Net- og upplýsingaöryggi
Stefna 2015–2026
Aðgerðir 2015–2018

01001110 01100101 01110100 00101101 00100000 01101111 01100111 00100000 01110101 01110000 01110000 01101100 11000011 10111101 01110011 01101001 01101110 01100111 01100001 11000011 10110110 01110010 01111001 01100111 01100111 01101001 00001010 01010011 01110100 01100101 01100110 01101110 01100001 00100000 00110010 00110000 00110001 00110101 00100000 11100010 10000000 10010011 00100000 00110010 00110000 00110010 00110110 00001010 01000001 11000011 10110000 01100111 01100101 01110010 11000011 10110000 01101001 01110010 00100000 00110010 00110000 00110001 00110101 00100000 00101101 00100000 00110010 00110000 00110001 00111000 00001010

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 Bjarmans á upphafi bókar Hemingways, *Hverjum klukkan glymur*.

Innanríkisráðuneytið
Apríl 2015

Innanríkisráðuneytið
Apríl 2015

Efnisyfirlit

Framtíðarsýn og stefna um net- og upplýsingaöryggi ... 3
Framtíðarsýn 2026 ... 3
Meginmarkmið stefnu ... 3
Inngangur ... 4
Netið: Tækifærin, traustið og ógnirnar ... 5
Traust – undirstaða notkunar Netsins ... 5
Vaxandi ógn vegna glæpa og óheimillar söfnunar og nýtingar upplýsinga ... 5
Áherslur grannþjóða ... 6
Ábati af samvinnu mismunandi aðila á grunni stefnu ... 7
Net- og upplýsingaöryggi – staðan hérlendis ... 8
Stefna og aðgerðir hérlendis: Með öryggi til sóknar ... 9
Endurskoðun stefnu og aðgerðaáætlunar ... 12
Nánari lýsing aðgerða ... 19
Meginmarkmið 1 – Efld geta ... 20
Meginmarkmið 2 – Aukið áfallaþol ... 23
Meginmarkmið 3 – Bætt löggjöf ... 27
Meginmarkmið 4 – Traust löggæsla ... 28

Framtíðarsýn og stefna um net- og upplýsingaöryggi

Hér er sett fram ***Framtíðarsýn 2026*** 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 nota net- og upplýsingaöryggi til framfara og ábata. Nánari lýsingu á meginmarkmiðum stefnunnar má finna aftar og fjallað er um aðgerðaáætlunina í síðari hluta þessarar skýrslu.

Framtíðarsýn 2026

> 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. **Efld geta**. Almenningur, fyrirtæki og stjórnvöld búi yfir þeirri þekkingu, getu og tækjum sem þarf til að verjast netógnum.
2. **Aukið áfallaþol**. Bætt geta til greiningar, viðbúnaðar og viðbragða eru lykilþættir í bættu áfallaþoli. Áfallaþol upplýsingakerfa samfélagsins og viðbúnaður verði aukinn þannig að hann standist samanburð við áfallaþol upplýsingakerfa á Norðurlöndum. Þetta sé t.d. gert með bættri getu við greiningu á ógnum, 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, hæfni 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 viðbragða 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 greindar 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 frá um 60 stofnunum og fyrirtækjum og annar ámóta fundur var haldinn þann 15. janúar 2015 sem um 60 fulltrúar sóttu. Við mótun þessarar stefnu var tekið mið af þeim athugasemdum sem fram komu á fundunum.

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 stefnunni 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 einstaklingar 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 valdið því að erfiðara er að greina uppruna tiltekinna árása. Álitið er að tiltölulega lítill vel menntaður hópur, jafnvel aðeins um hundrað manns, standi á bak 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. iðnaðarleyndarmálum) og ógnir gegn upplýsingakerfum

[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 meir og meir, svokallaða „glæpaþjónustu“ (á ensku: *Crime-as-a-Service,* CaaS)

mikilvægra innviða í samfélaginu. Tungumálið og fjarlægð voru okkur áður viss vörn gegn mörgum ógnum en 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 eftir sem mestu er að slægjast og þar sem varnir eru veikastar. Europol gaf út skýrslu 2. mars 2015[3], þar sem lýst er mati á hvernig skiplögð glæpastarfsemi sé að taka stakkaskiptum um þessar mundir og færa sig yfir á Netið í æ ríkari mæli. Lýst er hvernig ný tegund glæpamanna sé að verða algengari, menn sem bjóði ýmsa þjónustu á Netinu og noti það til afbrota, samskipta og greiðslumiðlunar.

Öryggisfyrirtækið McAfee gaf út skýrslu[4] 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. Kostnaðurinn geti hæglega verið 1% þjóðarframleiðslu. Hann 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 á hættu 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 ríki 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:

