Net- og upplýsingaöryggi
Stefna 2014 - 2025

01001110011001010111010000101101001000000110111101100111001000000111010101110000011100000110110011111101011100110110100101101110011001110110000111110110011100100111100101100111011001110110100100001101000010100101001101110100011001010110011001101110011000010010000000110010001100000011000100110100001000000001011010010000000011001000110000000011001000110101

Drög til kynningar - 26. nóvember 2014

Enginn maður er *eyland*, einhlítur sjálfum sér; sérhver maður er brot *meginlandsins*, hluti *veraldar*; ef sjávarbylgjur skola *moldarhnefa* til *hafs*, minnkar *Evrópa*, engu síður en eitt *annes* væri, engu síður en *óðal vina* þinna eða *sjálfs þín* væri; *dauði* sérhvers manns smækkar *mig*, af því ég er íslunginn *mannkyninu*; spyr þú því aldrei hverjum *klukkan* glymur; hún glymur *þér*.

John Donne, 1579-1631,
í þýðingu Stefáns Bjarman á upphafi bókar Hemingways, *Hverjum klukkan glymur*.

Ávarp ráðherra
(kemur síðar)

Efnisyfirlit

Framtíðarsýn og stefna um net- og upplýsingaöryggi

Hér er sett fram ***Framtíðarsýn 2025*** um net- og upplýsingaöryggi[1] og ***Meginmarkmið stefnu*** til að ná megi þeirri sýn. Í inngangi er fjallað um vinnu starfshópsins sem vann að mótun stefnunnar og aðgerðaáætlun sem byggð er á stefnunni. Því næst er lýst ýmsum ógnum við nýtingu Netsins og mikilvægi þess að brugðist sé við þeim. Þá er fjallað um hvernig íslenskt samfélag er í stakk búið til að glíma við þessa ógn og hvað sé unnt að gera til að snúa vörn í sókn og nýta net- og upplýsingaöryggi til framfara og ábata. Nánari lýsingu á meginmarkmiðum stefnunnar má finna aftast. Fjallað er um aðgerðaáætlunina í sérriti, enda er hún til skamms tíma í senn og verður endurskoðuð árlega.

Framtíðarsýn 2025

> Íslendingar búi við Net sem þeir geti treyst og þar séu í heiðri höfð mannréttindi,
> persónuvernd ásamt frelsi til athafna, efnahagslegs ávinnings og framþróunar.
> Örugg upplýsingatækni sé ein meginstoð hagsældar á Íslandi,
> studd af öflugri öryggismenningu og traustri löggjöf.
> Jafnframt sé samfélagið vel búið til að taka á netglæpum, árásum,
> njósnum og misnotkun persónu- og viðskiptaupplýsinga.

Meginmarkmið stefnu

1. **Bætt þekking**. Almenningur, fyrirtæki og stjórnvöld búi yfir þeirri þekkingu, hæfni og tækjum sem þarf til að verjast netógnum.
2. **Aukið áfallaþol**. Áfallaþol upplýsingakerfa samfélagsins og viðbúnaður verði aukinn þannig að hann standist samanburð við áfallaþol upplýsingakerfa á Norðurlöndum. Þetta sé t.d. gert með samvinnu og með því að öryggi verði órjúfanlegur þáttur í þróun og viðhaldi net- og upplýsingakerfa.
3. **Bætt löggjöf**. Íslensk löggjöf sé í samræmi við alþjóðlegar kröfur og skuldbindingar á sviði netöryggis og persónuverndar. Jafnframt styðji löggjöfin við nýsköpun og uppbyggingu þjónustu sem byggir á öryggi, t.d. hýsingu.
4. **Traust löggæsla**. Lögregla búi yfir eða hafi aðgang að faglegri þekkingu og búnaði til að leysa úr málum er varða net- og upplýsingaöryggi.

[1] Hér notað sem þýðing á enska hugtakinu *Cyber security*, þar til samstaða næst um aðra þýðingu.

Inngangur

Í júní 2013 var starfshópur um stefnumótun í net- og upplýsingaöryggi settur á fót á vegum innanríkisráðuneytisins. Aðalverkefni hópsins er að móta stefnu stjórnvalda um net- og upplýsingaöryggi og vernd upplýsingainnviða sem varða þjóðaröryggi, það er upplýsingakerfa mikilvægra innviða samfélagsins. Þau kerfi eru þó flest tengd öðrum upplýsingakerfum samfélagsins með einum eða öðrum hætti á Netinu.

Afmörkun stefnu

Stefnunni er ætlað að ná til verndar mikilvægra innviða landsins og nauðsynlegra viðbragðra vegna vaxandi netógna sem steðja að stjórnvöldum, viðskiptalífi og borgurum. Netið er orðið hluti af hversdagslegu umhverfi nær allra Íslendinga með æ margvíslegri hætti. Öryggi þessa umhverfis skiptir alla máli og því **snertir stefnan alla notkun net- og upplýsingatækni**.

Samfélagsleg markmið verksins eru sem hér segir:

- Að auka öryggi einstaklinga og þjóðfélagshópa með því að efla net- og upplýsingaöryggi.
- Að stuðla að órofa virkni mikilvægra samfélagsinnviða með því að auka þol net- og upplýsingakerfa gagnvart áföllum.
- Að efla samstarf og samhæfingu á milli stjórnvalda hér á landi og á alþjóðavettvangi um net- og upplýsingaöryggi.

