarende gjelder også Canada. Det er derimot ingen enkelt lov i USA som gir en omfattende regulering av databeskyttelse eller personvern. Dette løftes likevel frem som et viktig premiss, blant annet av DHS, og nevnes i både strategier og annet lovverk som omhandler IKT-sikkerhet. Nederland har en egen nasjonal «*Data Protection authority*» og vurderer også en potensiell ny paragraf i grunnloven som omhandler beskyttelsen av innbyggernes digitale rettigheter.

I 1980 vedtok OECD sine første retningslinjer om personvern og utveksling av personopplysninger over landegrensene. Retningslinjene er revidert og oppdatert, og foreligger nå på norsk. Disse oppfordrer medlemslandene til internasjonalt samarbeid for å fremme godt personvern. Slikt samarbeid er helt nødvendig i en verden der varer, tjenester og personopplysninger er i stadig bevegelse, og utfordringene er internasjonale.[17]

Det kan skilles mellom det som er felles for EU/EØS-stater (for eksempel direktiver som er inntatt i de enkelte lands lovgivning) og det som skjer i USA og Canada hva gjelder personvern. Canada har vært tydelige på personvern i mange sammenhenger og var det første landet som lanserte muligheter for å ivareta personvern med «*privacy by design*». *European Data Protection Supervisor (EDPS)*, er EUs ombudsmann for personvern. Artikkel 29 gruppen i EU, uttaler seg om ivaretakelse av personvern opp mot ulike andre hensyn.

3.3. Overføringsverdi

Over er det identifisert en rekke forhold ved andre lands arbeid med informasjonssikkerhet som potensielt kan ha overføringsverdi for Norge. Noen momenter er identifisert hos alle, eller de fleste av landene. For eksempel har alle et stort fokus på helhetlig tilnærming, selv om de organisatoriske løsningene for å ivareta denne er noe ulike. Samtlige land har også ett eller flere nasjonale responsmiljøer for håndtering av IKT-hendelser. Videre har flere av landene prioritert inkludering av offentlige og private virksomheter, sikkerhetsindustrien, akademia, organisasjoner og øvrige institusjoner både i utviklingen av sine cybersikkerhetsstrategier og i gjennomføringen av tiltak. FoU-innsatsen er i alle landene fremhevet som samarbeidsprosjekt mellom myndigheter, akademiske miljøer og privat sektor.

Videre har de ulike landenes tilnærming noen særskilte elementer som potensielt kan ha stor overføringsverdi for norske forhold. Tabellen nedenfor lister en del momenter som BDO mener er representativt for landenes arbeid med digitale sårbarheter, og som potensielt kan ha overføringsverdi til Norge.

[17] https://www.regjeringen.no/globalassets/upload/kmd/sta/dokumenter/oecds_retningslinjer_personvern.pdf?id=2221510

Tabell 1: Arbeid med overføringsverdi til Norge

	Nasjonale myndigheters styring og organisering	Nasjonale strategier	Hendelseshåndtering	Informasjonsdeling og offentlig-privat-samarbeid	Forskning og utvikling	Regulering	Person-vern
USA	*"Whole of government"* tilnærming til cybersikkerhet *En «whole of community» tilnærming til risikostyring,*	Behovet for utvikling av utenrikspolitikken knyttet til cyberdomenet	IKT-hendelseshåndtering som en samlet innsats mellom flere aktører, med et nasjonalt knutepunkt (NCCIC)	Offentlig-privat samarbeid Innovasjon gjennom informasjonsdeling og samarbeid NCCIC skal sikre at relevant informasjon relatert til risiko, hendelser og analyser blir både beskyttet og delt. NCCIC deler informasjon mellom offentlige og private virksomheter. Executive order 13691 promoterer informasjonsdeling i privat sektor og mellom private og myndighetene. Rammeverk for utvidet informasjonsdeling	Sikkerhets- og etterretnings-tjenester har et særskilt samarbeid med utvalgte universiteter	NIST rammeverk for cybersikkerhet (standarder og best practices)	
Canada	*Shared Services Canada*– a streamlining of federal IT communications *Communications Security Establishment Canada*– Bredt scope for å forsvare nettverks-infrastrukturer		Tydelig ansvarsdeling mellom første rapporterings-punkt, The *Canadian Cyber Incident Response Centre (CCIRC*), *The Government Operations Centre,* Politimyndighet og sikkerhets- og etterretnings-tjenesten	Samarbeidsavtale med USA Koalisjon mellom myndighetene, private selskaper og ideelle organisasjoner Anerkjenner behovet for å dele sensitiv informasjon, og et mål er å tilrettelegge for sikkerhetsklarering av private aktører			*Privacy by design*
Stor-britannia	Sterk forankring av cyber-sikkerhets-arbeidet på øverste myndighetsnivå	Prioritering av samarbeids- og informasjons-delings-mekanismer	Koordinerings-organ *«Cyber Essentials»,* Sertifisering som bedrifter bruker til å demonstrere sikkerhetsnivå til kunder og investorer Godkjennings-ordning for selskaper som jobber med IKT-sikkerhet.	Cyber-Security Information Sharing Partnership (CISP). Regionale samarbeidsmekanismer	Sikkerhets- og etterretnings-tjenester har et særskilt samarbeid med utvalgte universiteter.	*10 Steps to Cyber security* *Sikkerhets-krav til leverandører*	

	Nasjonale myndigheters styring og organisering	Nasjonale strategier	Hendelseshåndtering	Informasjonsdeling og offentlig-privat-samarbeid	Forskning og utvikling	Regulering	Person-vern
Tyskland	*"National Plan for Information Infrastructure Protection",* (NPSI) *The IT Security Act* – Forholdet mellom risiko, beskyttelse og ansvar	Digital Agenda 2014 -2017 Fremhever behovet for økt innovasjon knyttet til sikkerhetsløsninger	Nettverk av CERT-er, både statlige og private National Cyber Response Centre – Alle andre enheter deler og samarbeider om informasjon og analyser med senteret	Innovasjon gjennom samarbeid		Lovarbeid og regulering på området	
Nederland	Helhetlig tilnærming Offentlig-privat samarbeid om den nasjonale strategien Årlig *«Cyber Security Assessment»* Identifisere kritiske sektorer der cybersikkerhet bør prioriteres	Oppdaterte nasjonale strategier (ny versjon er ventet i 2016)	Samling av hovedtyngden av sin IKT-sikkerhets-ekspertise og hendelses-håndtering på ett nasjonal nivå	ISAC Offentlig- privat samarbeid ved utarbeidelse av nasjonal strategi			
Sverige				Flere samarbeidsforum der både statlige og regionale myndigheter, næringsliv og interessegrupper er inkludert. Felles for alle er den sentrale rollen til MSB beholdning. For utviklingen av svensk informasjons- og cybersikkerhet på et bredere nivå, er det MSB ledede Informasjons-sikkerhetsrådet	Fokus på informasjons-sikkerhet i forskning- og utdannings-miljøene		
Finland				The National Emergency Supply organization (NESO)	Bred tilnærming til FoU		

	Nasjonale myndigheters styring og organisering	Nasjonale strategier	Hendelseshåndtering	Informasjonsdeling og offentlig-privat-samarbeid	Forskning og utvikling	Regulering	Person-vern
Estland		Implementering av strategien involverer alle statlige aktører Høyt prioritert å sikre at man er forberedt på, og effektivt kan håndtere, en IKT-hendelse, så vel som forebygging.	The Estonian National Cyber Defence League. En frivillig responsenhet av IT-profesjonelle og representanter fra kritisk infrastruktur Kategorisering av IKT-hendelser etter gitte kriterier og alvorlighetsgrad Lovpålagt hendelses-rapportering for offentlige virksomheter	CIIP commission to promote public-private cooperation		*"The Regulation on Security Measures for Information Systems of Vital Services and Related Information Assets"*	

4. National Cyber Security: USA

4.1. National Government and Cyber Security

The USA has identified the cyber threat as one of the most serious economic and national security challenges.[18] As with its counterterrorism efforts, the United States Government is taking a "whole-of-government" approach to defend against and respond to this threat.[19]

The strategic approach to cybersecurity has been comprehensive, and based on principles that enhance public-private cooperation, knowledge and expertise, flexibility to adapt to a constantly evolving risk environment, and the protection of privacy and civil liberties.

The primary focus in the USA has been on improving cybersecurity, and on expanding information sharing and collaboration between the government and the private sector to improve cybersecurity. This approach has laid the foundations for a collaboration with the private sector to implement standards and best practices with market incentives.

Federal funding on cybersecurity has increased over the recent years, reflecting the intensity of threats U.S. companies and government agencies are facing from cyber intruders, both domestic and foreign. [20] The Department of Homeland Security (DHS), Department of Defense (DOD), The Office of the Director of National Intelligence (ODNI) and the Department of Justice (DOJ), constitute the primary government bodies responsible for cyber security in the US.

A number of steps to reduce the digital vulnerabilities are under way, such as the deployment of more intrusion detection mechanisms and prevention capabilities, increased information sharing between government and industry, and improved cyber incident response capabilities.

4.2. National Cyber Security Strategy and policy

4.2.1. US National Strategy to Secure Cyberspace

The US National Strategy to Secure Cyberspace was published in 2003. The cornerstone of the strategy was the invitation of public-private partnerships to implement this strategy. The National Strategy to Secure Cyberspace identified eight major actions and initiatives for cyberspace security response[21]:

1. Establish a public-private architecture for responding to national-level cyber incidents;
2. Provide for the development of tactical and strategic analysis of cyber-attacks and vulnerability assessments;
3. Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace;
4. Expand the Cyber Warning and Information Network to support the role of DHS in coordinating crisis management for cyberspace security;
5. Improve national incident management;
6. Coordinate processes for voluntary participation in the development of national public-private continuity and contingency plans;
7. Exercise cybersecurity continuity plans for federal systems; and

[18] https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative
[19] https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center
[20] http://www.reuters.com/article/2015/02/02/usa-budget-cybersecurity-idUSL1N0VC0XH20150202
[21] https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

8. Improve and enhance public-private information sharing involving cyber-attacks, threats, and vulnerabilities.

4.2.2. The Cyberspace policy review

Recognizing the challenges and opportunities, the President identified cybersecurity as one of the top priorities of his administration and directed a 60-day, comprehensive review to assess U.S. policies and structures for cybersecurity. The Cyberspace policy review - Assuring a Trusted and Resilient Information and Communications Infrastructure, was published in 2009.

The review addressed all missions and activities associated with the information and communications infrastructure, including computer network defense, law enforcement investigations, military and intelligence activities, and the intersection thereof with information assurance, counterintelligence, counterterrorism, telecommunications policies, and general critical infrastructure protection.[22]

4.2.3. The International Strategy for Cyberspace

The International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World was published in 2011. This Strategy outlines a vision for the future of cyberspace, and sets an agenda for partnering with other nations and peoples to realize it. To realize the future it seeks, the United States will combine diplomacy, defense, and development to enhance prosperity, security, and openness so all can benefit from networked technology. It also calls for harmonizing cybercrime laws internationally by expanding accession to the Budapest Convention. [23]

4.2.4. Department of Defense Strategy for Operating in Cyberspace

The Department of Defense published its Cyber strategy in April 2015[24]. The defense strategy outlines five strategic goals:

1. Build and maintain ready forces and capabilities to conduct cyberspace operations.
2. Defend the DOD information network, secure DOD data, and mitigate risks to DOD missions.
3. Be prepared to defend the U.S. Homeland and U.S. vital interests from disruptive cyberattacks of significant consequence
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.
5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

4.2.5. Comprehensive National Cybersecurity Initiative (CNCI)

President Obama determined that the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008, should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy.[25]

The CNCI consists of a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace:

1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.
2. Deploy an intrusion detection system of sensors across the Federal enterprise.

[22] http://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf
[23] ttps://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf
[24] http://www.defense.gov/home/features/2015/0415_cyber-strategy/
[25] https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

3. Pursue deployment of intrusion prevention systems across the Federal enterprise.
4. Coordinate and redirect research and development (R&D) efforts.
5. Connect current cyber ops centers to enhance situational awareness.
6. Develop and implement a government-wide cyber counterintelligence (CI) plan.
7. Increase the security of our classified networks.
8. Expand cyber education.
9. Define and develop enduring "leap-ahead" technology, strategies, and programs.
10. Define and develop enduring deterrence strategies and programs.
11. Develop a multi-pronged approach for global supply chain risk management.
12. Define the Federal role for extending cybersecurity into critical infrastructure domains.

4.2.6. Executive Order 13636, Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience

In February 2013, President Obama issued Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive-21 (PPD) on Critical Infrastructure Security and Resilience. These documents direct the Federal Government to take actions to strengthen the security and resilience of critical infrastructure against evolving threats through an updated and overarching national framework that acknowledges the increased role of cybersecurity in securing physical assets. Together, the EO and PPD drive action toward a whole of community approach to risk management, security and resilience. The EO directed the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework, based on a collection of cybersecurity standards and industry best practices. The EO also directed DHS to establish a voluntary program for critical infrastructure cybersecurity, to serve as a federal coordination point for cybersecurity resources and support increased cyber resilience by promoting use of the Framework. The Critical Infrastructure Cyber Community (C3) Voluntary Program (Pronounced "C-Cubed" Voluntary Program) will facilitate a community approach to risk management, security, and resilience.

4.2.7. Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing

In February 2015, President Obama issued Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing to encourage and promote sharing of cybersecurity threat information within the private sector and between the private sector and government. This Executive Order lays out a framework for expanded information sharing designed to help companies work together, and work with the federal government, to quickly identify and protect against cyber threats[26].

4.3. Incident Response

Cyber incident response in USA is a joint effort between the responsible entities in the intelligence community, US Defense, homeland security, law enforcement and counter intelligence, and civil response capabilities in the public and private sector.

4.3.1. Department of Homeland Security

The Department of Homeland Security (DHS) is the federal agency defined by statute as charged with homeland security, which includes strengthening cyberspace and critical infrastructure. The Secretary of Homeland Security is responsible for coordinating the domestic all-hazards preparedness efforts of all executive departments and agencies. Preparedness efforts include those actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against,

[26] https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform

mitigate the effects of, respond to, and recover from those threats and hazards that pose the greatest risk to the security and resilience of the Nation.