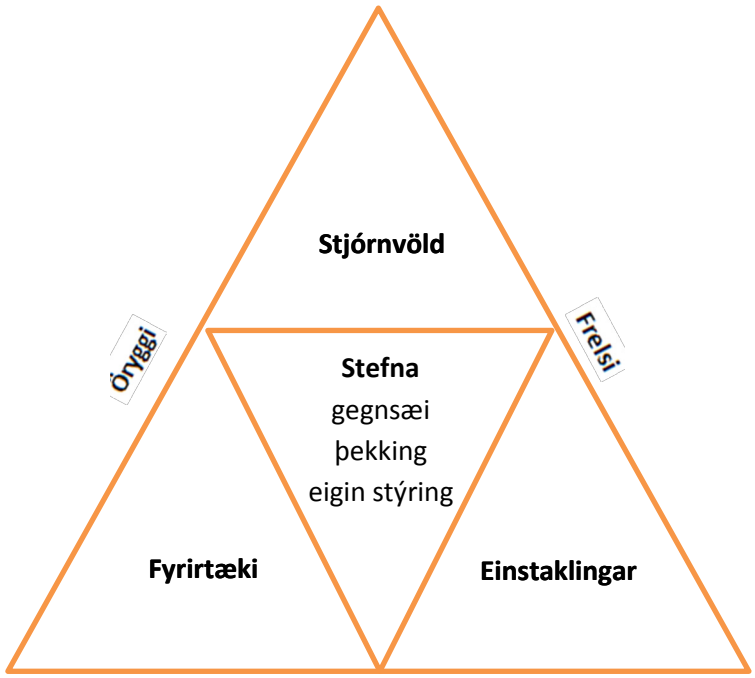
- Vitund og öryggismenningu varðandi tölvu- og netnotkun.
- Þekkingu og hæfni sérfræðinga, stjórnenda og almennra notenda á sviði net- og upplýsingaöryggis.
- Vernd upplýsinga, ekki síst persónuupplýsinga. Einstaklingar, fyrirtæki og hið opinbera þurfa að vera á varðbergi gagnvart óheimilli söfnun og 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.

[3] https://www.europol.europa.eu/content/massive-changes-criminal-landscape
[4] http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf

- 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.

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[5] 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).



Félags- og efnahagslegur ábati

Ábati af samvinnu mismunandi aðila, byggður á sameiginlegri stefnu.

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

Net- og upplýsingaöryggi – staðan hérlendis

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 hér á landi og lítið framboð náms á háskólastigi og þá helst sem sértæk námskeið. Þá verði öryggi gjarnan afgangsstærð í þróun hugbúnaðar, svipað og var með mengunarvarnir fyrr á tíð, þegar helst var rætt um 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. Enn fremur skorti hér að gerðar séu viðbragðsáætlanir um net- og upplýsingaöryggi og látið reyna á hversu vel þær virka með æfingum og prófunum.

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 í nútímasamfélagi, 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 hérlendis[6]. 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.

[6] 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. Í öllu þessu 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 öruggri 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[7] sem *Economist Intelligence Unit* tók saman. Þar er meðal annars horft til lagaumhverfis, menntunar (sérstaklega í raungreinum og verkfræði), tæknilegra innviða samfélagsins og nýtingar á upplýsingatækni.

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 hérlendis 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[8] 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 hér á landi og í Bretlandi, þá ætti samsvarandi

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

[8] 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

upphæð 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[9].

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.

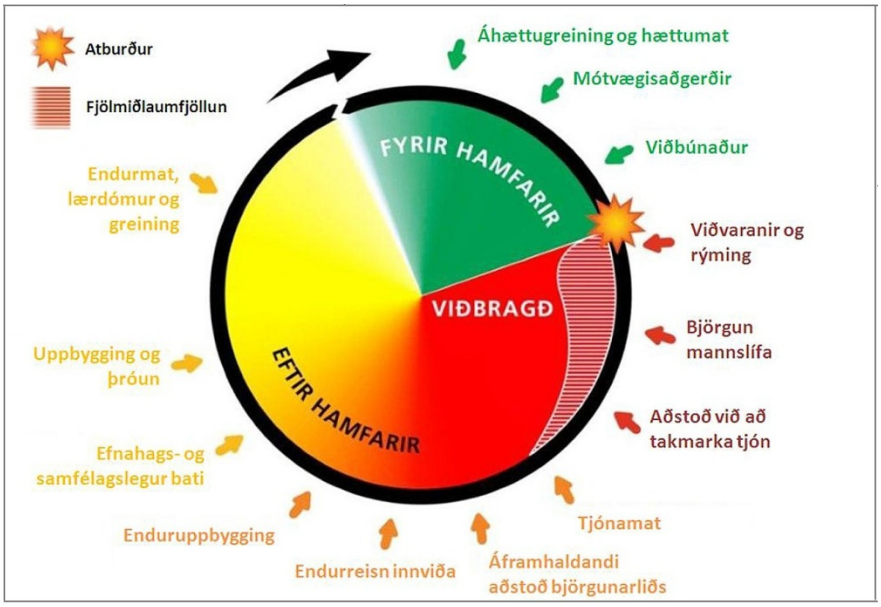
Meginstoðir í stefnu Íslands í öryggis og varnarmálum byggja á samstarfi við Norður-Atlantshafsbandalagið (NATO), virku samstarfi við grannríki og varnarsamningnum við Bandaríkin. Þær byggja einnig á þeim upplýsingainnviðum sem tilgreindir eru að framan. Að verja þá innviði sem þessi starfsemi hér á 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 marks 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 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 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.

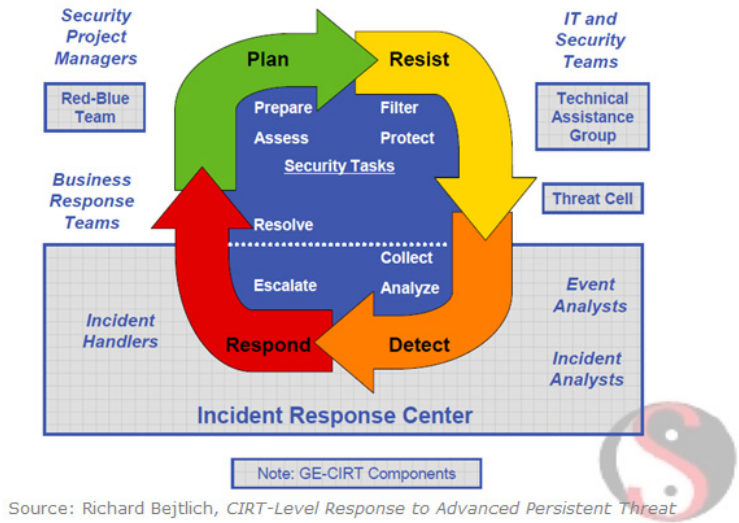
[9] http://www.financialfraudaction.org.uk/Fraud-the-Facts-2014.asp

Almannavarnahringrásin



Heimild: *Áhættuskoðun almannavarna: helstu niðurstöður* [Ritstjóri Guðrún Jóhannesdóttir, Reykjavík: Ríkislögreglustjóri, almannavarnadeild, 2011].