Koma þarf á skilvirku samstarfi stjórnvalda hér á landi og á alþjóðavettvangi og skýra ábyrgðarsvið og verkaskiptingu á sviði net- og upplýsingaöryggis. Við mótun þessarar stefnu var tekið mið af ýmsum innlendum stefnum og stefnum grannríkja á þessu sviði og þeirra alþjóðastofnana sem Ísland er aðili að.

Í starfshópnum eru: Sigurður Emil Pálsson sérfræðingur í innanríkisráðuneytinu, sem jafnframt er formaður, Guðbjörg Sigurðardóttir skrifstofustjóri upplýsingasamfélagsins, innanríkisráðuneytinu, Páll Heiðar Halldórsson og Ottó V. Winther, sérfræðingar í innanríkisráðuneytinu, Jón F. Bjartmarz yfirlögregluþjónn og Ágúst Finnsson (frá janúar 2014) sérfræðingur hjá embætti ríkislögreglustjóra, Hrafnkell V. Gíslason, forstjóri Póst- og fjarskiptastofnunar, Stefán Snorri Stefánsson hópstjóri CERT-ÍS hjá Póst- og fjarskiptastofnun, Jónas Haraldsson sérfræðingur í utanríkisráðuneytinu og Þorsteinn Arnalds (frá maí 2014), sérfræðingur hjá Persónuvernd.

Í störfum hópsins var lögð áhersla á að rýna almennan grunn og ráðleggingar sem stefnumótun á þessu sviði hefur verið byggð á, stefnur nokkurra grannþjóða hafa verið teknar til greiningar og rætt hefur verið við innlenda sem erlenda aðila, ráðgefandi sérfræðinga og opinbera fulltrúa um ýmsa þætti upplýsingaöryggis, ógnir og tækifæri og þá reynslu sem hefur fengist af þeim aðgerðaáætlunum sem hrint hefur verið í framkvæmd í grannríkjum.

Fjölsóttur samráðsfundur með hagsmunaaðilum var haldinn 2. júní 2014, þar sátu um 80 fulltrúar um 60 stofnana og fyrirtækja. Við mótun þessarar stefnu var tekið mið af þeim athugasemdum sem þar komu fram.

Tengsl við aðrar stefnur og ályktanir Alþingis

Stefnan um net- og upplýsingaöryggi tengist með beinum eða óbeinum hætti mörgum öðrum opinberum stefnum og ályktunum. Má þar nefna stefnu í almannavarna- og öryggismálum ríkisins, löggæsluáætlun, fjarskiptaáætlun, væntanlegri þjóðaröryggisstefnu og stefnuna um upplýsingasamfélagið, *Vöxtur í krafti netsins*.

Netið: Tækifærin, traustið og ógnirnar

Tækifærum, á sviði net- og upplýsingatækni fjölgar ört, ekki síst vegna þess að tölvutæknin er orðin stór þáttur nær alls umhverfis okkar og tölvur, stórar sem smáar verða æ tengdari. Orð John Donne, sem vísað er til á forsíðu, eiga ekki síður við nú en fyrr. Netið hefur gert jarðarbúa meira eða minna samtengda, með þeim kostum og göllum sem því fylgir. Þetta býður upp á umfangsmeiri gagnasöfnun, greiningu og nýtingu upplýsinga en nokkru sinni hefur þekkst. Upplýsingatæknin er grunnur viðskiptalífs og einnig æ mikilvægari markaðsvara í sjálfri sér. Það er ekki nóg með að efnahagslegur og félagslegur ávinningur af tölvutækninni geti verið gríðarlegur – grannþjóðir okkar skilgreina hana sem ómissandi grundvöll framfara og hagvaxtar. Net- og upplýsingaöryggi felur því meðal annars í sér að efla traust viðskiptaumhverfi með baráttu gegn netógnum, að styrkja áfallaþol upplýsingakerfa sem oftar en ekki geta ráðið úrslitum um ótruflað gangverk lykilinnviða þjóðfélagsins, að efla Netið sem frjálsan upplýsingamiðil og auka þekkingu og hæfni á sviði net- og upplýsinga-öryggis.

Traust – undirstaða notkunar Netsins

Það berast æ fleiri fregnir af innbrotum í tölvukerfi og viðskiptaupplýsingum jafnt sem persónulegum gögnum er stolið, sumt er birt og annað notað í öðrum tilgangi. Íslendingar hafa einnig fengið að kenna á þessari þróun. Til þess að net- og upplýsingatæknin geti skilað okkur framangreindum ávinningi verður notkun hennar að byggjast á trausti. Án trausts nýtum við ekki Netið til samskipta, viðskipta, öflunar fróðleiks eða til neins annars sem skiptir okkur máli. Ýmislegt hefur vegið að trausti á notkun Netsins á síðari árum og það er mikilvægt að bregðast við til að viðhalda traustinu.