The Department operates the National Cybersecurity and Communications Integration Center (NCCIC) which ensures relevant cybersecurity information related to risks, incidents and analysis is safeguarded and shared; provides technical assistance, risk management support and incident response and mitigation capabilities. It is a 24x7 center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement. The NCCIC shares information among the public and private sectors to provide greater understanding of cybersecurity and communications situation awareness of vulnerabilities, intrusions, incidents, mitigation, and recovery actions.[27]

The United States Computer Emergency Readiness Team (US-CERT), part of the NCCIC, leads efforts to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the privacy and constitutional rights of Americans.[28] Additionally, US-CERT collaborates with private sector critical infrastructure owners and operators, academia, federal agencies, Information Sharing and Analysis Centers (ISACs), state and local partners, and domestic and international organizations to enhance the Nation's cybersecurity posture.

The Federal Information Security Modernization Act of 2014 (FISMA) establishes in law the authorities of the Office of Management and Budget and DHS with respect to the security of federal systems. It authorizes the establishment of a federal information security incident center to assist agencies in handling a cyber incident. US-CERT operates the federal information security incident center required under FISMA.[29]

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), another part of the NCCIC, works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.[30]

DHS, through U.S. Immigration and Customs Enforcement Homeland Security Investigations, operates the Cyber Crime Center, which is responsible for providing domestic and international training; and the support, coordination and de-confliction of cyber investigations related to online economic crime, digital theft of export-controlled data, digital theft of intellectual property and online child exploitation investigations.

The U.S. Secret Service leads a network of Electronic Crimes Task Forces to bring together federal, state, and local law enforcement, prosecutors, private industry, and academia for the common purpose of preventing, detecting, mitigating, and investigating various forms of malicious cyber activity.

4.3.2. National Cyber Investigative Joint Task Force (NCIJTF).

The FBI is responsible for developing and supporting the National Cyber Investigative Joint Task Force (NCIJTF), which includes 19 intelligence agencies and law enforcement, working side by side to identify key players and schemes. Its goal is to predict and prevent what is on the horizon and to pursue the enterprises behind cyber attacks. Instead of

[27] http://www.dhs.gov/about-national-cybersecurity-communications-integration-center
[28] https://www.us-cert.gov/about-us
[29] https://www.us-cert.gov/incident-notification-guidelines
[30] https://ics-cert.us-cert.gov/

focusing on reducing cyber vulnerabilities, the NCIJTF focuses on making the Internet safer by identifying and pursuing the terrorists, spies, and criminals who seek to exploit US systems.[31]

4.3.3. US Cyber Command (USCYBERCOM)[32]

In 2009, the US Secretary of Defense directed the Commander of U.S. Strategic Command (USSTRATCOM) to establish USCYBERCOM. Initial Operational Capability (IOC) was achieved in May 2010. USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to USA's adversaries.

4.3.4. Intelligence Community—Incident Response Center (IC-IRC)[33]

The Intelligence Community – Incident Response Center (IC-IRC) provides Intelligence incident reporting and response for IC continuity of operations, and serves as cyber alert and notification focal point. The IC-IRC collaborated with and shares information among Intelligence and Computer Network Defense communities, Department of Defense, US-CERT and other incident response organizations. Its main function is to provide foreign threat-based analysis to assist in gaining attribution regarding a cyber attack. The IC-IRC provides network threat analysis and correlation, vulnerability management notification and status reporting for IC as well as threat message dissemination and status monitoring.

4.3.5. NSA/CSS Threat Operations Center (NTOC) [34]

The National Security Agency/Central Security Services Threat Operations Center (NTOC) facilitates and coordinates the identification and development of countermeasures, and provides support during security incidents when needed; felicitating security incident reporting to the appropriate authority and providing worldwide dissemination of threat advisories. NTOC collaborates with NIST, US-CERT, and other operational entities. NTOC facilitates cooperation, planning, and coordination between organizations (such as the Defense Information Security Agency - DISA) responsible for information systems security incidents.

NTOC reviews information to determine cyber threats and vulnerabilities and to develop mitigation strategies. NTOC coordinates analysis with the Defense Intelligence Agency (DIA) for all-source threat analysis. NTOC supports cyber defense elements of major Combatant Commander and national-level exercises and provides network analyst training courses at the National Cryptologic School. NTOC also publishes security configuration guides; partners with DHS to sponsor National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD).

4.3.6. DoD Defense Cyber Crime Center (DC3)

DC3 supports investigative missions for the Defense Criminal Investigations Organizations (DCIOs); The Defense Computer Forensics Laboratory (DCFL) and the Defense Cyber Investigations Training Academy (DCITA). DC3 serves as focal point for the Defense Industrial Base (DIB); collaborates with DoD offices and other agencies on digital forensic intelligence efforts. DC3 partners with governmental, academic and private sector computer security officials.[35]

[31] http://www.fbi.gov/about-us/investigate/cyber/ncijtf
[32]http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdfhttp://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf
[33] https://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf
[34] https://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf
[35] https://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf

4.3.7. Cyber Threat Intelligence Integration Center (CTIIC)

The new Cyber Threat Intelligence Integration Center will be a national intelligence center focused on "connecting the dots" regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests, and on providing all-source analysis of threats to U.S. policymakers.[36]

The CTIIC will not be an operational center. It will not collect intelligence, manage incident response efforts, direct investigations, or replace other functions currently performed by existing departments, agencies, or government cyber centers. Instead, the CTIIC will support the NCCIC in its network defense and incident response mission; the NCIJTF in its mission to coordinate, integrate, and share information related to domestic cyber threat investigations; and U.S. Cyber Command in its mission to defend the nation from significant attacks in cyberspace. The CTIIC will provide these entities, as well as other departments and agencies, with intelligence needed to carry out their cybersecurity missions. […] No decisions have been made regarding the CTIIC's specific location, but the current plan is to locate the CTIIC in […] an existing Intelligence Community facility.[37]

4.4. Legislative and Regulatory frameworks

Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for critical infrastructure, such as the Department of Transportation for the transportation sector. [38]

The Department of Homeland Security, together with the Department of Justice, Department of Defense and the National Security Agency, constitute the primary cross-sectoral federal cyber security authorities.

Existing legislation, executive orders, and national policy cover different aspects of cybersecurity in the USA, such as information sharing, critical infrastructure protection, cybercrime, and privacy.

Current US legislation that may have relevance to Norway and other allies, include the Homeland Security Act, the Federal Information Security Modernization Act[39], National Cybersecurity Protection Act of 2014[40], The Cybersecurity Workforce Assessment Act[41] and The Cybersecurity Enhancement Act of 2014[42]

4.4.1. The Homeland Security Act

The Homeland Security Act gives DHS responsibility for homeland security and critical infrastructure protection. This includes federal responsibility for cybersecurity in the civil sector.

4.4.2. The Federal Information Security Modernization Act of 2014 (FISMA)

FISMA gives DHS specific tasks related to overseeing and assisting government bodies in their work on cybersecurity. FISMA clarifies the responsibility federal organizations have related to cybersecurity.

4.4.3. The National Cybersecurity Protection Act of 2014

The National Cybersecurity Protection Act amends the Homeland Security Act of 2002 to establish a national cybersecurity and communications integration center in the Department of Homeland

[36] https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center
[37] https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center
[38] https://fas.org/sgp/crs/natsec/R42114.pdf
[39] https://www.congress.gov/bill/113th-congress/senate-bill/2521
[40] https://www.congress.gov/bill/113th-congress/senate-bill/2519
[41] https://www.congress.gov/bill/113th-congress/house-bill/2952/
[42] https://www.congress.gov/bill/113th-congress/senate-bill/1353

Security (DHS) to carry out the responsibilities of the DHS Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and related DHS programs.[43]

4.4.4. The Cybersecurity Workforce Assessment Act

Cybersecurity Workforce Assessment Act - Directs the Secretary of Homeland Security, within 180 days and annually thereafter for three years, to conduct an assessment of the cybersecurity workforce of the Department of Homeland Security (DHS).[44]

4.4.5. The Cybersecurity Enhancement Act of 2014

Cybersecurity Enhancement Act of 2014 amends the National Institute of Standards and Technology Act to permit the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), to facilitate and support the development of a voluntary, consensus-based, industry-led set of standards and procedures to cost-effectively reduce cyber risks to critical infrastructure.[45]

4.4.6. Corporate liability

There is an ongoing debate in the US regarding liability in case of corporate negligence concerning cyber security. The absence in many instances of legal requirements to meet specific standards makes this difficult to implement. Nevertheless, the Target Breach in 2013 shows that top executives can be held accountable for major security breaches.

4.5. Knowledge, Research and Education

The Cyberspace Policy Review clearly states the need for enhancing efforts on knowledge, research and education in cybersecurity. This was also addressed in the Comprehensive National Cybersecurity Initiative (CNCI). The initiative calls for a "technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees"[46]. The National Initiative for Cybersecurity Education (NICE) was established to follow up CNCI goals related to public awareness, education, professional development, and talent management. The target audiences for NICE include the general public, students, and the cybersecurity workforce.[47] The development of an adequate cyber workforce will begin with improvements in education, from kindergarten and into university.

Private entities, nongovernmental organizations, universities and other research institutions, play a significant role in developing knowledge and further advancements in the field of cybersecurity in USA. This is clearly acknowledged by the current Administration, and President Obama has on several occasions stressed the importance of making this a shared mission.

In addition to this, the NSA and DHS have developed criteria for cybersecurity education programs, and recognize institutions that met these criteria as "National Centers of Academic Excellence in Information Assurance Education (CAEIAE)". Many of these centers are now following the National Initiative for Cybersecurity Education (NICE) framework, guaranteeing even more alignment with the security standards needed by government and industry.[48]

4.6. Protection privacy and civil liberties

There is a strong commitment to privacy and civil liberties in cyber activities in the USA. Privacy and civil liberties protections are an integral part in all strategies, both civil and

[43] https://www.congress.gov/bill/113th-congress/senate-bill/2519
[44] https://www.congress.gov/bill/113th-congress/house-bill/2952/
[45] https://www.congress.gov/bill/113th-congress/senate-bill/1353
[46] https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative
[47] http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf
[48] http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace

military. Privacy and civil liberty is an important part of every executive order, every law, and public address related to cyber security.

The National Strategy for Trusted Identities in Cyberspace[49] (NSTIC) is a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of online transactions. The NSTIC Vision is that individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. A user-centric "Identity Ecosystem," is an online environment where individuals and organizations are able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities—and the digital identities of devices.

The Strategy specifies four Guiding Principles to which the Identity Ecosystem must adhere:

- Identity solutions will be privacy-enhancing and voluntary
- Identity solutions will be secure and resilient
- Identity solutions will be interoperable
- Identity solutions will be cost-effective and easy to use

According to the NSTIC the Identity-ecosystem will improve privacy with[50]:

- Standards
- Individual control
- Limited data access
- De-centralized
- Fewer PII (personal identifiable information) targets

The Identity Ecosystem will consist of different online communities that use interoperable technology, processes, and policies. These will be developed over time—but always with a baseline of privacy, interoperability, and security

5. National Cyber Security: Canada

5.1. National Government and cyber security

The Canadian Government is committed to keeping Canadians safe in cyberspace through partnerships with other governments and industry to ensure the resilience of cyber systems vital to Canadian security and economic prosperity.[51]

In 2010, the Government of Canada released a comprehensive set of strategies and action plans on IT security and critical infrastructure. The Canadian government sees collaboration, especially internationally, as an essential part of securing cyberspace. In their work on the national strategy, they sought input from stakeholders on a wide range of cyber threats and security practices.

Public Safety Canada (PSC) is responsible for implementing Canada's cyber security strategy.[52] PSC provides central coordination for assessing emerging complex threats and developing and promoting comprehensive and coordinated approaches to address risks[53].

[49] http://www.nist.gov/nstic/about-nstic.html
[50] http://www.nist.gov/nstic/privacy.html
[51] http://news.gc.ca/web/article-en.do?nid=912329
[52] http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-eng.aspx
[53] http://jmss.journalhosting.ucalgary.ca/jmss/index.php/jmss/article/viewFile/458/454

Communications Security Establishment Canada (CSE) is one of Canada's key security and intelligence organizations. Their mandate states that the CSEC is: *to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructure of importance to the Government of Canada*[54]. CSEC's technical knowledge and capacity to fulfill this mandate is assisted by the fact that they are also mandated: *"to acquire and use information from the global information infrastructure (GII) for the purposes of providing foreign intelligence, in accordance with Government of Canada intelligence priorities.*[55]*"* It is noteworthy that the scope of CSEC's mandate is not limited to military networks or even government networks. It has the legislative authority to protect/defend any information or information infrastructures of importance to the Government of Canada[56].

The main body responsible for overall situational awareness and identification of cyber vulnerabilities seems to be the Canadian Security Intelligence Service (CIS). They investigate threats against critical information systems and infrastructure posed by foreign countries, terrorists, and hackers.[57]

In support of the National Strategy for Critical Infrastructure and Canada's Cyber Security Strategy, the Canadian Security Telecommunications Advisory Committee (CSTAC) was established in November 2010. CSTAC allows the private and public sectors to exchange information and collaborate strategically on current and evolving issues that may affect the telecommunications infrastructure, including cyber security threats. It was the first of the National Cross-Sector Fora intended to promote collaboration across the sector networks, address interdependencies and promote information sharing across sectors[58].