Með þessari stefnu er miðað við að uppbygging upplýsinga- og netöryggis verði með svipuðum hætti og uppbygging annarra þátta almannavarna. Það verði stuðlað að áhættugreiningu, mótvægis-aðgerðum og viðbúnaði svipað og lýst er á mynd um almannavarnahringrásina að ofan og á eftirfarandi mynd af síðu SANS-stofnunarinnar[10]. Ef áfall eða árás verður þá verði lögð áhersla á skjóta upplýsingamiðlun á milli viðeigandi aðila til að takmarka tjón og síðan verði unnið að áframhaldandi aðgerðum, mati og uppbyggingu með svipuðum hætti og lýst er í almannavarnahringrásinni. Jafnframt verði atvikið greint svo draga megi viðeigandi lærdóm af því. Sé um atvik af völdum manna að ræða þá þarf einnig að tryggja að viðeigandi lögreglurannsókn geti farið fram með skilvirkum hætti.



Source: Richard Bejtlich, *CIRT-Level Response to Advanced Persistent Threat*

[10] Sjá vefsíðu: http://digital-forensics.sans.org/blog/2010/09/27/digital-forensics-security-incident-cycle/

Endurskoðun stefnu og aðgerðaáætlunar

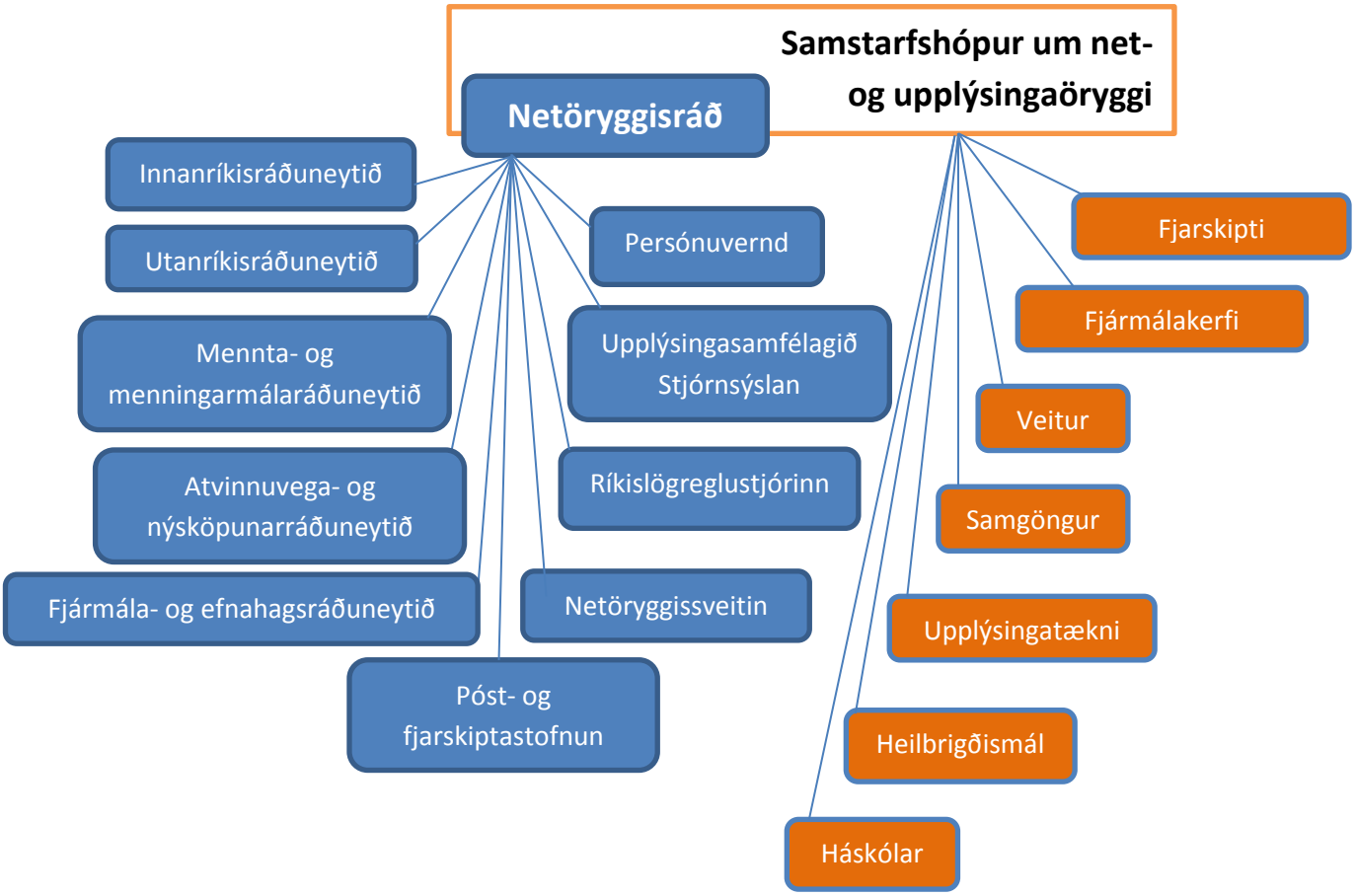
Þessi stefna skal rýnd og endurskoðuð eftir þörfum, eigi sjaldnar en á fjögurra ára fresti. Aðgerðir byggðar á stefnunni skulu vera til skemmri tíma og skulu endurskoðast eigi sjaldnar en árlega. Ferli við framkvæmd stefnunnar skal vera í anda opinnar stjórnsýslu.