Vaxandi ógn vegna glæpa og óheimillar söfnunar og nýtingar upplýsinga

Eðli netárása og innbrota hefur verið að breytast undanfarin ár. Það eru ekki lengur eintaklingar sem eru að smíða veirur og brjótast inn sem eru mest áberandi, skipulögð glæpasamtök og jafnvel ríki hafa tekið við. Ör þróun hefur verið í skipulagðri glæpastarfsemi á Netinu. Þetta geta verið glæpir sem eru hefðbundnir í eðli sínu, en sem taka á sig annað og mun stærra form vegna Netsins. Dæmi um þetta eru blekkingar eða stuldur sem beint er gegn mjög stórum hópi. Segja má að innan alþjóðlegrar glæpastarfsemi á þessu sviði hafi orðið viss iðnbylting[2]. Starfsemin byggist ekki lengur á að hafa mjög hæfa handverksmenn á þessu sviði. Árásartækni, viðkvæmar upplýsingar og gagnaþýfi eru orðin að torrekjanlegri söluvöru á svörtum alþjóðlegum markaði. Glæpamenn þurfa ekki að hafa mikla tækniþekkingu, hana má kaupa frá sérhæfðum aðilum auk búnaðar og ýmissar annarrar þjónustu. Fullkomin árásar- eða njósnakerfi geta því verið samsett úr einingum sem koma frá mismunandi löndum. Þetta getur gert erfiðara að greina uppruna tiltekinna árása. Álitið er að tiltölulega lítill vel menntaður hópur, jafnvel aðeins um hundrað manns, standi á baki við þróun öflugasta búnaðarins. Háþróað neðanjarðarhagkerfi þýðir hins vegar að þessi búnaður stendur mörgum til boða. Mörg innbrot hafa náð athygli fjölmiðla vegna þess að gerandinn hefur auglýst verknaðinn en ætla má að ótilkynnt innbrot séu mun fleiri. Þá láta ýmsar varasamar ógnir lítið yfir sér. Má þar m.a. nefna stuld á upplýsingum (t.d. iðnarleyndarmálum) og ógnir gegn upplýsingakerfum mikilvægra innviða í samfélaginu. Tungumálið og fjarlægð voru okkur áður viss vörn gegn mörgum

[2] Sjá t.d. matskýrslu Europol um stöðu netglæpa sem var gefin út 29. september 2014: *The Internet Organised Crime Threat Assessment* (IOCTA):
https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta
Þar kemur fram að sérhæfðir netglæpamenn tengist skipulagðri glæpastarfsemi í ört vaxandi mæli með því að bjóða fram þjónustu sem gengur kaupum og sölum á milli aðila sem eru í órekjanlegum tengslum hver við annan (og þekkjast ekki persónulega). Þetta er það viðskiptalíkan sem skipulögð glæpastarfsemi nýtir sér nú meira og meira, „glæpaþjónusta“ (á ensku: *Crime-as-a-Service,* CaaS)

ógnum, svo er ekki lengur. Glæpasamtökin kunna einnig vel að nýta sér veilur í lagalegu umhverfi, bæði hjá einstökum þjóðríkjum og hvað snertir alþjóðlega samvinnu. Þau láta til skarar skríða þar sem er eftir sem mestu að slægjast og þar sem varnir eru veikastar.

Öryggisfyrirtækið McAfee gaf út skýrslu[3] í júní 2014 um mat á hnattrænum kostnaði vegna glæpa á sviði net- og upplýsingaöryggis. Þar kemur fram það mat að flest ríki og fyrirtæki vanmeti þessa ógn og þann kostnað sem henni fylgi, beinan sem óbeinan. Jafnframt sé vanmetið hversu hratt þessi ógn getur aukist. Þessi kostnaður getur hæglega verið 1% þjóðarframleiðslu. Kostnaðurinn einn segi ekki alla söguna, því þessir glæpir beinist iðulega að þeim sviðum þjóðfélagsins þar sem nýsköpun og þróun ætti að vera mest. Glæpirnir hafi því áhrif á vinnumarkaðinn og skaði atvinnuþróunartækifæri. Tækni- og þekkingarstörfum fækki. Þetta getur einnig leitt til atgervisflótta úr landi. Auka þurfi upplýsingaflæði um netárásir, en nú kjósa flest fyrirtæki að tilkynna þær ekki. Vanmat áhættu verður til þess að ekki er gripið til nauðsynlegra varna og það eru skipulögð glæpasamtök að nýta sér í vaxandi mæli, því þeim finnst lítil áhætta fylgja glæpum á þessu sviði enn sem komið er. Lamandi áhrif skipulagðrar glæpastarfsemi getur því gætt víðar en ætla mætti í fyrstu.