5.2. National Cyber Security Strategy and Policy

The main objectives of the 2010 Canadian cyber security strategy are to protect government networks, securing systems outside of government through cooperation and strengthened partnerships, as well as ensuring online safety for Canadians.[59]

5.2.1. Purpose and actions of the national strategy[60]

- *Reflects Canadian values such as the rule of law, accountability and privacy;*
- *Allows continual improvements to be made to meet emerging threats;*
- *Integrates activity across the Government of Canada;*
- *Emphasizes partnerships with Canadians, provinces, territories, business and academe; and*
- *Builds upon our close working relationships with our allies.*

The cyber security strategy is complemented by the 2010-2015 Action Plan for Canada's cyber security. As part of the Action Plan, the Government launched Shared Services Canada in 2011 – a streamlining of federal IT communications. The mandates of Communications Security Establishment Canada and the Canadian Cyber Incident Response Centre were clarified to strengthen their ability to detect, prevent and mitigate cyber

[54] http://laws-lois.justice.gc.ca/eng/acts/N-5/
[55] http://jmss.journalhosting.ucalgary.ca/jmss/index.php/jmss/article/viewFile/458/454
[56] http://jmss.journalhosting.ucalgary.ca/jmss/index.php/jmss/article/viewFile/458/454
[57] https://www.csis.gc.ca/index-en.php
[58] http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf10727.html
[59] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx
[60] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

security incidents. The Government also launched GetCyberSafe, a national public awareness campaign and website with up to date information on threats and safe cyber practices.[61] The public may also report cyber security incidents on the Public Safety Canada homepage.[62]

Acknowledging the importance of the shared digital critical infrastructure, Canada and the United States signed a Cyber Security Action Plan in 2012 to further enhance cooperation.[63] In the same year, Public Safety Canada formed a new coalition with private sector companies, non-profit and Government organisations (including U.S. DHS).
Concerning critical infrastructure, the cyber security strategy must be seen in conjunction with the National strategy for critical infrastructure, also launched in 2010, and the renewed Action Plan for 2014-2017.[64] One of the goals in the Action Plan is to sponsor security clearances among private stakeholders, recognizing the need for sharing sensitive information. Furthermore, a strategy for engaging CEOs of critical infrastructure is ongoing.

5.3. Incident Response

As part of the Action Plan, Canada has developed a national incident management framework.[65] At the outset, every organization is responsible for its own internal cyber security.

There are several federal departments involved in providing support in response to cyber security incidents. The first point of contact will in most cases be the Canadian Cyber Incident Response Centre (CCIRC), part of Public Safety Canada and the national coordination centre for preparedness, prevention, mitigation and recovery related to cyber incidents. CCIRC also decides whether the incident handling needs further escalation. CCIRC works closely with federal agencies, provinces and territories, critical infrastructure owners and others in the private sector, as well as with international partners.

The Government Operations Centre takes the lead on handling significant cyber security incidents that result in physical consequences.

The Royal Mounted Police leads the criminal investigation of cyber security incidents. It also has a supporting role in providing guidance and advice on cybercrime threats.[66] The Canadian Security Intelligence Service investigates incidents concerning national security.

The Canadian Anti-Fraud Centre is the national resource centre relating to fraud, and assists in prevention through awareness, disrupting criminal activities and strengthening public-private partnerships.[67]

5.4. Regulatory framework

The Canadian Radio-television and Telecommunications Commission is responsible for ensuring access to communications systems as well as contributing to a more secure online environment. This includes powers and duties vested in the Commission by any special Act

[61] http://www.getcybersafe.gc.ca/
[62] http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/rprt-eng.aspx
[63] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-eng.aspx
[64] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx and
http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/index-eng.aspx
[65] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-eng.aspx
[66] http://www.rcmp-grc.gc.ca/index-eng.htm
[67] http://www.antifraudcentre-centreantifraude.ca/english/index.html

(further defined in that Act), and by *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*.[68] The Canadian Radio-television and Telecommunications Act has a scheme for verifying compliance, as well as a civil liability and penalty scheme.[69]

Canada recognizes international certification schemes for information security.

The Office of the Privacy Commissioner of Canada oversees compliance with both the Privacy Act, concerning the handling of personal information by federal organizations, and the Personal Information Protection and Electronic Documents Act, which is the federal private sector privacy law.[70]

5.5. Knowledge, Research and Education

According to the Action Plan, Defence Research and Development Canada and Public Safety Canada are committed to promoting cyber security research and development. Among other elements, this includes providing funds to the innovation system, including academic institutions, and commissioning research papers on cyber security. Classified research and development on cyber security is the responsibility of the Communications Security Establishment Canada (CSEC).[71] The Canadian Security Intelligence Service is also dedicated to fostering a clear understanding of cyber security issues, by supporting or hosting activities such as conferences, seminars, papers etc., through their Academic Outreach Program. This program aims to tap into networks of experts from various fields, such as universities, think-tanks, NGOs etc.[72]

5.6. Protection of privacy and civil liberties

In Canada, the Access to Information Act allows citizens to demand records from federal bodies. This is enforced by the Information Commissioner of Canada[73].

There is also a complementary Privacy Act. The acts purpose is to extend the present laws of Canada that protect the privacy of individuals, with respect to personal information about themselves held by a federal government institution and that provide individuals with a right of access to that information.[74]

Each province and territory in Canada has its own access to information legislation.

- *Freedom of Information and Protection of Privacy Act (Alberta)*
- *Freedom of Information and Protection of Privacy Act (Manitoba)*
- *Freedom of Information and Protection of Privacy Act (Nova Scotia)*
- *Freedom of Information and Protection of Privacy Act (Ontario)*
- *Freedom of Information and Protection of Privacy Act (Saskatchewan)*
- *Act respecting access to documents held by public bodies and the protection of personal information (Quebec)*

68 http://laws.justice.gc.ca/eng/acts/C-22/page-4.html#h-10
69 http://laws.justice.gc.ca/eng/acts/T-3.4/page-27.html#docCont
70 https://www.priv.gc.ca/index_e.asp
71 https://www.cse-cst.gc.ca/en
72 https://www.csis.gc.ca/bts/cdmctrch-en.php
73 http://laws-lois.justice.gc.ca/eng/acts/a-1/
74 http://laws-lois.justice.gc.ca/eng/acts/p-21/

Through the Federal Accountability Act and Action Plan, the Government of Canada brought forward specific measures to help strengthen accountability and increase transparency and oversight in government operations. [75]

6. National Cyber Security: Germany[76]

6.1. National Government and Cyber Security

Cybersecurity has been highly emphasized by the German government. Germany has a comprehensive cybersecurity strategy and complemented by a strong legal framework. Germany also has a network of computer emergency response teams (CERTs), with the national CERT, CERT-BUND, working closely with both state-level and non-governmental CERTs. Furthermore, the country has well-developed public-private partnerships, such as the Alliance for Cyber-Security and the UP KRITIS partnership, and its national policies and legal framework reflect this focus on cooperation.[77]

The Federal Ministry of the Interior[78] (BMI) oversees the activity of the Federal Office for Information Security (BSI), which is the national competent authority on IT security[79].

The BSI, created in 2007, is tasked with promoting the security of information technology and is the central reporting office on IT security. BSI tasks include preventing security threats to federal information technology, gathering and studying information on security risks, developing criteria, procedures and tools to test and evaluate IT systems (including those used for transmission of official confidential information). Furthermore, the BSI provides support and advice on organizational and technical security measures. The BSI also provides support to the police and prosecution authorities, and the federal intelligence service. Federal authorities are required to IT security incidents to the BSI upon detection. Every two years, seemingly, the BSI produces a comprehensive report on the state of IT security in Germany.[80]

6.2. National Cyber Security Strategy and Policy

The National Plan for Information Infrastructure Protection (NPSI) is Germany's umbrella strategy for IT security, and was adopted in 2005[81]. The latest National Cyber Security Strategy was adopted on 23 February 2011[82]. This strategy called for the establishment of the National Cyber Response Centre and the National Cyber Security Council. Further elaboration on IT security measures can be found in "Digital Agenda 2014 -2017"[83].

6.2.1. National policy for cyber security

Within the 10 strategic points in the National Cyber Security Strategy, the main priority is the protection of critical infrastructure. State authorities are to serve as a role model in IT security. The strategy foresees the creation of a federal network, a uniform and secure infrastructure for the federal administration. In accordance with this strategy the Federal Ministry of Economics and Technology has set up a task force on "IT security in the industry" to support small and medium sized businesses, aiming to ensure appropriate and consistent information. The strategy emphasizes the need for joint initiatives with

75 http://www.tbs-sct.gc.ca/faa-lfi/index-eng.asp
76 This chapter has been reviewed by the German Federal Ministry of the Interior.
77 http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf
78 http://www.bmi.bund.de/EN/Topics/IT-Internet-Policy/IT-Cybersecurity/it-cybersecurity_node.html
79 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile
80 https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html
81 http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2009/kritis.html
82 http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile
83 http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2014/digital-agenda.pdf?__blob=publicationFile

participation by the industry. To optimize operational cooperation, the strategy calls for establishing a National Cyber Response Centre, which also should take the interests of the private sector into account. Focusing on preventive measures and early warning, it submits recommendations to the National Cyber Security Council and reports to the BSI. The National Cyber Security Council is foreseen to maintain cooperation within the Federal Government and with the public. As an initiative on a federal level, business representatives are invited to participate as associate members.

6.2.2. Purpose and actions of the national strategy

The goal of the National Cyber Security Strategy is to maintain and promote economic and social prosperity in Germany. As concerns IT security, the "Digital Agenda 2014-2017" emphasizes the state responsibility in protecting the public in the digital age. Germany intends to make the industry and businesses more accountable for offering trustworthy hardware, software and service to safeguard the online security of their users. Another element in this is to adopt the encryption of private communication as the new standard.

The Digital Agenda is the Federal Government's strategy for guiding and advancing digitization in government, society and the economy. Secure information technology is crucial for every form of digitization and is thus central to the Digital Agenda.

Within the Digital Agenda, a key project of the Federal Ministry of the Interior is the proposed IT Security Act. The draft of the Act goes beyond the minimum requirements for IT security of critical infrastructures and the obligation to report significant incidents defined in the Coalition Agreement to address the security of systems and public protection in general. The Federal Government wants Germany's IT systems and digital infrastructure to be the most secure in the world.

The IT Security Act starts with the relationship between risk, protection and responsibility. Anyone who creates risks for others by using IT should also be responsible for protecting against these risks. Further, the more serious these risks are, the higher the standards for the necessary protection should be. Although IT security increasingly needs to be seen in a global context, it is based on decisive national action.

With this in mind, the bill covers the following areas:

1. Improving the IT security of businesses:
   This includes above all minimum standards for the IT security of critical infrastructures and the requirement to report significant IT security incidents, as formulated in the Coalition Agreement of the governing parties, the CDU/CSU and SPD.

2. Protecting individual users within a secure network:
   This includes raising security standards for public telecommunications networks and providers of telemedia services, and requiring telecommunications providers to inform their customers about cyber attacks and how to respond to them.

3. Strengthening the BSI:
   The bill responds to the growing role of the BSI by more clearly formulating its authority to issue warnings and by establishing it as an international point of contact.

4. Expanding the responsibilities of the Federal Criminal Police Office (BKA):
   The BKA's existing responsibility for law enforcement tasks will be expanded in the field of cybercrime. Particularly in the case of attacks on nation-wide structures, the division of responsibilities needs to be clearly defined.

6.3. Incident Response

Numerous authorities are co-operating on a national and international level in order to counter the threat posed by cyber attacks. For better co-ordination of this co-operation, the Nationales Cyber-Abwehrzentrum (National Cyber Response Centre) has been established in Germany. It began its work in April 2011 and aims at optimizing the co-operation of state authorities e.g. through the co-ordination of protective and response measures taken against IT incidents.[84]

The National Cyber Response Centre is a cooperation between the Federal Office of Information Security (*Bundesamt für Sicherheit in der Informationstechnik*), the domestic intelligence service (*Bundesamt für Verfassungsschutz*), the Federal Office of Civil Protection and Disaster Assistance (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe*), the Federal Police (*Bundeskriminalamt* and *Bundespolizei*), the Customs Service within the Federal Ministry of Finance (*Zollkriminalamt*), the Foreign Intelligence Service (the *Bundesnachrichtendienst*), and the Federal Armed Forces (*Bundeswehr*).[85]

All agencies merge their information and analyses within the National Cyber Response Centre. Hence, the BSI offers analysis on the technical aspects of a cyber incident, while the BfV and BND offers threat intelligence, and the BBK analyses the impact on critical national infrastructure. All agencies insert their findings on threats and vulnerabilities, thus enabling a swift and comprehensive response to an incident.[86]

CERT-Bund[87] (The Federal Computer Emergency Response Team) is the central point of contact regarding IT-security related incidents. CERT-Bund is part of BSI and focuses on both preventive and reactive measures, among which publishing recommendations, proposing mitigation measures, monitoring the constituency and vulnerability awareness are included. Primarily available to the federal authorities, CERT-Bund's services include 24-7 on call duty, a warning and information service, as well as support during IT-security incidents. CERT-Bund also runs the national IT Situation Centre.

Following the "National Plan for Information Infrastructure Protection", (NPSI), *The IT Situation Centre*[88] serves federal agencies, critical infrastructure operators and partners by monitoring government and partner networks, analysing the current IT situation, and assessing the need for mitigation at state level as well as within the private sector. The Centre has a specialist reachable 24/7. Beyond the strategic goals of prevention, response and sustainability, the goal of the Centre is to react effectively to IT security incidents.

Similarly, the *IT Crisis Reaction Centre*[89] was also established under the NPSI and is tasked with resolving disruptions to the information infrastructure. It ensures immediate response to serious incidents in order to avoid large-scale damage.

[84] http://www.verfassungsschutz.de/en/fields-of-work/cyber-attacks
[85] http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/cyberabwehrzentrum_node.html
[86] http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/cyberabwehrzentrum_node.html (unofficial translation)
[87] https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/Cert-Bund/cert-bund_node.html
[88] https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/IT-Situation-Centre/itsituationcentre_node.html
[89] https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/IT-Crisis-Reaction-Centre/itcrisisreactioncentre_node.html

6.4. Regulatory framework

The BSI Act is the legal basis for and regulates the activities of the BSI.[90]

The telecommunications sector is regulated by the Telecommunications Act, overseen by the Federal Network Authority within the Ministry of Economics.[91] Protection of personal data, i.e. privacy, is regulated by the Federal Data Protection Act and Teleservices Data Protection Act, with the Federal Commissioner on Data Protection as regulatory authority.[92] Parts of the German Criminal Code concern the definition and classification of data.[93] The "Digital Agenda 2014-2017" announces adaptation of German criminal law to the digital age, in particular regarding the handling of stolen data. Furthermore, it announces the adoption of a General Data Protection Regulation by 2015.

In order to provide the necessary framework for the preventive approach anchored in the Digital Agenda, the Federal Ministry of the Interior on 19 August 2014 forwarded its draft bill to the other federal ministries involved for further consultation.
The bill includes provisions to achieve the following:

- Improving IT security in businesses, in particular critical infrastructures;
- protecting individual IT users with a secure network;
- protecting the IT of the Federal Government and federal agencies;
- strengthening the Federal Office for Information Security (BSI);
- expanding the investigative authority of the Federal Criminal Police Office in the field of cybercrime.[94]

6.5. Knowledge, Research and Education

The National Strategy contains little information on education related to IT security. The Digital Agenda 2014-2017 states that, together with relevant stakeholders, the Federal Government will develop a digital learning strategy.