Áætlun um aðgerðir 2015–2018

Til að hrinda stefnunni um net- og upplýsingaöryggi í framkvæmd er lagt til að skipað verði sérstakt **netöryggisráð** með fulltrúum opinberra aðila sem koma að framkvæmd stefnunnar og jafnframt verði myndaður **samstarfshópur um net- og upplýsingaöryggi**, þar sem fulltrúar hagsmunaaðila eigi einnig fulltrúa.

Netöryggisráð
Yfirumsjón með framkvæmd stefnunnar hefur Netöryggisráð, sem skipað er af innanríkisráðherra. Netöryggisráðið samhæfir aðgerðir, sérstaklega þeirra sem lúta að opinberum aðilum. Það endurskoðar aðgerðaáætlunina eigi sjaldnar en árlega og gerir tillögu um forgangsröðun og fjármögnun verkefna. Netöryggisráð skilar árlega skýrslu til innanríkisráðherra um framkvæmd stefnunnar.

Samstarfshópur um net- og upplýsingaöryggi
Samstarfshópur um net- og upplýsingaöryggi er samvinnuvettvangur fulltrúa opinberra stofnana sem sitja í netöryggisráði og fulltrúa einkaaðila. Hópurinn getur samhæft framkvæmd verkefna hagsmunaaðila, í heild sinni eða að hluta, og skapað þar vettvang fyrir samvinnu um tiltekin verkefni sem snúa að net- og upplýsingaöryggi á afmörkuðum sviðum.



Aðgerðir fyrsta tímabils stefnunnar krefjast átaks til að koma á þeirri víðtæku samvinnu ríkis og hagaðila sem viðfangsefnið krefst. Miðað er við að þessar átaksaðgerðir fyrsta tímabils verði endurskoðaðar árlega, en á síðari tímabilum verði framkvæmdin samræmd því sem tíðkast í öðrum stefnum. Stefnunni er ætlað að vera grundvöllur samvinnu og framþróunar í net- og upplýsingaöryggi. Stefnan sjálf ein sér breytir ekki ábyrgð og skyldum þeirra sem koma að net- og upplýsingaöryggi þótt fram kunni að koma tillögur um aðgerðir sem feli slíkar breytingar í sér.

Skipulag á innleiðingu stefnunnar verður með þeim hætti að fyrri hluta árs 2015 verði myndaður samstarfsvettvangur með hagaðilum, „Samstarfshópur um net- og upplýsingaöryggi“. Þar verði einstakar aðgerðir útfærðar nánar og kostnaðarmetnar. Margar aðgerðir fela í sér samhæfingu í starfi mismunandi aðila og sérstakt fjármagn er því ekki nauðsynlegt til þess að unnt sé að hefjast handa. Þó má reikna með að til þess að átakið verði nægilega öflugt þurfi um 20 milljónir króna í samhæfingu, úttektir og fræðslu. Gert er ráð fyrir að fyrirtæki fjármagni hluta kostnaðar í sumum verkefnum. Tillögum að verkefnum sem krefjast opinbers fjármagns sé skilað til netöryggisráðs, sem geri tillögu um forgangsröðun verkefna að höfðu samráði við hagsmunaaðila.

Við lok hvers tímabils mun netöryggisráð taka saman skýrslu byggða á samantektum ábyrgðaraðila allra aðgerða, kynna árangur starfsins og leggja fram tillögur að höfðu samráði við hagsmunaaðila um aðgerðaáætlun næstu þriggja ára.

Stefnt er að gegnsæi í starfi netöryggisráðs, fundargerðir verði birtar og gögn gerð opinber, nema um sé að ræða gögn sem óheimilt sé að birta lögum samkvæmt, t.d. vegna persónuverndarsjónarmiða.

Hér á eftir eru meginmarkmiðin sett fram og aðgerðir við hvert þeirra. Aðgerðunum er síðan nánar lýst á frá og með blaðsíðu 20. Margar aðgerðirnar tengjast þótt mismunandi aðilar geti komið að framkvæmd þeirra. Það er því mikilvægt að við nánari útfærslu á einstökum aðgerðum sé hugað að slíkum tengingum og hugsanlegri skörun. Það er á ábyrgð Netöryggisráðs að það sé gert.

Meginmarkmið 1: Efld geta

Almenningur, fyrirtæki og stjórnvöld búi yfir nægilegri þekkingu, hæfni og tækjum sem þarf 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 tölvunotkun og kennslu á öllum skólastigum. Vitundarvakning er lykilatriði í stefnu flestra grannþjóða okkar. Vitundarvakningin verður að tala til öruggrar hönnunar, notkunar og að persónuvernd verði í heiðri höfð.

Hérlendis, 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.

Hér á landi eru sérfræðingar sem hafa unnið gott starf árum saman. Það er engu að síður stórt átaksverkefni að byggja upp traustan grunn 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.