Fullyrt hefur verið að ýmis þjóðríki standi á bak við innbrot í tölvukerfi, sérstaklega þegar um er að ræða tölvukerfi mikilvægra innviða annarra ríkja. Erfitt getur verið að sanna slíkt, jafnvel þegar um stórtæka netárás er að ræða, því hún getur verið gerð frá tölvubúnaði þriðja aðila, jafnvel að honum óafvitandi. Ýmis stórfyrirtæki sem bjóða þjónustu á Netinu fjármagna hana með því að selja upplýsingar notenda sinna. Vaxandi umræða er víða um lönd hvar sé rétt að draga mörkin í þessum efnum, jafnvel þegar notandi hefur samþykkt skilmála sem hafa verið gerðir honum aðgengilegir. Í allri þessari söfnun og nýtingu upplýsinga er mikilvægt að tryggja að ekki sé brotið á einstaklingum, fyrirtækjum og stofnunum, t.d. á sviði persónuverndar. Alþjóðlegar kröfur um vernd persónu-upplýsinga og rekjanlegt gagnaöryggi eru sífellt að verða strangari. Sumt af þessu hefur beint gildi í íslensku lagaumhverfi og má þar nefna reglugerðir Evrópusambandsins.

Áherslur grannþjóða

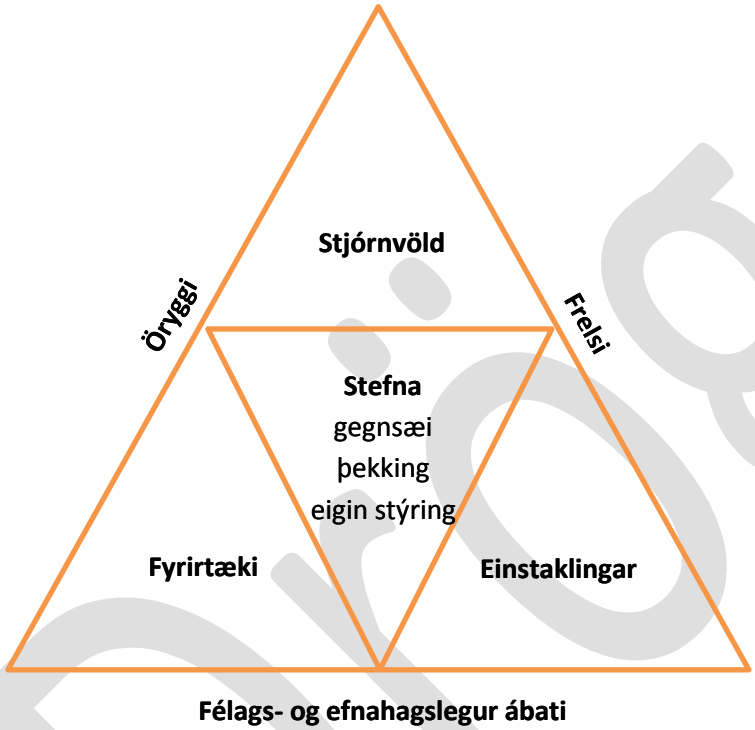
Meðal þess sem grannþjóðir okkar hafa tilgreint í stefnum sínum um net- og upplýsingaöryggi er að takast þurfi á við eftirfarandi atriði til að efla framfarir:

- Vitund og öryggismenning varðandi tölvu- og netnotkun.
- Þekking og hæfni sérfræðinga, stjórnenda og almennra notenda á sviði net- og upplýsingaöryggis.
- Vernd upplýsinga, ekki síst persónuupplýsinga. Einstaklingar, fyrirtæki og hið opinbera þurfa að vera á varðbergi gagnvart óheimilli söfnun og nýtingu upplýsinga.
- Vernd net- og upplýsingaöryggis mikilvægra innviða þjóðfélagsins. Víða er lögð vaxandi áhersla á þetta vegna þess hve margir samverkandi þættir eru orðnir tengdir Netinu með einum eða öðrum hætti.
- Geta til að verja tölvukerfi, að greina tilraunir til árása og geta brugðist við þeim. Upplýsingar um veikleika tölvu- og netkerfa eru vel þekktar og nýjar upplýsingar dreifast fljótt og til eru mörg árásartól sem nýta þær.
- Geta til að takast á við tölvubrot. Hér er átt við glæpi tengda tölvum, hvort sem þeir snúa að tölvu- og netbúnaði sem slíkum eða að tölvum er beitt til annarra glæpa. Skipulögð glæpastarfsemi á þessu sviði er í örum vexti.
- Að grunngildi samfélagsins séu einnig höfð að leiðarljósi í netheimum, til dæmis persónufrelsi, frelsi til að afla sér upplýsinga, gagnkvæm virðing og umburðarlyndi.

[3] http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf

Ábati af samvinnu mismunandi aðila á grunni stefnu

Í stefnum ýmissa landa hefur verið reynt að sýna með einföldum hætti hvernig mismunandi aðilar í þjóðfélaginu þurfi að vinna saman og hvernig afrakstur þess samstarfs getur orðið. Í nýlegri endurskoðaðri hollenskri stefnu[4] er svipuð mynd og hér er birt til skýringar en hún sýnir samverkan mismunandi aðila (einstaklinga, fyrirtækja og stjórnvalda) í stefnumótun og afrakstur hennar (öryggi, frelsi og félags- og efnahagslegan ábata).



Ábati af samvinnu mismunandi aðila, byggður á sameiginlegri stefnu.