In recent years, research funding by the Federal Ministry of Education and Research (BMBF) to protect IT infrastructures and systems has helped to make Germany one of the leading nations in the area of IT security. In order to secure and enhance Germany's position, the BMBF, as the German Ministry responsible for this area, has established research into innovative approaches to IT security as a priority task. This long-term research funded program focuses on strengthening Germany's position as an industrial location and protecting the data and privacy of its citizens.[95]

6.6. Protection of privacy and civil liberties[96]

The German Federal Data Protection Act has separate provisions for data processing in the public and private sectors. Germany also has special privacy provisions for electronic information and communication services (telemedia) and yet another set of privacy rules for the providers of services that transmit electronic signals. All these laws apply to some extent to the providers of online services.

Through these laws, Germany transposed European Union (EU) Directives 95/46 and 2002/58. In keeping with the Directives, Germany generally prohibits the collection and

[90] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile
[91] http://www.iuscomp.org/gla/statutes/TKG.htm and http://www.bundesnetzagentur.de/EN/Home/home_node.html
[92] http://www.iuscomp.org/gla/statutes/BDSG.htm and http://www.iuscomp.org/gla/statutes/TDDSG.htm
[93] http://www.gesetze-im-internet.de/englisch_stgb/ section 93 onwards and http://www.gesetze-im-internet.de/bundesrecht/s_g/gesamt.pdf for related security practices.
[94] http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/EN/2014/08/it-security-bill.html
[95] http://www.bmbf.de/en/73.php?hilite=cybersecurity
[96] http://www.loc.gov/law/help/online-privacy-law/germany.php

use of personal data unless the law specifically permits this or the data subject has given his or her informed consent. German law also follows the Directives on issues relating to rights and remedies of data subjects, security requirements, restrictions on location data, minimization of data, and safeguards against transmitting personal data to third countries with lesser standards of protection. The German provisions, however, often call for the balancing of competing interests and the application of the principle of proportionality. These provisions have resulted in an extensive and varied case law.

In Germany, data protection has constitutional dimensions that flow from the guarantees of human dignity and personhood. From these, the Federal Constitutional Court (FCC) crafted the right of informational self-determination that permits the processing of personal data only if authorized by statue or by consent of the data subject. In 2008, the FCC expanded these principles by articulating a constitutional guarantee of the confidentiality and integrity of IT systems. In 2010, the FCC struck down a German law transposition of the EU Data Retention Directive, for violating the principle of proportionality and the individual's rights of personhood.

Germany has a Federal Data Protection Agency and sixteen state data protection agencies. These often act in concert when making recommendations on how the consumer may navigate safely through the Internet. In addition, German experts often discuss the data protection problems that arise from the widespread collection of data by search engines and social media, and the use of these data to profile the data subject for commercial purposes. Although German law prohibits these practices unless informed consent has been given and although German law applies to any collection of data on German soil, Germany cannot enforce these laws against global players.

7. National Cyber Security: United Kingdom

7.1. National Government and Cyber Security

Cyber security is high on the agenda of the UK government. The National Security Strategy categorizes cyber-attacks as a Tier 1 threat to national security, alongside international terrorism[97]. In response to this, the UK launched its National Cyber Security Strategy in November 2011.

The responsibility for cyber security lies across several parts of the UK government. The Office for Cyber Security and Information Assurance (OCSIA) sits in the Cabinet Office as part of the National Security Secretariat (NSS), and is responsible for the Cyber Security Strategy and there delivery of the National Cyber Security Program (NCSP); the mechanism through which the Cyber Security Strategy is delivered.

Within the Cabinet Office, the Chancellor of the Duchy of Lancaster, supported by the Minister for Cabinet Office has ultimate responsibility for the Cyber Security Strategy and for the delivery of the National Cyber Security Programme. OCSIA provides strategic direction on cyber security, coordinating the program across government, enhancing cyber security and information assurance in the UK[98].

The CESG[99] is the information security arm of the Government Communications Headquarters (GCHQ) and the UK's national technical authority for information assurance. It advises government and public organizations in helping them to maintain network integrity and strengthen cybersecurity.

[97] https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty
[98] https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance
[99] www.cesg.gov.uk

The Centre for the Protection of National Infrastructure[100] (CPNI) is the UK government authority that provides security advice to help protect critical infrastructure against national security threats. CPNI's work contributes to the UK government's counter terrorism strategy (CONTEST) and its cyber security strategy. CPNI facilitates public-private information exchanges that enable vulnerabilities and mitigating measures. Current information exchanges include the Network Security Information Exchange (NSIE). The UK has many computer emergency response teams (CERTs) in both public and private sector. CERT-UK[101] is the UKs national CERT and supports UK industry, prioritizing operators. CERT-UK also engages with private sector CERTs and international counterparts. GovCertUK[102] supports government agencies in dealing with cyber security incidents

7.2. National Cyber Security Strategy and Policy

The United Kingdom's cybersecurity strategy was published in 2011. In order to secure the vast economic and social benefits that cyberspace offers, the UK government laid out that they sought to transform their approach to cyber security threw the national cyber security strategy.

The strategy includes a strong statement of principles and an assessment of cybersecurity threats faced by the UK. The implementation plan contained within the strategy is based around key-targeted objectives:

- Objective 1: The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace
- Objective 2: The UK to be more resilient to cyber-attacks and better able to protect our interests in cyberspace
- Objective 3: The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies
- Objective 4: The UK to have the crosscutting knowledge, skills and capability it needs to underpin all our cyber security objectives

7.2.1. National policy for cyber security

The principles of the UK government in approaching the field of cyber security is laid out in the national strategy: It is a risk-based approach, where the actors are working in partnership because the government cannot act alone and must recognize the limits of its competence in cyberspace. It also stress the importance of balancing security with freedom and privacy: *"Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society"*[103].

"That means a UK where:

- *Individuals know how to protect themselves from crime online.*
- *Businesses are aware of the threats they face, their own vulnerabilities and are working with Government, trade associations, and business partners to tackle them. We want to see UK companies building on our strengths to create a thriving and vibrant market in cyber security services around the world. In the current economic climate, the UK needs more than ever to identify and exploit areas of international competitive strength to drive growth. We believe that being able to show the UK is a safe place to do business in cyberspace can be one such strength.*

[100] http://www.cpni.gov.uk/
[101] https://www.cert.gov.uk/
[102] http://www.cesg.gov.uk/policyguidance/GovCertUK/Pages/index.aspx
[103] https://www.gov.uk/government/publications/cyber-security-strategy

- *Government has: sharpened the law enforcement response to cybercrime; helped the UK take opportunities to provide the cyber security services that will be needed across the world; encouraged business to operate securely in cyberspace; bolstered defences in our critical national infrastructure against cyber attack; strengthened our capabilities to detect and defeat attacks in cyberspace; enhanced education and skills; and established and strengthened working relationships with other countries, business and organisations around the world to help shape an open and vibrant cyberspace that supports strong societies here and across the globe."* [104]

To achieve this the UK set aside £860 million over five years to deliver the strategy under a National Cyber Security Programme (NCSP).

The United Kingdom also has a well-developed system of public-private partnerships in which the private sector actively participates. This collaborative approach also is strongly supported by its cyber security strategy[105].

7.2.2. Progress and future plans

The work against reaching the objectives set forth in the national cyber security strategy is supported by the National Cyber Security Program (NCSP), which with dedicated funding of £860 million over five years has supported a wide range of projects to develop cyber security capabilities and stimulate the UK"s cyber security market. The following projects is potentially of particular interest[106]:

- Government has been working to raise businesses' awareness of the threat from cybercrime and espionage and encourage firms to embed effective cyber security risk management practices. As a part of this work, they have published its '10 Steps to Cyber Security' guidance for business. A Cyber Security Governance Health Check has backed use of these steps. The Health Check assesses how the boards of top UK companies are managing cyber risks and enables them to benchmark themselves against their peers and competitors.

- To help business gauge the potential impact of cyber attacks BIS publishes the annual Information Security Breaches Survey to assess the level of information security breaches affecting UK businesses and raise awareness of the need for industry to take action.

- GCHQ has certified firms working in Cyber Incident Response, and has been enabling industry to deliver a broader supply of assured cyber security products to defend against cyber attack through Commercial Product Assurance (CPA).

- To facilitate information-sharing between firms the UK Government in March 2013 launched the Cyber Security Information Sharing Partnership (CISP). CISP provides a platform for companies to share cyber threat information in real time. A fusion cell (composed of industry and government network defence analysts) examines the data and provides enriched information and advice to the CISP community. CERT-UK, working with police Regional Organised Crime Units (ROCUs), has also begun a nationwide initiative to introduce Regional Cyber Information Sharing Partnerships (CISP fora). These aim to promote the sharing of cyber security information regionally to help local businesses to protect themselves from cybercrime.

[104] https://www.gov.uk/government/publications/cyber-security-strategy
[105] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_unitedkingdom.pdf
[106]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf

- In June 2014 GCHQ, BIS and Cabinet Office launched Cyber Essentials, a major new Government-backed and industry-supported scheme to incentivize widespread adoption of basic security controls that will help to protect organizations against the commonest kind of internet attacks. The scheme is constructed to be affordable and practical for all firms, small as well as large. Certification comes with a badge which firms can use to help demonstrate their security credentials to customers and investors, and which insurers can take into account when considering firms for relevant insurance policies.

- For higher education, the Government is working with academia, professional bodies, trade associations and industry to define a framework for the required learning outcomes in cyber security within computing science and related courses. From next year, cyber security will be a mandatory subject of study in all undergraduate courses accredited by the British Computer Society and the Institution of Engineering & Technology.

7.3. Incident Response

CERT-UK was established in 2014 in response to the National Cyber Security Strategy [107]. It is responsible for promoting cyber security situational awareness and for national cybersecurity incident management including providing support for entities engaged with national critical infrastructure.

CERT-UK is tasked with incident reporting and collecting information about cybersecurity incidents. It provides an online reporting structure to log cybersecurity incidents. CERT-UK acts according to the Cyber Security National Incident Management policy, which includes reporting and notification requirements[108].

CERT-UK works closely with GovCertUK, which is responsible for coordinating security and incident response measures for UK government institutions[109].

CERT-UK hosts a secure online information sharing platform – known as the CiSP; the Cyber Security Information Partnership for companies and government to exchange information about cyber attacks, threats and good practice.
The Council for Registered Ethical Security Testers (CREST) has introduced an incident response scheme based on company assessment and professional qualifications, which has been endorsed by GCHQ and CPNI. The scheme focuses on appropriate standards for incident response aligned to demand from all sectors of industry, the wider public sector and academia. Companies included in this scheme have demonstrated that they have effective policies, processes and procedures in place to help organisations plan for, manage and recover from significant cyber security related incidents. These companies will also have access to professionally qualified staff in intrusion analysis and reverse engineering. [110] CESG have a more formal scheme of certification for 'Cyber Incident Response' companies deemed capable of responding to incidents arising from advanced persistent threats.

[107] https://www.cert.gov.uk/what-we-do/
[108] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_unitedkingdom.pdf
[109] http://www.cesg.gov.uk/policyguidance/GovCertUK/Pages/index.aspx
[110] http://www.crest-approved.org/why-use-crest/index.html

7.4. Regulatory framework

There is no overarching regulation of cyber security in the UK, although a growing number of organisations are complying with voluntary standards.[111]

The Communications Electronic Security Group (CESG)[112], the information security arm of the Government Communications Headquarters (GCHQ), has published guidelines for public organizations related to information security.

The Government Security Classifications Policy[113], which came into force in 2014, details a three-tiered system of classification for information that is required by domestic laws, including the Official Secrets Act 1989[114], to be classified. The three classification levels are assigned according to the sensitivity of the information and the risk level involved in disclosing the information. The classification levels are assigned with consideration of the level risk involved in disclosing the information. The policy then maps specific security requirements according to classification level[115].

The UK generally recognizes international certification schemes, although some additional voluntary guidance on security standards is provided by the UK's National Technical Authority on Information Assurance. In June 2014, the government issued a new cybersecurity standard known as the Cyber Essentials Scheme[116]. From 1 October 2014, the UK government will require all suppliers bidding sensitive and personal information handling contracts to be certified against the Cyber Essentials Scheme. The scheme includes some overlaps with, but also some differences to, international standards

The UK Cyber Security Strategy acknowledges the ease and benefits of continuous monitoring of data with relation to digitization, however, a specific auditing process and the frequency with which it should be carried out is not detailed[117].

There is no legislation or policy in place in the United Kingdom that requires mandatory reporting of cybersecurity incidents, however, voluntary guidelines issued by both CERT-UK and GovCertUK recommend the reporting of all incidents[118].

7.5. Knowledge, Research and Education

The UK Cyber Security Strategy includes a plan to "look at the best ways to improve cybersecurity education at all levels so that people are better equipped to use cyberspace safely». There is also a commitment to "building a culture that understands the risks and enables people to use cyberspace and improving cybersecurity skills at all levels".
In practice, the UK has developed some of the most advanced cybersecurity education initiatives in the region, including the Get Safe Online program[119].