Aðgerðir

1. **Vitundarvakning**
   Almenn vitund um net- og upplýsingaöryggi verði efld.
2. **Hugtök**
   Viðeigandi alþjóðlegum skilgreiningum hugtaka, sem eru mikilvæg varðandi net- og upplýsingaöryggi, verði safnað og þess gætt að þau hafi verið þýdd þar sem þörf er á.
3. **Grunnnám**
   Net- og upplýsingaöryggi verði hluti tölvutengds námsefnis á öllum skólastigum.
4. **Framhaldsnám**
   Nemendur með grunnpróf frá íslenskum háskólum eigi kost á framhaldsnámi í net- og upplýsingaöryggi sem uppfylli sambærilegar kröfur og grannþjóðir gera til náms á því sviði.
5. **Hönnunargildi**
   Örugg hönnun og persónuvernd verði meðal grunngilda í eflingu íslensks hugbúnaðarstarfs.
6. **Persónuvernd**
   Hugað verði að alþjóðlegum kröfum og skuldbindingum um persónuvernd við uppbyggingu net- og upplýsingaöryggis.

Meginmarkmið 2: Aukið áfallaþol

Áfallaþol upplýsingakerfa samfélagsins verði aukið. Bætt geta til greiningar, viðbúnaðar og viðbragða eru lykilþættir í bættu áfallaþoli.

Efla þarf vöktun og getu til að bregðast við óeðlilegu ástandi á Netinu, þó þannig að viðeigandi persónuverndarsjónarmiða sé gætt.

Aðilar þurfa að geta skipst skjótt á upplýsingum um hugsanlegar ógnir. Því er mikilvægt að myndaður sé samstarfsvettvangur, 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 hratt 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, einstakar stofnanir eða fyrirtæki.

7. **Samstarfsvettvangur**
   Samstarfsvettvangur verði þróaður þar sem fulltrúar frá opinberum aðilum og einkafyrirtækjum geti unnið saman að málum sem varða net- og upplýsingaöryggi.
8. **Öryggisviðmið**
   Val á viðeigandi viðmiðum (stöðlum jafnt sem öðrum) varðandi net- og upplýsingaöryggi.
9. **Alþjóðlegt samstarf**
   Efla og samhæfa þátttöku Íslands í netöryggisstarfi á erlendum vettvangi.
10. **Traust grunnkerfi**
    Fjarskiptakerfi og grunnkerfi flutningsneta styðji með skilgreindum áreiðanleika net- og upplýsingakerfi mikilvægra innviða samfélagsins, bæði tengingar innanlands og til útlanda.
11. **Stjórnsýslan**
    Net- og upplýsingaöryggi í stjórnsýslunni verði eflt með aukinni fræðslu, samhæfingu og samvinnu.
12. **Greining**
    Helstu ógnir á sviði net- og upplýsingaöryggis verði greindar og mikilvægir innviðir samfélagsins skilgreindir.
13. **Vernd innviða**
    Geta netöryggissveitar til stuðla að vernd og að aðstoða mikilvæga innviði samfélagsins verði efld og virk viðbragðsgeta verði til staðar allan sólarhringinn, alla daga ársins. Sérstök áhersla verði lögð á fjarskipta-, veitu- og fjármálafyrirtæki og þau kerfi sem eru mikilvæg vegna flugsamgangna við umheiminn.
14. **Viðbragð**
    Viðbragðsáætlanir vegna netógna verði þróaðar og prófaðar með æfingum, með sérstakri áherslu á mikilvæga innviði samfélagsins.

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) á þessu sviði.

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 2001.
- 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 eftirsóknarvert 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. Æskilegt er að skyldan sé útfærð 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. Hér má taka mið af því skipulagi sem nú þegar er þekkt við rannsóknir samgönguslysa, eftir því sem við á.

15. Bætt löggjöf

Íslensk löggjöf verði endurskoðuð þannig að tryggt sé að hún sé í samræmi við alþjóðlegar skuldbindingar og geri mögulegt að glíma við netógnir með sambærilegum hætti og tíðkast í grannlöndum okkar. Jafnframt sé löggjöfin þannig úr garði gerð að hægt verði að takast á við netógnir með sambærilegum hætti og aðrar ógnir í samfélaginu, eftir því sem við á.

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 hafa 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.

16. **Löggæsla**
    Hæfni lögreglu til að fást við glæpi tengda net- og upplýsingaöryggi verði bætt með aukinni þekkingu byggðri á kennslu, fræðslu, efldri innlendri og alþjóðlegri samvinnu og þeim búnaði sem til þarf.

Nánari lýsing aðgerða

Hér á eftir fylgir nánara yfirlit yfir aðgerðir. Fyrir hverja aðgerð er tilgreint:

- Markmið
- Eigandi
- Ábyrgð
- Verkefnastjórn
- Aðrir lykilaðilar
- Lýsing
- Mælikvarði

Aðilar sem eru innan Netöryggisráðs eða ætlað er að verði innan Samstarfshóps um net- og upplýsingaöryggi eru að jafnaði ekki tilgreindir sérstaklega sem „aðrir lykilaðilar“.