[4] https://www.ncsc.nl/english/organisation/about-the-ncsc/background.html

Staða á Íslandi varðandi net- og upplýsingaöryggi

Á Íslandi hefur verið blómleg nýting tölvutækni og margvíslegar nýjungar þróaðar. Íslenskir sérfræðingar á sviði net- og upplýsingaöryggis hafa þó um árabil bent á ýmis hættumerki á fundum og ráðstefnum. Þótt áhugi á öryggismálum hafi virst fara vaxandi hefur sérfræðingum lítið þótt vera um aðgerðir. Í prófun sem gerð var hérlendis haustið 2014 kom fram að rúmlega 70% útstöðva hjá fyrirtækjum voru með veikar varnir gegn innbrotum. Það séu fáir með menntun eða vottun á þessu sviði á Íslandi og lítið framboð náms á háskólastigi og þá helst sem sértæk námskeið. Þá verði öryggi gjarnan afgangsstærð í þróun hugbúnaðar, svipað og mengunarvarnir í gamla daga, þegar helst var rætt hvort setja þyrfti síu á strompinn í stað þess að bæta framleiðsluferlið. Sé öryggið aftast í þróunarferlinu, þá er það gjarnan skorið fyrst burt þegar tími og fé eru af skornum skammti. Til að verja fyrirtæki kaupa stjórnendur gjarnan lausn í tilteknum búnaði eða fela tæknimanni með takmarkað umboð að koma á öryggi. Ef byggja á upp umferðaröryggi dugir ekki að fela það bara bifvélavirkja, hversu góður sem hann kann að vera, allir notendur umferðar þurfa að koma að verkefninu. Þótt hér séu til góðir sérfræðingar á mörgum sviðum net- og upplýsingaöryggis, þá skortir vettvang til samstarfs og til að byggja upp nauðsynlega öryggismenningu á þessu sviði hérlendis. Ennfremur skorti hér að gerðar séu viðbragðsáætlanir varðandi net- og upplýsingaöryggi og látið reyna á með æfingum og prófunum hversu vel þær virka.

Íslensk fjármálafyrirtæki hafa gert margt til að verjast netglæpum. Með batnandi efnahag á Íslandi og afnámi gjaldeyrishafta verður eftir meiru að slægjast hér á landi fyrir skipulagða glæpastarfsemi. Það getur því þurft að huga sérstaklega að betri vörnum íslensks fjármálakerfis.

Tölvur er víðar að finna en fólk hyggur í fyrstu. Mörgum lykilþáttum nútímasamfélags, t.d. orkudreifingu, vatnsveitu og samgöngum, er stjórnað með iðntölvum, sem hafa í vaxandi mæli verið nettengdar á síðustu árum. Þetta hefur boðið upp á margvíslega hagræðingu í nýtingu og rekstri, því það er hægt að vakta og stýra búnaði án þess að nokkur þurfi að vera nálægur. Nettengingunni fylgir þó einnig áhætta. Hönnuðir búnaðar til innbrota á tölvukerfi hafa á síðari árum lagt meiri áherslu á þróun búnaðar til að brjótast inn í þessi stjórnkerfi. Yfirvöld hafa almennt brugðist við og lagt meiri áherslu á varnir og hefur það einnig verið gert hérlendis. Mörg ríki álíta netárás á stýrikerfi mikilvægra innviða samfélagsins eina helstu netógnina sem bregðast þurfi við, enda hafa skimanir á Netinu sýnt að margar iðntölvur virðast vera aðgengilegar til innbrota, einnig á Íslandi[5]. Jafnvel þótt tölvur í grunnkerfum séu vel varðar, þá er ekki víst að aðrar tölvur, sem geti tengst þeim með beinum eða óbeinum hætti og haft áhrif á starfsemi þeirra, séu nægilega varðar. Það er því afar mikilvægt að hugað sé vel að öryggi iðntölva mikilvægra innviða samfélagsins.

Flugsamgöngur skipta Íslendinga mjög miklu máli. Nútímastjórnun á flugsamgöngum er háð nýtingu upplýsingatækni, ekki síst Netsins. Það er því mikilvægt að vel sé hugað að öryggi á þessu sviði.

[5] Sjá t.d. Project SHINE (SHodan INtelligence Extraction) Findings Report, 1 október 2014, umfjöllun um skýrsluna: http://www.securityweek.com/project-shine-reveals-magnitude-internet-connected-critical-control-systems

Stefna og aðgerðir hérlendis: Með öryggi til sóknar

Þær ógnir og áskoranir sem að framan er lýst kalla á viðbrögð. En í þessum áskorunum felast einnig mikilvæg tækifæri til sóknar og til þess að gera íslenskt hugbúnaðarumhverfi samkeppnisfærara á erlendum vettvangi. Með því að hafa öryggi í öndvegi strax við frumhönnun má iðulega losna við kostnaðarmyndandi þætti síðar. Með öruggri grunnhönnun má hanna traust flókin tölvukerfi, svipað og að með öryggri hönnun má reisa skýjakljúfa, án hennar verða þeir aðeins skýjaborgir. Í erlendum stefnum er æ algengara að sjá áherslu á *„security by design“* og *„privacy by design“*, þ.e. að öryggis og persónuverndar sé gætt strax við frumhönnun. Þetta þurfa einnig að verða grunngildi í íslenskri hugbúnaðarhönnun. Net- og upplýsingaöryggi þarf að verða hluti tölvutengds náms á öllum skólastigum. Jafnframt þarf að efla slíkt nám á háskólastigi og mynda tengsl við erlenda háskóla, þannig að nemendur með viðeigandi grunnpróf frá íslenskum háskóla geti stundað framhaldsnám í net- og upplýsingaöryggi.