[111] http://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf
[112] http://www.cesg.gov.uk/Pages/homepage.aspx
[113]https://www.gov.uk/government/publications/government-security-classifications
[114] http://www.legislation.gov.uk/ukpga/1989/6
[115] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_unitedkingdom.pdf
[116] www.gov.uk/government/publications/cyber-essentialsscheme-overview
[117] https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty
[118] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_unitedkingdom.pdf
[119] www.getsafeonline.org

The work om cyber security knowledge, skills and capability made in 2014[120]:

Schools	Learning and teaching materials at GCSE and A-level, new Key Stage 3 (age 11-14) materials to be released in 2015; now interventions at every level of the education system
Training and apprenticeships	250 new entry-level cyber security jobs through the Tech Partnership and employers, to add to 140+ GCHQ apprentices, plus a Cyber Intrusion Analyst Trailblazer Apprenticeship in 2015
Higher Education	4 development fund grants to colleges and universities given via Higher Education Academy, a mentoring scheme and "Cyber Camps" for graduates and undergraduates
Postgraduates	GCHQ has certified six „Master"s degrees in General Cyber Security", plus 2 Centres of Doctoral Training to deliver 66 additional PhDs from 2017 on top of GCHQ"s PhD programme
Wider educational support	Open University developed Massive Open Online Course „Introduction to Cyber Security" – nearly 24,127 sign ups to the first offering, and a new App from GCHQ on coding, „Cryptoy"
The Cyber Security Challenge	18,800 registered for the Masterclass competition; 800 schools participating in the Schools" competition; over 22,000 young people have used the learning resources

7.6. Protection of privacy and civil liberties

The Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights. ICO's role is to uphold information rights in the public interest. ICO covers the following legislation:

- Data Protection Act
- Freedom of Information Act
- Privacy and Electronic Communications Regulations
- Environmental Information Regulations
- INSPIRE Regulations

[120]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf

The Data Protection Act[121] controls how organizations, businesses or the government in the UK uses your personal information. Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the UK without adequate protection

There is stronger legal protection for more sensitive information, such as ethnic background, political opinions, religious beliefs, health, sexual health or criminal records.[122]

8. National Cyber Security: The Netherlands

8.1. National Government and Cyber Security

The Netherlands has a comprehensive approach to the field of cyber security. The national government's responsibilities in this area is made clear through the legal and policy framework for cybersecurity, which includes their second National Cyber Security Strategy of 2013. The Dutch government has a mature approach to the field of cybersecurity. The third cyber security strategy is expected in the second half of 2016.

In the national strategy, the government states that the Netherlands stands for safe and reliable ICT and the protection of the openness and freedom of the Internet. The Dutch government highly prioritizes public-private partnership in this area, which is clearly addressed through contributions from a broad range of public and private parties, knowledge institutes and social organizations in the second national strategy.

The Ministry of Security and Justice[123] is responsible for maintaining the rule of law in the Netherlands. The Ministry consists of different branches, each of which has its own duties.

The Public Prosecution Service (OM) is a part of the judiciary and the only body in the Netherlands that can prosecute in criminal cases, including cybercrime.

The National Coordinator for Counterterrorism and Security (NCTV) and his staff falls under the responsibility of the Minister of Security and Justice. The NCTV is the result of a merger between the former National Safety and Security Department, the National Coordinator for Counterterrorism (NCTb) and Directorate General for Security (part of the Ministry of Interior and Kingdom Relations) and the Government Computer Emergency Response Team (GOVCERT.NL).

The NCTV's Cyber Security Department (DCS) includes the National Cyber Security Centre (NCSC) - and a policy cluster. *The National Cyber Security Centre*[124] (NCSC) is a government initiative that opened 12 January 2012. Ensuring digital security is the task of

[121] http://www.legislation.gov.uk/ukpga/1998/29/contents
[122] https://www.gov.uk/data-protection/the-data-protection-act
[123] http://www.government.nl/ministries/venj
[124] https://www.ncsc.nl/english

various parties and the NCSC acts as the link, which binds together the many different activities. The centre has three main tasks: serving as the leading knowledge and expertise centre for cyber security, managing the Computer Emergency Response Team (CERT) and carrying out crisis coordination in the event of a cyber-incident.

Before NCSC, GOVCERT.NL was the government organization dedicated to cyber security and incident response. The tasks and employees of GOVCERT.NL have all been transferred to the center. The NCSC cooperates with partners in the Netherlands and abroad with the aim of continuing to expand knowledge and expertise so that possible threats can be identified and warded off.

8.2. National Cyber Security Strategy and Policy

The Netherlands' current National Cyber Security Strategy 2 (NCSS2) was adopted in 2013. This was the second Dutch cybersecurity strategy. The first strategy was released in 2011. The Dutch government is clear on the fact that cyber security is crucial for the proper functioning of society and the economy.

8.2.1. National policy for cyber security

In the national strategy of 2013, it is proposed that the correlation between security, freedom and social economic benefits is a dynamic balance that is intended to be realized in a constantly open and pragmatic dialogue between all stakeholders, both national and international. With this purpose, the Dutch government seeks to establish a clear governance model. "*The underlying fundamental principle is that the responsibilities that apply in the physical domain should also be taken in the digital domain"*[125].

Three management areas are of utmost importance, and have been included in the strategy: *(self) regulation, transparency and knowledge development*[126]. According to the strategy, the Dutch government seeks to play an active role in the digital domain by both increasing investments in the security of its own networks and services, and by bringing parties together and by taking action if the security of companies and private individuals or the latter's privacy come under threat. Frameworks and standards will also be established, where this is assessed to be necessary

8.2.2. Purpose and actions of the national strategy[127]

The purpose of the first strategy of 2011 was *"to realize a secure, reliable and resilient digital domain through an integral cyber security approach based on public-private partnerships, as well as to seize the ensuing opportunities for society"*. The second strategy is a revision based on the progress resulting from the first strategy, and the different priority areas that have emerged in the intervening year. It entails the government's broader vision on cyber security and states responsibilities. About 130 parties, including public and private parties, knowledge institutions and social organizations, were involved in the drafting of this new cyber security strategy. Furthermore, extensive consultations were held with the wider ICT community[128].

The NCSS2 contains a comprehensive assessment of the cyber threats faced by the Netherlands and the best practices to address them. The "action program" section of the strategy contains clear objectives and action items.[129]

[125] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_netherlands.pdf
[126] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_netherlands.pdf
[127] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_netherlands.pdf
[128] file:///C:/Users/cn2271/Downloads/national-cyber-security-strategy-2_tcm92-520278%20(1).pdf
[129] file:///C:/Users/cn2271/Downloads/national-cyber-security-strategy-2_tcm92-520278%20(1).pdf

Objectives of the 2014-2016 action program:

1. *The Netherlands is resilient to cyberattacks and protects its vital interests in the digital domain.*
2. *The Netherlands tackles cybercrime.*
3. *The Netherlands invests in secure ICT products and services that protect privacy.*
4. *The Netherlands builds coalitions for freedom, security and peace in the digital domain.*
5. *The Netherlands has sufficient cyber security knowledge and skills and invests in ICT innovation to attain cyber security objectives.*

They seek to achieve these objectives by focusing on the following central elements:

1. *Risk analyses, security requirements, information sharing within critical infrastructure*
2. *More active approach to cyber espionage*
3. *Feasibility study on separate vital network*
4. *Enhancing civil-military cooperation*
5. *Strengthening the National Cyber Security Centre*
6. *International approach to cybercrime: updating and strengthening legislation*
7. *Supported standards, 'security by design' and 'privacy by design'*
8. *Cyber diplomacy: hub for expertise for conflict prevention*
9. *Taskforce on cyber security education*
10. *Encouraging innovation in cyber security*

8.3. Incident Response

The National Cyber Security Center (NCSC) is the center for expertise on cyber security and incident response of the Dutch government in order to increase the Netherlands' digital resilience. It is aimed at preventing ICT and internet related incidents and coordinates response to these incidents[130].

The NCSC constitutes the central reporting and information point for IT threats and security incidents. With its establishment in 2012, the CERT function of the superseded GOVCERT.NL[131] was incorporated. NCSC is responsible for the coordination of incident response measures for the Dutch government institutions, as well as entities engaged with critical infrastructure.[132]

8.3.1. A brief summary of the goal of NCSC-NL[133]*:*

The NCSC cooperates in enhancing the resilience of the Netherlands in the digital domain. The goal is to realize a safe, open and stable information society by sharing knowledge, providing insight and proper perspective for action. The NCSC is national and international 'National Point of Contact' in case of cybersecurity incidents and ICT threats and is information hub and centre of expertise for cyber security. Their main tasks include:

- Response to incidents and threats
- Providing insight and perspective for action
- Strengthening crisis management
- Platform for cyber security cooperation.

[130] Operational Framework NCSC-NL: file:///C:/Users/cn2271/Downloads/Operational+Framework+NCSC-CSIRT+%252828-11-2011%2529.pdf
[131] GOVCERT.NL was established in 2002 as CERT-RO and operates to deal with computer security problems and their prevention, within its constituency. CERT-RO was renamed into GOVCERT.NL as of 01-02-2003.
[132] https://www.ncsc.nl/english/services/incident-response.html
[133] Operational Framework NCSC-NL: file:///C:/Users/cn2271/Downloads/Operational+Framework+NCSC-CSIRT+%252828-11-2011%2529.pdf

The primary target group of the NCSC is the Dutch central government and the vital infrastructure. Vital sectors are crucial for the proper functioning of Dutch society. Examples of vital sectors are energy, water and telecom.

8.3.2. NCSC-NL provides 4 basic services for the constituency[134]:

- I*ncident Prevention (e.g. security advisories, alerts, training, exercises, …)*
- *Incident Response (24x7 availability for incident reporting and coordination*
- *Monitoring (12x7 active watch, network monitoring, …)*
- *Knowledge Sharing (Best practices, factsheets, symposium, …) and advise*

NCSC-NL also works in a joint effort on veiliginternetten.nl, aimed at end-users in SMB and the public. The NCSC is tasked with liaising with the private sector in carrying out its duties. In addition to the NCSC, the Netherlands hosts two major public-private partnerships relevant to cybersecurity[135]:

- *ECP* is a public-private platform for promoting the use of information and communications technology in the Netherlands.
- *The National Continuity Forum (NCO-T*) is a public-private partnership between the government and suppliers of telecommunication networks.

8.4. Regulatory framework

The regulatory framework regarding government IT, in the field of information security is covered largely by *the Government Decision on Information Security — Special Information 2013[136], Baseline Informatiebeveiliging Rijksdienst (BIR),* along with the guidelines issued by the National Cyber Security Centre[137].

The policy letter Protecting Critical Infrastructure 2005 and the Third Progress Letter on National Security 2010 provide an assessment of the quality of the protection of Dutch critical infrastructure, and definitions for "critical infrastructure protection".[138]

The Government Decision on Information Security — Special Information 2013requires information important to the state, its ministries or its allies to be classified. The information is classified by a four-tiered classification system, as set out in the decision. The classification levels are assigned according to the level of risk involved in disclosing the classified information. It also requires information systems to go through periodic audits, however, they are not set to occur within a mandatory timeframe. [139].

The Cyber Security Assessment Netherlands (CSAN) is a government cybersecurity report published annually by the NSCS. However, it is not an audit of cybersecurity practices and procedures. The Netherlands recognizes international certification schemes for information security — and only has local accreditation requirements for organizations handling some specific Government classified material.[140].

The Netherlands is currently working on legislation that requires mandatory reporting of cybersecurity incidents. The Netherlands recognizes international certification schemes for

[134] Operational Framework NCSC-NL: file:///C:/Users/cn2271/Downloads/Operational+Framework+NCSC-CSIRT+%252828-11-2011%2529.pdf
[135] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_netherlands.pdf
[136] http://wetten.overheid.nl/BWBR0033507/geldigheidsdatum_29-04-2015
[137] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_netherlands.pdf
[138] http://www.government.nl/issues/crisis-national-security-and-terrorism/protecting-critical-infrastructure
[139] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_netherlands.pdf
[140] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_netherlands.pdf

information security, and only has local accreditation requirements for organizations handling some specific Government classified material[141].

The Dutch regulator for the telecommunications industry is the Authority for Consumers and Markets (ACM). The specific regulator for frequency matters and duty of care for providers is the Radio Communications Agency Netherlands (*Agentschap Telecom, AT*) and for privacy matters the specific regulator is the Dutch Data Protection Authority (*College Bescherming Persoonsgegevens, CPB*). Other sectorial duty of care and duty of notification is regulated through sectorial legislation. All operators are privately owned.

8.5. Knowledge, Research and Education

One of the five main objectives in the Dutch cybersecurity strategy, and its 2014-2016 action program, is sufficient cyber security knowledge and skills, along with investment in ICT innovation, to attain the cyber security objectives.

A strong commitment to cybersecurity education is built around the establishment of a task force on cybersecurity education. The objective of the task force is to: *"enlarge the pool of cyber security experts and enhance users' proficiency with cyber security, the business community and the government join forces to improve the quality and breadth of ICT education at all academic levels (primary, secondary and professional education)".*

Through the Taskforce, and the Netherlands Organization for Scientific Research, investment are made in education and research in the field of cyber security. The national strategy makes it clear that a multidisciplinary approach in which the non-technical sub-areas are also included is needed to promote cyber security innovation.[142]

Additionally the Dutch National Cyber Security Research Agenda (NCSRA) focusses on the 'Security and Trustworthiness of Infrastructure'. The objectives of the agenda are:

- To improve the security and trustworthiness of the ICT infrastructure and ICT services.
- To prepare the Netherlands for the security challenges of the next 6-12 years.
- To stimulate the Dutch security economy and promote innovation in this sector.

To strengthen and broaden Dutch security research by fostering cooperation between knowledge institutions and relevant public and private organizations.

In 2012, the NCSRA provided the context for two calls for research proposals (a call for long-term research and a call for short-term research). These calls for proposals were made available by four Dutch ministries and NWO (the Netherlands Organisation for Scientific Research). These calls were very successful and in 2013, six Dutch ministries and NWO announced two new calls for research proposals.

8.6. Protection privacy and civil liberties

The Personal Data Protection Act[143] broadly governs the protection of personal data. Online privacy is addressed in particular by the Telecommunications Act[144], which was recently amended to incorporate privacy provisions deemed by some commentators to be stricter than those of the EU.

[141] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_netherlands.pdf
[142] file:///C:/Users/cn2271/Downloads/national-cyber-security-strategy-2_tcm92-520278.pdf
[143] http://www.coe.int/t/dghl/standardsetting/dataprotection/national%20laws/NL_DP_LAW.pdf
[144] http://www.government.nl/documents-and-publications/notes/2012/06/07/dutch-telecommunications-act.html

The Netherlands has incorporated key European Union directives on privacy, such as the Directive on Personal Data, the Data Retention Directive, and the Privacy and Electronic Communications Directive, into its national law[145].

The processing of any personal data in the Netherlands requires the data subject's unambiguous consent; certain types of personal data, such as that concerning a person's religion may not be processed, however. Internet service providers have an obligation to protect the privacy of users and subscribers[146].

The Dutch Data Protection Authority is a key agency involved in the protection of personal data, but two other agencies play a role in supervising telecommunications service providers and the telecom market. Among possible future changes in the Dutch legal framework of online privacy is the adoption of a constitutional amendment on the protection of digital rights[147].