Meginmarkmið 1 – Efld geta

Aðgerð 1 - Vitundarvakning

Markmið:	Almenn vitund um net- og upplýsingaöryggi verði efld.
Eigandi:	Innanríkisráðuneytið
Ábyrgð:	Netöryggisráð
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Menntamálaráðuneytið, samstarfshópur um net- og upplýsingaöryggi, hópar sem vinna að þessu markmiði.
Lýsing:	Efld vitund allra sem koma að nýtingu net- og upplýsingatækni er meginatriði í stefnu flestra grannþjóða okkar. Verkefnið er svipað og að byggja upp umferðarmenningu, það er ekkert eitt atriði og enginn einn aðili sem leysir málið. Efla þarf umræðu um net- og upplýsingaöryggi víða og með margvíslegum hætti. Hugsanlega væri æskilegt að hafa vettvang á Netinu sem sameiginlegan tengilið.
Mælikvarði:	Opnir fundir/vinnustofur þar sem sérstaklega er fjallað um netöryggismál fyrir sérfræðinga verði eigi sjaldnar en árlega. Árlegir opnir fundir/vinnustofur sem miðast við þarfir skólakerfisins, foreldrasamtaka og annarra sem áhuga hafa á netöryggismálum, þar með talinn almenning. Tryggja umfjöllun um netöryggismál í fjölmiðlum. Fyrsta samantekt um árangur liggi fyrir 15. janúar 2016.

Aðgerð 2 – Hugtök

Markmið:	Viðeigandi alþjóðlegum skilgreiningum hugtaka, sem eru mikilvæg varðandi net- og upplýsingaöryggi, verði safnað og þess gætt að þau hafi verið þýdd þar sem þörf er á.
Eigandi:	Innanríkisráðuneytið
Ábyrgð:	Netöryggisráð
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Utanríkisráðuneytið, Samstarfshópur um net- og upplýsingaöryggi, hér væri einnig æskilegt að fá til samstarfs orðanefnd sem hefur starfað á þessu sviði og aðila sem sinna staðlamálum.
Lýsing:	Orðanefnd Skýrslutæknifélagsins hefur unnið mikið og gott starf árum saman við að þýða hugtök tengd tölvunotkun og safna þeim saman í orðalista. Í þýðingum á stöðlum hefur einnig þurft að þýða hugtök sem snerta net- og upplýsingaöryggi. Taka þarf upp samstarf við orðanefndina varðandi þýðingar á mikilvægum hugtökum tengdum net- og upplýsingaöryggi sem enn eru óþýdd. Þetta er sérlega mikilvægt varðandi lagalega túlkun, samninga og aðrar alþjóðlegar skuldbindingar því það getur verið blæbrigðamunur í skilgreiningu hugtaka eftir því hvaða samning er um að ræða og því ekki sjálfgefið að unnt sé að nota sömu þýðingu alls staðar. Það getur því verið góð lausn að Þýðingamiðstöð utanríkisráðuneytisins visti sérstaklega lista yfir slíkar þýðingar, þannig að það sé rekjanlegt hvaðan frumskilgreining hugtaksins er runnin og við hvaða aðstæður þýðingin á við.
Mælikvarði:	Listi yfir mikilvægustu hugtök og þýðingar liggi fyrir 1. október 2015.

Aðgerð 3 – Grunnnám

Markmið:	Net- og upplýsingaöryggi verði hluti tölvutengds námsefnis á öllum skólastigum.
Eigandi:	Mennta- og menningarmálaráðuneytið
Ábyrgð:	Mennta- og menningarmálaráðuneytið
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Netöryggisráð, Samstarfshópur um net- og upplýsingaöryggi, ráðgjafafyrirtæki á sviði net- og upplýsingaöryggis, hópar sem hafa starfað á þessu sviði.
Lýsing:	Net- og upplýsingaöryggi verði hluti tölvutengds námsefnis á öllum skólastigum, frá leikskóla til háskólastigs. Mikilvægt er að öryggið verði hluti af eðlilegri notkun og vitund um tölvutækni.
Mælikvarði:	Fyrsta áætlun um aukna áherslu á net- og upplýsingaöryggi liggi fyrir í október 2015 og verði síðan endurskoðuð árlega.

Aðgerð 4 – Framhaldsnám

Markmið:	Nemendur með grunnpróf frá íslenskum háskólum eigi kost á framhaldsnámi í net- og upplýsingaöryggi sem uppfylli sambærilegar kröfur og grannþjóðir gera til náms á því sviði.
Eigandi:	Innanríkisráðuneytið
Ábyrgð:	Innanríkisráðuneytið
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Mennta- og menningarmálaráðuneytið, háskólar, Netöryggisráð, Samstarfshópur um net- og upplýsingaöryggi, ráðgjafafyrirtæki á sviði net- og upplýsingaöryggis
Lýsing:	Það er mikilvægt að efla tengsl við erlenda háskóla sem bjóða öflugt framhaldsnám og stunda rannsóknir á sviði net- og upplýsingaöryggis. Hér er bæði átt við tengsl við íslenskar háskólastofnanir og að efla möguleika íslenskra stúdenta til framhaldsnáms í þessum greinum.
Mælikvarði:	Fyrir liggi skjalfest samstarf við erlenda háskóla með öflugt framhaldsnám á sviði net- og upplýsingaöryggis eigi síðar en í október 2016.

Aðgerð 5 – Hönnunargildi

Markmið:	Örugg hönnun og persónuvernd verði meðal grunngilda í eflingu íslensks hugbúnaðarstarfs.
Eigandi:	Innanríkisráðuneytið
Ábyrgð:	Verkefnastjórn um upplýsingasamfélagið
Verkefnastjórn:	(ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Atvinnuvega- og nýsköpunarráðuneytið, mennta- og menningarmálaráðuneytið, Netöryggisráð, Samstarfshópur um net- og upplýsingaöryggi, háskólar, samtök og hópar sem vinna á þessu sviði.
Lýsing:	Leggja þarf meiri áherslu á öryggi við hönnun, innkaup, rekstur og notkun hugbúnaðar. Kaupendur geri viðeigandi kröfur um öryggi og vernd upplýsinga. Hvatt verði til aukinnar áherslu á net- og upplýsingaöryggi við þróun hugbúnaðar. Komið verði upp samhæfðum kröfum og viðmiðum varðandi öryggismál sem hægt er að setja inn í samninga við upplýsingatæknifyrirtæki. M.a. fyrir opinbera vefi, hýsingu kerfa, þróun og viðhald kerfa og almenna þjónustu við þau.
Mælikvarði:	Fyrsta útgáfa um „samhæfðar kröfur og viðmið“ fyrir opinbera vefi verði tilbúin 1. september 2015 (upplýsingasamfélagið) og birt á vefnum ut.is Fyrsta útgáfa af „stöðluðum kröfum og viðmiðum“ fyrir kaup á hugbúnaði, þjónustu, rekstri og hýsingu verði tilbúin 1. febrúar 2016.