Líklegt er að á markaði fyrir hugbúnað og hugbúnaðartengda þjónustu verði gerðar æ strangari kröfur um öryggi kerfa. Mörg lönd ætla sér að nýta þetta til að skapa sér samkeppnislegt forskot miðað við önnur lönd, að bjóða upp á net- og upplýsingaumhverfi sem styður vel við þarfir viðskipta, iðnaðar og einstaklinga. Það getur bæði falist í öruggara umhverfi til rafrænna viðskipta og einnig í því að verða í fararbroddi í net- og upplýsingaöryggi og gera það að verðmætri útflutningsvöru. Varnir gegn iðnaðarnjósnum eru einnig mjög mikilvægur þáttur, enda eru þær stór hluti efnahagsskaða af völdum netógna. Ráðgjafafyrirtæki eru farin að nota stöðu ríkja varðandi net- og upplýsingaöryggi sem mælikvarða fyrir fyrirtæki sem hyggjast t.d. setja upp gagnaveitur eða aðra tölvutengda þjónustu. Það sést t.d. í skýrslu[6] sem *Economist Intelligence Unit* tók saman. Þar er meðal annars horft til lagaumhverfis, menntunar (sérstaklega í raungreinum og verkfræði), tæknilegra innviða þjóðfélagsins og nýtingar upplýsingatækni í þjóðfélaginu.

Lagaumhverfi hérlendis þarf einnig að vera þannig að það styðji við hugbúnaðartengda þróun og veiti jafnframt vernd gegn glæpsamlegri notkun Netsins, þannig að til dæmis skipulögð glæpasamtök telji Ísland ekki hentugt starfsumhverfi vegna bágborins net- og upplýsingaöryggis. Gæta verður þess á hverjum tíma hvernig íslensk löggjöf er í samanburði við löggjöf grannríkja okkar. Lögreglan verður síðan að hafa getu til að fylgja þessum lögum eftir. Huga þarf sérstaklega að persónuvernd, enda er tækniþróunin það ör að viðmið geta breyst fljótt og mikilvægt er að á Íslandi gildi ekki síðri persónuvernd en í grannlöndum okkar.

Með einfaldri vitundarvakningu má einnig ná miklum árangri. Talið er að draga megi verulega úr ógn bæði gagnvart einstaklingum og fyrirtækjum með tiltölulega einföldum varúðaraðgerðum. Til mikils er að vinna í baráttu gegn tölvubrotum (glæpum tengdum tölvum). Reynt hefur verið að meta tjón af þeirra völdum í Bretlandi[7] og er talið að það hlaupi á hverju ári á að minnsta kosti milljörðum punda. Sé gert ráð fyrir að kostnaður á íbúa sé sá sami á Íslandi og Bretlandi, þá ætti samsvarandi upphæð

[6] Skýrslan var tekin saman fyrir Booz Allen Hamilton ráðgjafafyrirtækið:
http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf

[7] Í skýrslu sem var gefin út 2011 var þessi kostnaður metinn 27 milljarðar punda á ári. Stutt samantekt skýrslunnar:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf
Heildartexti: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
Fleiri greinargerðir hafa verið gerðar og í þeim er matið almennt lægra. Bresk stjórnvöld gáfu út ítarlega skýrslu þann 7. október 2013: *„Cyber crime: a review of the evidence“*. Þar er komist að þeirri niðurstöðu að nákvæmt mat sé að öllum líkindum illmögulegt, en þó sé raunhæft að áætla að kostnaður vegna tölvubrota hlaupi að minnsta kosti á milljörðum punda á ári (e. *„ .. the cost of cyber crime could reasonably be assessed to equate to at least several billion pounds per year“*).
https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

fyrir Ísland að hlaupa á að minnsta kosti milljörðum króna. Hér er eingöngu talinn sá kostnaður sem fylgir glæpum, ekki netógnum almennt. Þótt margir óvissuþættir geti verið í slíku mati, þá er mikill ávinningur af góðum vörnum. Varnir fjármálakerfa geta dregið verulega úr tjóni. Samtök sem bresk fjármálafyrirtæki hafa gegn misferli (*Financial Fraud Action UK*) meta að sértækar lögregluaðgerðir gegn glæpum af þessu tagi hafi dregið úr tjóni um 450 milljónir punda á þeim rúmlega áratug sem þessar gagnaðgerðir hafa staðið[8].

Efla þarf varnir mikilvægra innviða samfélagsins. Það er fjölþætt verkefni. Öflug netöryggissveit er mikilvæg til að greina ýmsar árásir og veita aðstoð. Fjarskiptakerfi og grunnkerfi flutningsneta þurfa að vera traust. Efla þarf upplýsingatækni og öryggi innan stjórnsýslunnar, til dæmis hvað varðar samhæfingu og fræðslu.