9. Nationell informations- och cybersäkerhet: Sverige[148]

9.1. Regering och offentlig förvaltning

Enligt den svenska ansvarsprincipen är alla myndigheter ansvariga för att upprätthålla en tillräcklig informations- och cybersäkerhet inom sin verksamhet. Förutom riksdag och regering som stiftar lagar och utfärdar förordningar på området finns flera myndigheter med ett särskilt formellt ansvar för informations- och cybersäkerhet i Sverige. Myndigheter med ett mer utpekat ansvar har formella uppdrag där det kan ingå tillsynsansvar, det vill säga utövande av kontroll över en verksamhet, samt föreskriftsrätt på området. De departement som har myndigheter under sig vilka fyller någon av funktionerna som nämnts ovan är Finansdepartementet, Försvarsdepartementet, Justitiedepartementet och Näringsdepartementet. Berörda myndigheterna och deras roller beskrivs nedan.

9.1.1. Statliga myndigheter

Myndigheten för samhällsskydd och beredskap (MSB),[149] ska stödja och samordna arbetet med samhällets informations- och cybersäkerhet, samt att analysera och bedöma omvärldsutvecklingen. I detta ingår att lämna råd och stöd om förebyggande arbete i offentlig och privat sektor. MSB har rätt att utfärda föreskrifter på området rörande statliga myndigheter.
MSB svarar också för den nationella CSIRT:n CERT-SE [150] vilken ska förebygga och hantera it-incidenter.

Datainspektionen (DI),[151] som är tillsynsmyndighet enligt personuppgiftslagen, har som en övergripande uppgift att arbeta för att behandlingen av personuppgifter inte medför otillbörligt intrång i enskildas personliga integritet och att reglerna för sådan behandling följs. Arbetet bedrivs både preventivt och åtgärdande.[152]

[145] http://www.loc.gov/law/help/online-privacy-law/netherlands.php
[146] http://www.loc.gov/law/help/online-privacy-law/netherlands.php
[147] http://www.loc.gov/law/help/online-privacy-law/netherlands.php
[148] Landomtalen er skrevet av Åke Holmgren, Myndigheten for Samhällsskydd och beredskap/Medlem av Lysneutvalget
[149] Myndigheten för samhällsskydd och beredskap: https://www.msb.se/en/?ResetTargetNavigation=true
[150] CERT-SE: https://www.cert.se/, mer information om denna funktion återfinns i avsnittet Incidenthantering.
[151] Datainspektionen: http://www.datainspektionen.se/in-english/
[152] Mer information om Datainspektionen och arbetet med skyddet av den personliga integriteten finns i det sista avsnittet - Skydd av personlig integritet och medborgliga rättigheter.

E-legitimationsnämnden[153] har i uppgift att stödja och samordna främst den offentliga sektorns behov av säkra metoder för elektronisk identifiering och signering.

Den svenska *Polismyndigheten*[154] arbetar med att förebygga och hantera it-relaterade brott.

Säkerhetspolisen (SÄPO)[155] har som en av huvuduppgifterna att förebygga, förhindra och upptäcka brottslighet som bland annat kan inkludera både cybersabotage och cyberspionage. Säpo har rätt att utfärda föreskrifter avseende tillämpningen av säkerhetsskyddslagen.

Post- och telestyrelsen (PTS)[156] bevakar området elektronisk kommunikation i Sverige, så som telekommunikationer, it och radio. En av målsättningarna är att säkerställa tillgång i hela landet till bra telefoni, bredband och post med det övergripande målet att kommunikation ska vara säker. PTS kan utfärda föreskrifter för teleoperatörernas verksamhet.

Försvarets radioanstalt (FRA)[157] står för en hög teknisk kompetens inom informations- och cybersäkerhetsområdet och stödjer statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig ur sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. FRA ska stödja insatser vid nationella kriser med it-inslag, medverka till identifieringen av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser och ge annat tekniskt stöd. FRA tilldelar civila myndigheter och samhällsviktiga företag av Försvarsmakten godkänd signalskyddsutrustning. FRA utfärdar inte några föreskrifter men ger stöd och råd avseende en rad olika tekniska informationssäkerhetsaspekter.

Försvarets materielverk (FMV)[158] med CSEC verkar som Sveriges nationella certifieringsorgan för it-säkerhet enligt Common Criteria, en standard som används för kravställning och opartisk granskning av IT-säkerhet. CSEC representerar även Sverige inom det internationella samarbetet CCRA för säkra it-produkter.

Försvarsmakten (FM)[159] leder signalskyddsverksamheten och arbetet med säkra kryptografiska funktioner och har bemyndigats att ge ut föreskrifter och instruktioner för statliga myndigheter inom detta område. Försvarsmaktens föreskrifter och allmänna råd för signalskyddstjänsten inom totalförsvaret syftar till att få ett väl fungerande signalskydd genom användningen av säkra kryptografiska funktioner och genom detta undvika långvariga och dolda skadeverkningar för rikets säkerhet och Sveriges krisberedskap.

Jämte de statliga myndigheterna bedrivs mycket av det för Sverige viktiga informations- och cybersäkerhetsarbete hos alla de privata aktörer som exempelvis tillhandahåller central infrastruktur eller andra samhällsviktiga funktioner.

[153] E-legitimationsnämnden:
http://www.elegnamnden.se/omoss/theswedisheidentificationboard.4.3aa8c78a1466c584587cfe.html
[154] Polisen: https://polisen.se/en/Languages/Startpage/, mer information om Polisens verksamhet återfinns i avsnittet Incidenthantering.
[155] Säkerhetspolisen: http://www.sakerhetspolisen.se/en/swedish-security-service.html
[156] Post- och telestyrelsen: http://www.pts.se/en-GB/
[157] Försvarets radioanstalt: http://www.fra.se/snabblankar/english.10.html
[158] Försvarets materielverk: http://www.fmv.se/en/
[159] Försvarsmakten: http://www.forsvarsmakten.se/en/

9.1.2. Samverkan

Ett utspritt ansvar för informations- och cybersäkerhet i Sverige i kombination med områdets komplexitet och gränsöverskridande karaktär kräver en effektiv samverkan. Därför finns det ett flertal samverkansforum där både statliga och regionala myndigheter, näringslivet samt intresseorganisationer ingår. Gemensamt för alla dessa olika samverkansforum är den centrala roll som MSB innehar.

Samverkansgruppen SAMFI[160] består av de centrala myndigheterna inom informations- och cybersäkerhetsområdet. SAMFI:s verksamhet fokuseras på genomförande av åtgärdsförslagen i den nationella handlingsplanen för samhällets informationssäkerhet.

SAMFI bör dessutom ha beredskap för att hantera frågeställningar inom huvudsakligen följande aktivitetsområden:

- Strategi och regelverk
- Tekniska frågor och standardiseringsfrågor
- Nationellt och internationell utveckling inom informationssäkerhetsområdet
- Informationsaktiviteter
- Övningar och utbildning
- Hantering och förebyggande av IT-incidenter

Säkerhetspolisen, Försvarsmakten/Must och FRA påbörjades i december 2012 samarbetet Nationell samverkan till skydd mot allvarliga IT-hot (NSIT). NSIT analyserar och bedömer hot och sårbarheter samt skyddsåtgärder när det gäller allvarliga eller kvalificerade it-hot mot de mest skyddsvärda nationella intressena. Syftet är att utveckla samverkan för att försvåra för en kvalificerad angripare att komma åt eller skada svenska skyddsvärda civila och militära resurser. MSB är sedan 2014 observatör i NSIT.

För utveckling av svensk informations- och cybersäkerhet på ett bredare plan finns det av MSB ledda Informationssäkerhetsrådet[161] där ett flertal centrala aktörer på området sammanträder 4 gånger per år. För informationsdelning om industriella styrsystem och finanssektorn finns grupperna Fidi SCADA, Fidi FINANS och Fidi Vård.

9.2. En nationell strategi för informations- och cybersäkerhet

9.2.1. NISU 2014 och utvecklingen av en strategi för svenska staten

Utveckling av en övergripande strategi för den svenska staten har gjorts i och med informationssäkerhetsutredningen NISU 2014.[162] Utredningen mynnade ut i ett förslag om en nationell strategi för statens informations- och cybersäkerhet med sex mål:

- att stärka styrning och tillsyn inom området,
- att staten ska ställa tydliga krav vid upphandling på it-området,
- att statliga myndigheter ska kommunicera säkert,
- att samtliga statliga myndigheter rapporterar it-incidenter,
- att arbetet med att förebygga och bekämpa it-relaterad brottslighet stärks och
- att Sverige ska vara en stark internationell partner.

Förslagen i strategin som uteredningen gav är begränsade till det statliga området och till utformning av författningsreglering på förordnings- och föreskriftsnivå.

[160] SAMFI med medlemmarna MSB, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Post- och telestyrelsen, Säkerhetspolisen samt Rikskriminalpolisen:
https://www.msb.se/sv/Forebyggande/Informationssakerhet/Informationssakerhet-i-samhallet/Samverkansgruppen-SAMFI/
[161] Informationssäkerhetsrådet: https://www.msb.se/sv/Forebyggande/Informationssakerhet/Informationssakerhet-i-samhallet/Informationssakerhetsradet/
[162] NISU 2014: http://www.sou.gov.se/wp-content/uploads/2015/03/SOU-2015_23_webb.pdf

9.2.2. Nationell handlingsplan samhällets informationssäkerhet

Handlingsplanen[163] som togs fram 2012 utgörs av ett trettiotal åtgärdsförslag arbeta inom fem strategiska områden:

- Informationssäkerhet i verksamheter,
- Kompetensförsörjning,
- Informationsdelning, samverkan och respons,
- Kommunikationssäkerhet,
- Säkerhet i produkter och system

Planen är framtagen av myndigheterna i samverkansgruppen SAMFI.

I planen framgår vilka områden som myndigheterna inom SAMFI anser vara särskilt viktiga att lyfta fram och vilka åtgärder som planeras för att höja säkerheten inom dessa områden. Den enskilda organisationen kan genom detta få ett stöd för hur det egna säkerhetsarbetet ska utformas.
Handlingsplanen ska ge väsentliga samhällsaktörer stöd för att förbättra sin informationssäkerhet. Bland dessa finns myndigheter, landsting och kommuner men även privata aktörer som levererar tjänster som är viktiga för att det svenska samhället ska fungera.

9.3. Incidenthantering

Som tidigare nämnt ligger ansvaret på varje enskild aktör att se till så att tillräcklig informations- och cybersäkerhet upprätthålls, så är det även när det kommer till det operativa hanterandet av incidenter. Det finns däremot centrala stödfunktioner för operativ incidenthantering.

Den svenska Polisen bedriver verksamhet på området i och med sin brottsutredande verksamhet, av dataintrång och datorbedrägeri, där bland annat it-forensik ingår. Polisen driver även ett projekt för att införa ett it-brottscentrum i den nya Polismyndigheten. Detta centrum blir bland annat kontaktpunkt till EC3 (European Cybercrime Centre)[164]. Säkerhetspolisen och FRA hanterar, inom sina uppdrag incidenter

CERT-SE är Sverige nationella CERT-funktion (Computer Emergency Response Team) och är placerad inom MSB. Till CERT-SE:s uppgifter hör bland annat att:

- Agera skyndsamt vid inträffade it-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade.
- Samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet.
- Vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa.

CERT-SE är medlem i flera internationella nätverk som TF-CSIRT (Task Force - Collaboration of Security Incident Response Teams), FiRST (Forum of Incident Response and Security Teams), IWWN (International Watch and Warning Network) och EGC (European Government CERT).

[163] Nationell handlingsplan 2012: https://www.msb.se/RibData/Filer/pdf/26290.pdf . Statusrapport: https://www.msb.se/RibData/Filer/pdf/27493.pdf
[164] European Cybercrime Centre: https://www.europol.europa.eu/ec3/ec3-in-action

9.3.1. Nationell hanterandeplan

På ett övergripande plan har Sverige även antagit en *nationell hanterandeplan för allvarliga it-incidenter*[165], vilken togs fram av MSB och gäller från 2011 och framåt. Planen är baserad på fyra huvudkomponenter: nationell lägesbild, informationssamordning, samlad konsekvens- och hanterandebedömning samt teknisk operativ samverkan. Hanterandeplanen aktiveras efter beslut av MSB, men ställer inte några uttalade krav på hanterande vid andra myndigheter. Däremot preciseras i planen vad som förväntas av andra aktörer i form av informationsdelning och samverkan.

9.4. Reglerande lag och standarder

9.4.1. Nationell lagstiftning[166]

Det finns ingen svensk informationssäkerhetslag men likväl regleras hanterandet av information på en mängd ställen i den svenska lagstiftningen. Lagstiftningen som reglerar svensk informations- och cybersäkerhet är fördelad på en rad olika lagar där formellt ansvar för tillsyn och föreskriftsrätt som tidigare nämnt är utspritt hos en rad olika statliga myndigheter[167]. Vissa lagar reglerar hur arbetet med informationssäkerhet ska utföras, andra lagar reglerar hur viss typ av information ska skyddas.
De i Sverige övergripande lagstiftningar som har påtagligast påverkan på informationssäkerhetsarbetet i myndigheter är *offentlighet- och sekretesslagen* (2009:400) och *personuppgiftslagen* (1998:204).

Offentlighet- och sekretesslagens (OSL) regelverk har krav som innebär ett uttalat behov av informationssäkerhet. Centralt i lagen är upprätthållandet av informationssäkerhetaspekten konfidentialitet, det vill säga säkerställa att de som inte är behöriga att ta del av en sekretessbelagd uppgift inte heller gör det. Utöver den aspekten innebär OSL även krav på spårbarhet, tillgängligt samt riktighet.

Personuppgiftslagen (PuL) reglerar i sin tur skyddet av medborgarnas personliga integritet vid behandling av personuppgifter. De bestämmelser som främst är inriktade på informationssäkerhet i personuppgiftslagen är kravet på att lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda de personuppgifter som behandlas. Sättet på vilket informationssäkerhetsarbetet hos exempelvis vårdgivarna ska bedrivas är dessutom reglerat i *föreskrifter om informationshantering och journalföring i hälso- och sjukvården* (SOSFS 2008:14), vilka utfärdats med stöd av *patientdataförordningen* (2008:360).