Aðgerð 6 – Persónuvernd

Markmið:	Hugað verði að alþjóðlegum kröfum og skuldbindingum um persónuvernd við uppbyggingu net- og upplýsingaöryggis hér á landi.
Eigandi:	Persónuvernd
Ábyrgð:	Persónuvernd
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Netöryggisráð, Samstarfshópur um net- og upplýsingaöryggi.
Lýsing:	Huga þarf að persónuvernd við hönnun og innkaup hugbúnaðar, alþjóðlegum kröfum á þessu sviði og þeim breytingum sem þær kunna að taka. Fræðsla og kynningar verði hluti þessa starfs.
Mælikvarði:	Árlegar kynningar á þróun alþjóðlegra viðmiða varðandi persónuvernd í málefnum sem snerta net- og upplýsingaöryggi, sú fyrsta eigi síðar en í nóvember 2015.

Meginmarkmið 2 – Aukið áfallaþol

Aðgerð 7 – Samstarfsvettvangur

Markmið:	Samstarfsvettvangur verði þróaður þar sem fulltrúar frá opinberum aðilum og einkafyrirtækjum geti unnið saman að málum sem varða net- og upplýsingaöryggi.
Eigandi:	Innanríkisráðuneytið
Ábyrgð:	Netöryggisráð
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Samstarfshópur um net- og upplýsingaöryggi, netöryggissveitin CERT-ÍS
Lýsing:	Mikilvægt er að þróaður verði samstarfsvettvangur þar sem hagsmunaaðilar geti unnið saman að málum sem snerta net- og upplýsingaöryggi og til dæmis skipst skjótt á upplýsingum um netógnir og unnið saman til að lágmarka skaða af árásum. Hér getur verið um fleiri en einn vettvang að ræða, t.d. fyrir mismunandi atvinnugreinar. Mögulega þarf að gæta að því að slíkt samstarf brjóti ekki gegn samkeppnislögum og lögum um persónuvernd (ef til dæmis miðla þyrfti upplýsingum um stolnar aðgengisupplýsingar).
Mælikvarði:	Tillögur um samstarfvettvang liggi fyrir eigi síðar en í maí 2015 og fyrsti sameiginlegi fundur samstarfsvettvangsins verði haldinn fyrir lok júní 2015.

Aðgerð 8 – Öryggisviðmið

Markmið:	Val á viðeigandi viðmiðum (stöðlum jafnt sem öðrum) varðandi net- og upplýsingaöryggi.
Eigandi:	Innanríkisráðuneytið
Ábyrgð:	Netöryggisráð
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Samstarfshópur um net- og upplýsingaöryggi, Póst- og fjarskiptastofnun
Lýsing:	Hvaða kröfur skuli vera lögfestar og hvernig skal hátta eftirliti með að þeim sé fylgt, hvaða kröfur ættu að vera valkvæðar og hvernig skal staðið að vottun þeirra. Að auki geta komið ráð sem aðilar sammælast (eða ekki) um að fylgja án þess að nokkur eftirfylgni sé með því. Þetta verkefni tengist verkefni um endurskoðun laga sem varða netöryggismál og aðgerð 6 hér að framan. Skilgreina skal kröfur til birgja varðandi upplýsingaöryggi kerfa og þjónustu.
Mælikvarði:	Netöryggisráð móti tillögur um hvaða leið verði valin til að samræma og innleiða öryggisviðmið, þ.e. hvort og hvað þarf að innleiða í lög og reglugerðir og hvar nóg sé að setja viðmiðunarreglur og beita fræðslu til að auka öryggi. Tillögurnar liggi fyrir 1. október 2015.

Aðgerð 9 – Alþjóðlegt samstarf

Markmið:	Efla og samhæfa þátttöku Íslands í netöryggisstarfi á erlendum vettvangi.
Eigandi:	Innanríkisráðuneytið / Utanríkisráðuneytið
Ábyrgð:	Innanríkisráðuneytið / Utanríkisráðuneytið
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Netöryggissveitin CERT-ÍS, ríkislögreglustjóri, Netöryggisráð, Samstarfshópur um net- og upplýsingaöryggi,
Lýsing:	Málefni Netsins eru alþjóðleg í eðli sínu og mikilvægt að fylgjast vel með þeirri öru þróun sem er á alþjóðavettvangi. Málefni sem snerta net- og upplýsingaöryggi eru víða til umfjöllunar á alþjóðavettvangi, til dæmis hjá stofnunum sem Ísland á aðild að. Má þar nefna norrænt samstarf, Evrópuráðið, Sameinuðu þjóðirnar og NATO. Auk þess er það til umfjöllunar í ýmsu starfi sem Ísland tekur þátt í á vegum Evrópusambandsins. Mikilvægt er að þetta starf sé samhæft þannig að sem best megi nýta samverkandi þætti þess. Ekki síst ber að huga að þeim tækifærum sem felast á sviði norræns samstarfs.
Mælikvarði:	Árleg samantekt fyrir Netöryggisráð um helstu atriði í alþjóðlegu samstarfi á sviði net- og upplýsingaöryggis, sem Ísland tekur virkan þátt í. Fyrsta samantekt verði tilbúin í janúar 2016, byggð á reynslu ársins 2015.