Meginstoðir í stefnu Íslands í öryggis og varnarmálum byggja á samstarfi við Norður-Atlantshafsbandalagið (NATO), virku samstarfi við grannríki og varnarsamningnum við Bandaríkin. Þær byggja einnig á þeim upplýsingainnviðum sem tilgreindir eru að framan. Að verja þá innviði sem þessi starfsemi hér á landi reiðir sig á er því eitt af mikilvægustu atriðum í vörnum landsins. Af því tilefni var nýverið skrifað undir samkomulag við NATO *Cyber Defence Management Board* sem mun leiða til aukins samstarfs á þessu sviði. Til merkis um áherslu bandalagsins á netöryggi var ákveðið á nýafstöðnum leiðtogafundi þess að netárás gæti fallið undir fimmtu grein stofnsáttmálans.

Aukið samstarf við aðrar alþjóðastofnanir á við Sameinuðu þjóðirnar, Evrópuráðið, Evrópusambandið og Öryggis- og samvinnustofnun Evrópu í málaflokknum geta einnig stuðlað að bættu netöryggi á Íslandi.

Það getur verið eftir miklu að slægjast ef tekst að breyta vörn í sókn. Efling net- og upplýsingaöryggis er verkefni sem enginn einn aðili í þjóðfélaginu getur tekið að sér. Til að ná sem mestum árangri verður að nálgast verkefnið á heildstæðan hátt og með samstilltu átaki sem flestra sem nýta net- og upplýsingatækni og vísast þar jafnt til opinberra aðila sem einkaaðila. Mikilvægt er að hefjast handa strax og skapa sameiginlegan vettvang til framþróunar og samvinnu, til dæmis um öryggisviðmið, samhæfingu, greiningu öryggisógna og skipulagningu viðbragða. Ekki síst er mikilvægt að ganga að þessu verki vitandi að það þurfi að vera lifandi og í sífelldri endurskoðun eftir því sem verki miðar og sýn skýrist, leyst er úr málum og nýjar áskoranir birtast.

Lýsing meginmarkmiða

Meginmarkmið 1: Bætt þekking

Almenningur, fyrirtæki og stjórnvöld búi yfir nægjanlegri þekkingu og hæfni (verkfærum) til að verjast netógnum.

Þekking er undirstaða þess að byggja upp net- og upplýsingaöryggi. Viðfangsefnið er svipað og að byggja upp umferðaröryggi. Hluti þess er tæknilegur, svipað því að hafa sem öruggust ökutæki og umferðarmannvirki. Almennur borgari á ekki að þurfa að vera bifvélavirki til að njóta umferðar-öryggis. Hann verður þó að vera virkur þátttakandi í umferðarmenningunni, hafa ákveðna þekkingu á öryggi búnaðar og hegðun, sjálfum sér og öðrum til hagsbóta. Virk öryggismenning á ekki að þurfa að vera íþyngjandi, þvert á móti þá gerir hún meiri umferð mögulega en annars. Öryggismenning verður að vera hluti af tölvumenningu frá upphafi, frá fyrstu kynnum barna af tölvum og í tengslum við

[8] http://www.financialfraudaction.org.uk/Fraud-the-Facts-2014.asp

tölvunotkun og kennslu á öllum skólastigum. Vitundarvakning er lykilatriði í stefnu flestra grannþjóða okkar.

Á Íslandi, eins og annars staðar, felst hluti þekkingar í því hvernig við tölum um viðfangsefni okkar, orðaforðanum og hugtakanotkun. Til að svið nái að dafna þarf að samhæfa orða- og hugtakanotkun. Það þarf einnig að vera skýr verkaskipting, hver gerir hvað, hvaða ábyrgð ber hver notandi og hvaða væntingar er raunhæft að gera til annarra.

Á Íslandi eru til sérfræðingar sem hafa unnið gott starf árum saman. En það er engu að síður stórt átaksverkefni að byggja upp traustan og breiðan grunn á þessu sviði og sem öflug öryggismenning á sviði net- og upplýsingaöryggis þarf að hvíla á. Staða slíkrar öryggismenningar er einn af þeim mikilvægu þáttum sem fjárfestar horfa til þegar metið er hversu vænleg viðskipta- og upplýsingatækniumhverfi mismunandi landa eru.

Meginmarkmið 2: Aukið áfallaþol

Áfallaþol upplýsingakerfa samfélagsins verði aukið.

Efla þarf vöktun og getu til að bregðast við óeðlilegu ástandi á Netinu, þó þannig að viðeigandi persónuverndarsjónarmiða sé gætt. Þetta er svipað og í umferðinni, eitt er að fylgjast með umferðarþunga á vegum og annað að fara að skoða hverjir eru þar á ferð og hvaða farm þeir flytja. Vöktunin sem hér er átt við er hliðstæð þeirri þegar fylgst er með umferðarþunga.

Aðilar þurfa að geta skipst skjótt á upplýsingum um hugsanlegar ógnir. Það er því mikilvægt að mynda samstarfsvettvang, einn eða fleiri, þar sem aðilar geta skipst á upplýsingum varðandi net- og upplýsingaöryggi, með vel skilgreindum hætti þannig að samkeppnissjónarmiða og persónuverndar sé gætt. Þetta gæti krafist milligöngu opinbers aðila til að tryggja að unnt sé að dreifa skjótt upplýsingum um eðli árásar án þess að auglýsa þurfi hvert fórnarlambið var.