Mer specifikt inriktade lagar är *Säkerhetsskyddslagen* (1996:627), *säkerhetsskyddsförordningen* (1996:633) samt *Rikspolisstyrelsens föreskrifter* (RPSFS 2010:3) är de regelverk som ställer krav på att vissa verksamheter ska ha ett tillfredsställande säkerhetsskydd. Såväl offentliga som privata verksamheter som är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism omfattas av lagen.

Lagen (2003:389) om *elektronisk kommunikation* reglerar villkoren för att tillhandahålla elektroniska kommunikationstjänster, lagen (2000:832) om *elektroniska signaturer* reglerar framställandet och utfärdandet av elektroniska signaturer, och lagen (2006:24) om *nationella toppdomäner för Sverige på Internet* reglerar den tekniska driften av nationella

[165] Nationell hanterandeplan för allvarliga it-incidenter:
https://naturolyckor.msb.se/Upload/Nyheter_press/Nationell_hanterandeplan_for_allvarliga_IT-incidenter.pdf
[166] För en utförlig redogörelse för svensk lagstiftning på informations- och cybersäkerhetsområdet se kapitlet ”Säker informationshantering i digitala miljöer” i boken… NAMN? - HA
[167] För en utförlig genomgång av svensk lagstiftning och centrala aktörer på området se Riksrevisionens rapport Informationssäkerheten i den civila statsförvaltningen, kap. 3:
http://www.riksrevisionen.se/PageFiles/20759/RIR_2014_23_infos%c3%a4kerhet_Anpassad.pdf

toppdomäner för Sverige på internet samt tilldelning och registrering av domännamn under dessa toppdomäner.

Förordningen (2006:942) om *krisberedskap och höjd beredskap* (krisberedskapsförordningen) verkar på ett övergripande plan och syftar till att statliga myndigheter genom sin verksamhet ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter under fredstida krissituationer och höjd beredskap, bland annat inom informations- och cybersäkerhet. *Föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser* (MSBFS 2009:10) följer att de myndigheter som har ett särskilt ansvar för krisberedskap ska redovisa sin förmåga kopplat till informationssäkerhetsfrågor med hjälp av ett antal indikatorer. Föreskrifterna omfattar sex paragrafer som kompletteras med allmänna råd.

9.4.2. Standarder och svensk lagstiftning

Svensk lagstiftning om informations- och cybersäkerhet lutar sig i stor utsträckning på krav och definitioner hos ISO 27000-serien. Standarderna SS-ISO/IEC 27001 och SS-ISO/IEC 27002 är bland annat intimt kopplade till införandet av LIS (ledningssystem för informationssäkerhet) i svenska myndigheter där dessa anger detaljerade krav att förhålla sig till. Ett annat exempel är Datainspektionens allmänna råd om säkerhet för personuppgifter där det pekas på ISO-standarderna 27001 och ISO/IEC 27002. EU-lagstiftningen hänvisar också till ISO-standarden, bl.a. måste Statens Jordbruksverk och länsstyrelserna nu ISO-certifiera utbetalningar i de delar av verksamheten som omhändertar utbetalning av jordbruksstöd.

9.5. Kunskap, forskning och utbildning

Forskningen inom informations- och cybersäkerhet i Sverige bedrivs hos en mängd olika aktörer där högskolor och universitet står för en stor andel. Utöver högskolorna och universiteten bedriver även *Totalförsvarets forskningsinstitut* (FOI) och SICS (Swedish ICT) forskningsverksamhet på området[168]. För aktörer inom forskningsområdet finns nätverket SWITS. Även kommersiella aktörer MSB har tagit fram en forskningsstrategi för 2014-2018[169] i vilken informationssäkerhet betonas som ett viktigt område och flera utlysningar för forskning på området återfinns. Bl.a. har myndigheten pågående och kommande utlysningar rörande industriella styr- och kontrollsystem, cyberfysiska system och risk- och sårbarhetsanalys för informationssäkerhet.

Totalförsvarets signalskyddsskola (TSS) bedriver utbildning i traditionellt signalskydd och it-säkerhet samt krypto för skyddsvärda uppgifter (KSU).

Dessutom finns en bred samling utbildningar i olika aspekter av informations- och cybersäkerhet. Inom universitets- och högskolevärlden finns exempelvis *Försvarshögskolans* Chief Information Assurance Officer-utbildning samt kurs i informationssäkerhet för chefer [170], *Stockholms universitets* masterprogram i informationssäkerhet[171], vid institutionen för data- och systemvetenskap och *Institutet för Rättsinformatiks* kurser. Utöver dessa finns både myndighets- och kommersiellt knutna utbildningar som MSB:s DISA-utbildning om grunderna i informationssäkerhet, .SE:s utbildningar i IPv.6 och SIS Informationssäkerhetsakademis utbildningar inom området datavetenskap.

[168] Totalförsvarets forskningsinstitut: http://www.foi.se/en/ och SICS: https://www.sics.se/

[169] Forskning för ett säkrare samhälle: https://www.msb.se/RibData/Filer/pdf/27246.pdf

[170] Kurser i informationssäkerhet vid Försvarshögskolan (uppdragsutbildningar): http://www.fhs.se/sv/utbildning/uppdragsutbildningar/informationssakerhet/

[171] Masterprogram i informationssäkerhet (SU-DSV): http://dsv.su.se/utbildning/alla-utbildningar/masters/masterprogram-i-informationss%C3%A4kerhet

9.6. Skydd av personlig integritet

Skyddet av medborgarnas personliga integritet är främst knuten till reglerandet av personuppgiftsbehandling i *personuppgiftslagen* (1998:204).

Personuppgiftslagen är subsidiär vilket gör att exempelvis *Patientdatalagens* (2008:355), *Patientdataförordningen* (2008:360) och *Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården* (SOSFS 2008:14) bestämmelser samt andra specifika myndighetsförfattningar går före i sättandet av krav på behandlandet av personuppgifter.
Datainspektionen (DI) är tillsynsmyndighet på området och lägger stor vikt vid just det förebyggande arbetet, bl.a. genom information och rådgivning. Inspektionen utfärdar föreskrifter och allmänna råd och ger synpunkter på utredningar och lagförslag. Dessutom bedriver DI tillsynsverksamhet. Myndigheten har även ansvar för kameraövervakningslagen.

Bestämmelserna som är inriktade på informationssäkerhet i personuppgiftslagen är att lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda de personuppgifter som behandlas. DI möjlighet att fatta beslut om vilka säkerhetsåtgärder den personuppgiftsansvarige ska vidta. DI har även gett ut allmänna råd för att ge exempel på hur man uppfyller lagkraven. För en organisation som ska hantera personuppgifter i exempelvis ett eget register finns två val – antingen kan detta anmälas till DI eller så kan ett *Personuppgiftsombud* tillsättas inom organisationen.
Personuppgiftsombudet har som uppgift att, liknande en internrevisor, påpeka fel och brister till den som är personuppgiftsansvarig inom organisationen. Ombudet får stöd av DI dit denne även ska anmälas då denne utses.

10. National Cyber Security: Finland

10.1. National Government and Cyber Security

The Government of Finland is responsible for providing political guidance and strategic guidelines for cyber security as well as for taking the required decisions regarding the resources and prerequisites to be allocated to it.[172]

In line with the basic principles of the Security Strategy for Society, the competent authorities are responsible for disturbance management and associated contingency planning. Each ministry sees to the legislative process within its administrative domain, guides the action within its branch and, when necessary, participates in intersectoral cooperation.[173]

The Cyber Security Strategy does not change the tasks defined in the Security Strategy for Society, pursuant to which the Ministry of Transport and Communications is responsible for safeguarding the functioning of electronic ICT systems, and the Ministry of Finance is responsible for safeguarding the state administration's IT functions and information security, and the service systems common to the central government.[174]

The Security Committee [175] coordinates cyber security preparedness, monitors the implementation of the Cyber Security Strategy and issues recommendations on its further

[172] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[173] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[174] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[175] http://www.defmin.fi/en/overview/ministry_of_defence/departments_and_units/secretariat_of_the_security_committee

development. The Security Committee closely cooperates with other collaborative bodies that coordinate cyber security-related issues as part of their duties. The Cyber Security Centre[176] supports and assists cyber security actors within the scope of its tasking. The Government Information Security Management Board (VAHTI) supports the Government and the Ministry of Finance in administrative data security-related decision-making. VAHTI processes and coordinates all of the central government's important matters that relate to data security and cyber security.

The police will develop and bolster national IT crime prevention techniques by increasing cooperation between different police forces, including their rapid response capabilities. In accordance with the order of the National Police Board, the National Bureau of Investigation maintains a situation picture of international and organised crime. Moreover, the National Bureau of Investigation, together with the local police, maintains an integrated crime situation picture. The joint PCB (Police, Customs and the Border Guard) authorities' criminal intelligence and investigation centre is utilised in the compilation of the situation picture. The Finnish Security Intelligence Service maintains a situation picture of its field of activities.[177]

The Defence Forces will protect their own systems and networks; they will also create and maintain cyber intelligence and cyber warfare capabilities. The Defence Forces and the Cyber Security Centre cooperates in the compilation of the cyber situation picture.[178]

10.2. National Cyber Security Strategy and Policy

Finland's Cyber Security Strategy was adopted in 2013. The Strategy is yet to be fully implemented.

The vision of Finland's cyber security strategy is that:

- Finland can secure its vital functions against cyber threats in all situations.
- Citizens, the authorities and businesses can effectively utilize a safe cyber domain and the competence arising from cyber security measures, both nationally and internationally.
- By 2016, Finland will be a global forerunner in cyber threat preparedness and in managing the disturbances caused by these threats.

10.2.1. The objectives of the strategy[179]

1. Create an efficient collaborative model between the authorities and other actors for the purpose of advancing national cyber security and cyber defence.
2. Improve comprehensive cyber security situation awareness among the key actors that participate in securing the vital functions of society.
3. Maintain and improve the abilities of businesses and organisations critical to the vital functions of society as regards detecting and repelling cyber threats and disturbances that jeopardise any vital function and their recovery capabilities as part of the continuity management of the business community.
4. Make certain that the police have sufficient capabilities to prevent, expose and solve cybercrime.
5. The Finnish Defence Forces will create a comprehensive cyber defence capability for their statutory tasks.

[176] https://www.viestintavirasto.fi/en/cybersecurity.html
[177] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[178] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[179] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

6. Strengthen national cyber security through active and efficient participation in the activities of international organisations and collaborative fora that are critical to cyber security.
7. Improve the cyber expertise and awareness of all societal actors.
8. Secure the preconditions for the implementation of effective cyber security measures through national legislation.
9. Assign cyber security related tasks, service models and common cyber security management standards to the authorities and actors in the business community.
10. The implementation of the Strategy and its completion will be monitored.

10.2.2. Public-private partnerships

The National Emergency Supply organisation (NESO) is a network of multiple public-private partnership initiatives whose objectives are related to the security of supply. NESO is responsible for measures related to developing and maintaining the security of supply.[180]

The Finnish Information Security Cluster (FISC) <fisc.fi> is an association of Finnish information security companies. Their role is primarily business advocacy, however in representing the information security sector, FISC is significantly engaged with Finnish cybersecurity.[181]

10.3. Incident Response

Cyber incident management will follow the rule of law and the existing division of duties. The same cyber incident management principles that are used in normal conditions will be applied in emergency conditions. The authorities' division of duties and the modi operandi of the cooperation bodies will remain as they are in normal conditions.[182]

The National Cyber Security Centre Finland (NCSC-FI) was established in 2014 through a merger of CERT-FI and NCSA-FI. This body is responsible for the coordination of incident response and information security measures for both government institutions and the private sector.[183]

The Cyber Security Centre will:[184]

- Compile and disseminate the cyber security situation picture
- Compile and maintain a cyber-threat risk analysis, in conjunction with different administrative branches and actors
- Support the competent authorities and actors in the private sector in the management of widespread cyber incidents.
- Intensify cooperation and support the development of expertise.

While the National Cyber Security Centre Finland (NCSC-FI) is responsible for incident management, security incident reporting is managed by Finnish Communications Regulatory Authority (FICORA), of which the NCSC-FI is a sub-agency. Incidents are logged through an online form on the FICORA website.[185]

[180] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_finland.pdf
[181] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_finland.pdf
[182] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[183] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_finland.pdf
[184] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[185] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_finland.pdf

In accordance with its monitoring activities, the threat scenarios of the Security Strategy for Society, the cyber threat scenario and real-time national intelligence information, the Cyber Security Centre alerts businesses and authorities critical to the vital functions of society concerning new cyber threats to Finland and increased cyber threat levels and, upon request, assists them in contingency planning.[186]

The Government Situation Centre (GOVSITCEN) compiles the situation picture for the state leadership. Close cooperation between the GOVSITCEN and the Cyber Security Centre improves intersectoral monitoring and analysis capabilities, on which the integrated situation picture relies. Integrated situation awareness makes it possible to appropriately respond to threats at political and operational levels.[187]

10.4. Regulatory framework

No uniform cyber threat regulation exists in national legislation. Standards that address operations in IT networks are fragmented, and they approach cyber threats from different angles. Even though cyber operations by their very nature cross the boundaries of administrative branches, at the national level administrative branches define cyber threats from their own perspective. Moreover, powers also tend to be branch-specific. Depending on its origin and scope, a cyber threat can be considered an individual criminal act, a wider terrorist offence or an issue affecting state relations and military defence. This hampers the achievement of legal rulings and a consistent, national legal interpretation of the situation.[188]

The Government Decision on the Security of Supply 2008 is the latest set of official goals and standards relating to the protection of critical infrastructure. Section 2.2 of the decree addresses critical information technology infrastructure in particular. The decree is based is on the policies and systems defined in the Security of Supply.[189]

While there is no legislation or policy in place in Finland that requires the establishment of a written information security plan, the Ministry of Finance established Government Information Security Management Board (VAHTI) and published the Government Information Security Guideline in 2009. It contains security requirements expected of government organisations, including required handling and storage procedures.[190]

The Instructions on Implementing the Decree on Information Security in Central Government outlines “regular” auditing as part of the implementation and monitoring process of the Government Decree on Information Security in Central Government 2010, though the requirement is not in the decree itself.

The Finnish National Security Authority has published the National Security Auditing Criteria, which covers “information assurance” in detail.[191] There is no legislation or policy in place in Finland that requires mandatory reporting of cybersecurity incidents.[192]

[186] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[187] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[188] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[189] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_finland.pdf
[190] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_finland.pdf
[191] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_finland.pdf
[192] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_finland.pdf

10.5. Knowledge, Research and Education

Regarding the importance of cyber security to society, the goal in Finland's cyber security strategy is to improve understanding, competence and skills among the authorities, the business community and citizens and create a strong national cluster of cyber know-how. Cyber security research will be developed as part of national top-level research and a strategic cyber security center of excellence will be established at already existing structures. The purpose of exercises is to improve the participants' ability to identify vulnerabilities in their activities and systems, and to improve their skills and train their personnel. Different sectors regularly test their preparedness when it comes to managing disturbances in vital functions.[193]

The study of basic cyber security skills must be included at all levels of education. The learning requirements of cybersecurity must be included on the curricula of basic education (comprehensive school), vocational upper secondary education, general upper secondary education and higher education".[194]

An interdisciplinary, strategic cyber security centre of excellence will be established at the existing ICT-SHOK (TIVIT). It will provide an opportunity for top-level research teams and companies that utilise the results to engage in effective cooperation over the long term. The centre of excellence will employ an application-oriented and interdisciplinary research strategy, which companies, universities and research establishments have together defined.[195]

10.6. Protection of privacy and civil liberties

The right to privacy is protected in the Constitution of Finland (731/1999). This right is enforced through a number of statutes, including the Personal Data Act (523/1999) The PDA implements Directive 95/46/EC on data protection (Data Protection Directive) and applies to all types of processing of personal data. The PDA is supplemented by the Act on the Data Protection Board and the Data Protection Ombudsman (389/1994), which contains provisions concerning the supervising authorities: The Data Protection Ombudsman and the Data Protection Board.

There are also a number of sectoral laws, which have priority over the PDA. The act on the Protection of Privacy in Electronic Communications (516/2004) implements Directive 2002/58/EC on the protection of privacy in the electronic communications. *The objective of the Act is to ensure confidentiality and protection of privacy in electronic communications and to promote information security in electronic communications and the balanced development of a wide range of electronic communications services.*[196]

[193] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[194] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[195] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
[196] https://www.finlex.fi/fi/laki/kaannokset/2004/en20040516.pdf

11. National Cyber Security: Estonia

11.1. National Government and Cyber Security

Estonia was one of the first countries to develop a national cybersecurity strategy in 2008, followed by the release of an updated strategy in 2014. The Strategy developed in 2008 laid out a national action program for the national work and development in the field of cyber security, up to 2013.[197]

The national government of Estonia lays out the following principles of cyber security:[198]
- *Whole of nation (industry, individual users)*
- *Government role as regulator who establishes societal expectations, rules*
- *Public – private partnership and close cooperation*

After the release of the first national strategy in 2008, a Cyber Security Council was added to the Security Committee of the Government of the Republic in 2009.[199]

In 2010, The Estonian Informatics Centre was given government agency status, and the Estonian Information System Authority (RIA) received additional powers and resources. The Ministry of Economic Affairs and Communications directs cyber security policy, and RIA is a subdivision of the Ministry. RIA coordinates the development and administration of the state's information system, organizes activities related to information security, and handles the security incidents that have occurred in Estonian computer networks. RIA advises the providers of public services on how to manage their information systems as per requirements and monitors them, and is an implementing entity of the structural assistance of the European Union.

The Department of Critical Information Infrastructure Protection (CIIP) was formed within the RIA, with the purposes of organizing the protection of infrastructure. In early 2010, the RIA launched the critical information infrastructure (CII) mapping project, which identified the dependencies of vital services on information systems. Based on the mapping, security requirements for vital information systems necessary for the functioning of the state were developed. In 2011, a CIIP commission was formed to promote public-private cooperation. The purpose of the commission, which brings together cyber security and IT managers from vital services agencies, is to exchange operational information, identify problems and make suggestions for improving the cyber security of the country's critical infrastructure.

The main duties of RIA:[200]

- Executing supervision over information systems used to provide vital services and the implementation of the security measures of the information assets related to them.
- Organizing activities related to the state's information system and the information security of the Estonian critical information infrastructure.
- Handling the security incidents that occur in Estonian computer networks.
- Executing supervision over the fulfilment of the requirements arising from legislation that regulates the administration of the state's information system.
- Maintaining the administration system for the state's information system.
- Maintaining X-Road, the data exchange layer of the state's information system (development and administration).
- Coordinating the functioning of the public key infrastructure.

[197] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_estonia.pdf
[198] https://www.ria.ee/public/publikatsioonid/EISA_on_Cyber_Security_2012.pdf
[199] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_estonia.pdf
[200] https://www.ria.ee/about-estonian-information-system-authority/

- Coordinating the development projects of the state's information system, preparing international projects and participating in them.
- Maintaining the state portal eesti.ee.
- Serving as the implementing entity of European Union structural assistance.
- Organising basic infrastructure and data communication.
- Participating in the development of the legislation, policies, strategies and development plans regulating its area of activity.

The cybercrime investigation capabilities of the Police and Border Guard Board (PBGB) were consolidated into a single department in 2012. In 2013, officials dealing with cybercrime and digital evidence management procedures from various units in the prefectures were consolidated into cybercrime and digital evidence services. The PBGB is also engaged in raising awareness regarding cyber threats. In addition, the Estonian Internal Security Service strengthened its investigative capabilities in order to prevent threats to national security, including cyber-attacks and espionage.[201]

There is not a defined public-private partnership for cybersecurity in Estonia. While no formalized public-private partnerships exist, public entities seem to be working closely with several private sector organizations[202].

The Estonian National Cyber Defence League is a cyber-response unit comprised of IT professionals and representatives from entities engaged with critical infrastructure. The league is a voluntary organization aimed at protecting Estonian cyberspace, and it is specifically mentioned in Estonia's Cyber Security Strategy.[203]

In addition to national bodies, NATO's Cyber Security Centre of Excellence,[204] is based in Estonia.

11.2. National Cyber Security Strategy and Policy

The updated Estonian National cyber security strategy of 2014 is a continuation of the implementation of the 2008 goals. However, it includes new threats and needs that were not covered in the previous strategy.[205]

Purpose and actions of the national strategy
The government vision for cyber security outlined in the national strategy is that *"Estonia is able to ensure national security and support the functioning of an open, inclusive and safe society"*.

Furthermore, the strategy outlines eight principles, on which the government bases its work on national cyber security:[206]

1. *Cyber security is an integral part of national security; it supports the functioning of the state and society, the competitiveness of the economy and innovation.*
2. *Cyber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information, and identity.*

[201] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf
[202] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_estonia.pdf
[203] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf
[204] https://ccdcoe.org/about-us.html
[205] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf
[206] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

3. *Cyber security is ensured based on the principle of proportionality while taking into account existing and potential risks and resources.*
4. *Cyber security is ensured in a coordinated manner through cooperation between the public-, private- and third sectors, taking into account the interconnectedness and interdependence of existing infrastructure and services in cyberspace.*
5. *Cyber security starts with individual responsibility for safe use of ICT tools.*
6. *A top priority in ensuring cyber security is anticipating as well as preventing potential threats and responding effectively to threats that materialize.*
7. *Cyber security is supported by intensive and internationally competitive research and development.*
8. *Cyber security is ensured via international cooperation with allies and partners. Through cooperation, Estonia promotes global cybersecurity and enhances its own competence*

Responsibilities relating to the national strategy
The Ministry of Economic Affairs and Communications coordinates the implementation of the strategy. However, the strategy's implementation involves all ministries and government agencies. The strategy especially highlights the responsibilities of the Ministry of Defence, the Information System Authority, the Ministry of Justice, Police and Border Guard Board, the Government Office, the Ministry of Foreign Affairs, the Ministry of the Interior and the Ministry of Education and Research. It is also made clear that NGOs, business organizations, governments, and educational institutions cooperates in the implementation and assessment of the strategy. Among other things, agencies involved in executing the strategy will submit a written overview of the implementation of the measures and activities each year.[207]

11.3. Incident Response

Estonia's computer emergency response team, CERT Estonia, is under the administration of the Estonian Information System Authority. CERT Estonia was established in 2008. It is responsible for coordinating security and incident response measures across all Estonian networks.

CERT Estonia is tasked with managing the reporting of cybersecurity incidents, and provides an email-based reporting structure to log cybersecurity incidents. CERT Estonia deals with security incidents that occur in Estonian networks, start there, or which it has been notified about by citizens or institutions either in Estonia or abroad.[208]

The support the CERT provides will depend on the type and severity of the security incident, on the number of users potentially affected by it and on resources available for the organization. Estonia has categorized security incidents, and prioritized them according to their potential severity and scope. The prioritization takes into account: the number of affected users, the type of an incident, the target of an attack as well as the attack's point of origin, resources required to handle the incident. *"High-priority incidents include, for instance: attacks that may jeopardize people's lives, attacks on Internet infrastructure (name servers, major network nodes and large-scale automatic attacks on web servers), etc".*[209]

National incident management procedures are outlined in the Emergency Act 2009, however cybersecurity incidents are not addressed in particular.

[207] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf
[208] https://www.ria.ee/cert-estonia/
[209] https://www.ria.ee/cert-estonia/

By law, public sector institutions and providers of vital services are required to report major information security incidents. In 2012, the Department of Supervision registered 41 significant incidents, but none of these amounted to an emergency.[210]

11.4. Regulatory framework

Estonia also has a wide range of legislation that covers information security and cybersecurity[211].

The Emergency Act 2009 provides the legal bases for crisis management, including preparing for emergencies and responding to emergencies as well as ensuring the continuous operation of vital services. The act identifies the critical infrastructure of Estonia and regulates the organization and procedures involved in responding to related emergencies. Subsection 40, Paragraph 2 of the Emergency Act 2009 compels the government to establish security measures for certain vital information systems by means of regulation.[212]

The Regulation on Security Measures for Information Systems of Vital Services and Related Information Assets 2013 regulates the organization for the implementation of security measures for information systems in particular. "*The purpose of the Regulation is to ensure the capacity for consistent operation of information systems used for providing vital services and the possibility to restore them after an interruption*"[213]

The State Secrets and Classified Information of Foreign States Act 2007 assigns information deemed appropriate to be treated as state secret a classification level, according to a four-tiered system. The requirements that deem information a state secret are organised by the agency or area to which the information relates. The Act maps security practices to the classification level assigned to information deemed a state secret. These classification levels represent the importance of the information to the various functions of the Estonian government and foreign governments, including the level of risk involved in disclosing the information.

The State Secrets and Classified Information of Foreign States Act 2007 requires *an annual inspection of the existence and integrity of media containing state secrets classified as 'secret' and 'top secret'*.[214]

The Electronic Communications Act 2004, as amended in 2011, entitles the Technical Surveillance Authority of Estonia to require that any communications provider carry out a security audit. There is no timetable that indicates when the security audits should be required.[215]

The 2008 Cyber Security Strategy requires that the Cyber Security Strategy Committee will monitor the implementation of the Cyber Security Strategy by submitting annual reports to the government, measuring the progress of the implementation against the

[210] https://www.ria.ee/public/publikatsioonid/EISA_on_Cyber_Security_2012.pdf

[211] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_estonia.pdf

[212] http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXXX26&pg=1&tyyp=X&query=H%E4daolukorra+seadus&ptyyp=RT&keel=en

[213] https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf

[214] http://www.nsa.ee/files/State%20Secrets%20And%20Classified%20Information%20Of%20Foreign%20States%20Act.pdf

[215] http://www.legaltext.ee/text/en/X90001K4.htm

Implementation Plan[216]. The current Cyber Security Strategy does not include this provision but does state that it retains the goals and objectives of the 2008 strategy.

The Regulation on Security Measures for Information Systems of Vital Services and Related Information Assets 2013 requires entities engaged with "vital services" to each appoint an individual to notify the Estonian Information System Authority in the event of a security incident, including cybersecurity incidents. The entity must also submit a report to the Estonian Information System Authority following the resolution of the security incident[217].

Estonia recognizes international certification schemes for information security.

11.5. Knowledge, Research and Education

Estonia's Cyber Security Strategy includes a comprehensive education program. The 2014 Cyber Security details the success of the implementation of these goals and commits to continuing the same educations outcomes[218].

The program includes the following activities:

Organizing information security awareness-raising for the wider public in cooperation with the private sector, with a particular focus on home users, small and medium-sized enterprises, employees of local governments and state agencies, teachers and students. Conducting targeted media campaigns on cybersecurity and computer protection, and public advertising programs.

Raising awareness of cyber culture in every Estonian agency and company by training senior executives and officials in the promotion of secure computer and Internet use in all fields.

The cyber security strategy of 2014 lists some of the developments that have been made in this area since the first strategy was released. Among other things, the main provider of training and awareness raising in this field is the Information Technology Foundation for Education (HITSA). HITSA training is offered to pre-schoolers as well as older children, while also involving parents and teachers in the process. In cooperation between Tallinn University of Technology (TUT) and the University of Tartu, the international Master's program in Cyber Security was opened in 2009, with 50 students accepted into the program each year in 2014.

11.6. Protection of privacy and civil liberties[219]

The Personal Data Protection Act of Estonia was passed 12 February 2003. The purpose of the Act is protection of the fundamental rights and freedoms of people in accordance with public interests with regard to processing of personal data[220].

[216] http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

[217] https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf

[218] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

[219] http://www.legislationline.org/topics/country/33/topic/3

[220] http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.EE

"The purpose of this Act is to ensure that the public and every person has the opportunity to access information intended for public use, based on the principles of a democratic and social rule of law and an open society, and to create opportunities for the public to monitor the performance of public duties"[221].

The Electronic Communications Act concerns protection from unwanted electronic direct marketing. *"The purpose of this Act is to create the necessary conditions for the development of electronic communication, to promote the development of electronic communications networks and communications services without giving preference to specific technologies and to ensure the protection of the interests of users of electronic communications services by promoting free competition and the purposeful and just planning, allocation and use of radio frequencies and numbering".*[222]

[221] https://www.riigiteataja.ee/en/eli/510072014004/consolide

[222] http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X90001K2&keel=en&pg=1&ptyyp=RT&tyyp=X&query=electronic+communication