Þróun í net- og upplýsingaöryggi er mjög ör. Það er því mikilvægt að allir sem komi að þessum málaflokki séu virkir í alþjóðlegri samvinnu, hver á sínu sviði. Með góðri samvinnu innanlands og skilvirkum skiptum á upplýsingum er unnt að bregðast sameiginlega við örri þróun. Það þarf einnig að vera virk þátttaka í alþjóðlegu samstarfi til þess að viðhalda þekkingu og tengslum og til þess að geta unnið með öðrum þjóðum og ríkjasamböndum þegar netvá ber að. Í alþjóðlegu samstarfi þarf einnig að vera tryggt að Ísland komi fram með samhæfða stefnu í þeim málum sem snerta net- og upplýsingaöryggi.

Bætt áfallaþol hugbúnaðarkerfa byrjar með öruggri hönnun. Örugg hönnun þarf að verða grunnviðmið við kaup og þróun á hugbúnaði, sérstaklega þegar um mikilvæga innviði er að ræða. Gildir þá einu hvort átt er við samfélagið í heild eða einstakar stofnanir eða fyrirtæki.

Meginmarkmið 3: Bætt löggjöf

Íslensk löggjöf sé í samræmi við alþjóðlegar kröfur og skuldbindingar á sviði netöryggis og persónuverndar. Jafnframt styðji löggjöfin við nýsköpun og uppbyggingu þjónustu (t.d. hýsingu).

Góð löggjöf er lykilatriði í uppbyggingu net- og upplýsingaöryggis. Mikilvægi hennar er margþætt:

- Ísland á aðild að alþjóðlegum samningum sem gera ákveðnar kröfur til löggjafar. Þetta gildir ekki síst um *Samninginn um tölvubrot* (Búdapest samninginn) frá 2002.
- Netið er alþjóðlegt og því er mikilvægt að löggjöf hérlendis sé vel samhæfð löggjöf í grannlöndum okkar, eftir því sem við á. Löggjöfin verður að tryggja persónuvernd og hana má

nýta til að skapa eftirsóknavert umhverfi fyrir þróun og rekstur upplýsingatæknifyrirtækja. Hún má þó ekki skapa veikleika sem skipulögð glæpastarfsemi kann að sækja í.
- Evrópusambandið er að vinna stefnu um net- og upplýsingaöryggi. Taka verður tillit til þeirrar stefnu í íslenskri löggjöf þegar hún er tilbúin.
- Nýting skýjatækni (cloud technology) hefur ýmsar lagalegar áskoranir í för með sér, taka þarf tillit til hvað önnur lönd og Evrópusambandið gera á þessu sviði og hver lagatúlkun þeirra er.
- Öryggisatvik þurfa að verða tilkynningarskyld, það er þó æskilegt að það sé útfært þannig að aðilar sjái sér hag í því að tilkynna jafnframt því að vera skuldbundnir til þess. Hér er átt við að koma í veg fyrir að aðilar telji e.t.v að þeir skaði ímynd sína eða samkeppnisstöðu með því að tilkynna atvik á meðan þeir sem þegja njóti góðs af.

Meginmarkmið 4: Traust löggæsla

Lögregla búi yfir eða hafi aðgang að faglegri þekkingu og búnaði til að leysa úr málum er varða net- og upplýsingaöryggi

Alþjóðlegt eðli Netsins getur vakið upp mörg úrlausnarefni varðandi löggæslu og rannsókn sakamála. Þetta á til dæmis við varðandi lögsögu mála á Netinu og aukna notkun á skýjalausnum.

Íslensk lögregla verður að hafa getu til að rannsaka glæpi tengda net- og upplýsingaöryggi. Til að ná því markmiði þarf ekki einungis fræðslu og þjálfun fyrir sérfræðinga, heldur einnig fræðslu fyrir almenna lögregluþjóna um hvernig skuli þekkja og bregðast við glæpum á þessu sviði. Lögregla þarf að geta átt aðgang að íslenskum og erlendum sérfræðingum eftir því sem við á, ekki síst hjá Europol og því þekkingarsetri sem þar hefur verið komið upp.

Efla þarf getu til varna gegn netnjósnum og annarri óeðlilegri söfnun upplýsinga á Netinu.

Hæfni til að taka á glæpsamlegri notkun Netsins er forsenda þess að íslenskt samfélag nái að nýta sér til fulls þau samfélagslegu og efnahagslegu tækifæri sem Netið hefur upp á að bjóða.

Geta til löggæslu er einn þeirra þátta sem fyrirtæki horfa til varðandi öruggt starfsumhverfi. Sýnileg geta á þessu sviði getur því haft verulegan ávinning í för með sér fyrir íslenskt samfélag.

Endurskoðun stefnu og aðgerðaáætlunar

Þessi stefna skal rýnd og endurskoðuð eftir þörfum, eigi sjaldnar en á fjögurra ára fresti. Aðgerðum til að fylgja stefnunni skal lýsa í sérriti, þær skulu vera til skemmri tíma og skulu endurskoðast eigi sjaldnar en árlega. Ferli við framkvæmd stefnunnar skal vera í anda opinnar stjórnsýslu.