Aðgerð 10 – Traust grunnkerfi

Markmið:	Fjarskiptakerfi og grunnkerfi flutningsneta styðji með skilgreindum áreiðanleika net- og upplýsingakerfi mikilvægra innviða samfélagsins, bæði tengingar innanlands og til útlanda.
Eigandi:	Póst- og fjarskiptastofnun
Ábyrgð:	Póst- og fjarskiptastofnun
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Netöryggisráð, Samstarfshópur um net- og upplýsingaöryggi
Lýsing:	Grunnkerfi landsins byggjast á viðamiklum og flóknum flutnings- og dreifikerfum rafmagns, fjarskipta o.fl. Tryggja þarf skilgreint öryggi allra þessara grunnkerfa. Högun, viðhald og rekstur þessara kerfa þurfa að uppfylla skilgreindar gæðakröfur og öryggisviðmið. Eftirlitsaðilar vinni með rekstraraðilum að því að innleiða og viðhalda skilgreindum kröfum. Jafnframt þarf að tryggja heildaryfirsýn yfir öll grunnkerfin og kortleggja samspil þeirra; t.d. milli raforku og fjarskipta. Stjórnvöld, í samstarfi við rekstraraðila grunnkerfanna, þurfa á hverjum tíma að hafa uppfærða mynd af stöðu og virkni kerfanna, þ.m.t. virka stöðumynd ef þjónusturof verður í þessum kerfum. Löggjöf verði þróuð með þetta í huga og m.a. horft til þróunar á löggjöf innan ESB um þessi mál.
Mælikvarði:	Þróaðir verði mælikvarðar á þjónustutíma kerfanna í samráði við rekstraraðila og niðurstöður birtar almenningi reglulega. Þróun mælikvarða sé lokið í október 2015.

Aðgerð 11 – Stjórnsýslan

Markmið:	Net- og upplýsingaöryggi í stjórnsýslunni verði eflt með aukinni fræðslu, samhæfingu og samvinnu.
Eigandi:	Innanríkisráðuneytið
Ábyrgð:	Verkefnisstjórn um upplýsingasamfélagið
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Netöryggisráð, Samstarfshópur um net- og upplýsingaöryggi.
Lýsing:	Haldin verði árleg námskeið um net- og upplýsingaöryggi fyrir markhópa: Vefstjóra opinberra vefja og tæknifólk sem vinnur við opinber upplýsingakerfi (tölvunarfræðingar/kerfisfræðingar). Komið verði upp og viðhaldið ítarlegu fræðsluefni um net- og upplýsingaöryggi, m.a. á vefnum ut.is. Mat á öryggi verði þáttur í úttekt á opinberum vefjum ríkis og sveitarfélaga sem framkvæmd er annað hvert ár, næst 2015.
Mælikvarði:	Námskeið séu haldin árlega. Net- og upplýsingaöryggi verði fastur liður í úttekt á opinberum vefjum.

Aðgerð 12 – Greining

Markmið:	Helstu ógnir á sviði net- og upplýsingaöryggis verði greindar og mikilvægir innviðir samfélagsins skilgreindir.
Eigandi:	Ríkislögreglustjóri
Ábyrgð:	Ríkislögreglustjóri
Verkefnastjórn:	(ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Netöryggisráð, Samstarfshópur um net- og upplýsingaöryggi.
Lýsing:	Skilgreina þarf með formlegum hætti helstu ógnir á sviði net- og upplýsingaöryggis og hverjir eru mikilvægir innviðir samfélagsins í því sambandi. Þetta er lögum samkvæmt hlutverk ríkislögreglustjóra.
Mælikvarði:	Greining liggi fyrir í júlí 2015 og verði endurskoðuð/yfirfarin árlega. Skilgreining á mikilvægum innviðum liggi fyrir í júní 2015.

Aðgerð 13 – Vernd innviða

Markmið:	Geta netöryggissveitar til verndar og aðstoðar mikilvægra innviða samfélagsins verði efld og virk allan sólarhringinn alla daga ársins. Sérstök áhersla verði lögð á fjarskipta-, veitu- og fjármálafyrirtæki og þau kerfi sem eru mikilvæg vegna flugsamgangna við umheiminn.
Eigandi:	Innanríkisráðuneyti
Ábyrgð:	Netöryggissveitin
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Póst- og fjarskiptastofnun, Netöryggisráð, Samstarfshópur um net- og upplýsingaöryggi.
Lýsing:	Miðað er við að netöryggissveitin verði flutt til almannavarnadeildar ríkislögreglustjóra og verði *Netöryggissveit almannavarna*. Sveitin geti brugðist við atvikum allan sólarhringinn, alla daga vikunnar og starfssvið sveitarinnar hafi verið víkkað þannig að auk fjarskiptafyrirtækja þá taki það einnig til stjórnvalda og annarra mikilvægra innviða samfélagsins sem geta verið viðkvæmir gagnvart netárásum, einkum orku-, hitaveitu- vatnsveitu- og fráveitufyrirtæki, fjármalafyrirtæki og fyrirtæki sem hafa umsjón með alþjóðaflugi og flugöryggi. Þetta krefst meðal annars beitingu sérhæfðs greiningarbúnaðar í samvinnu við þessa aðila og samvinnu um æfingar og fleira. Þar til ný lög hafa verið sett um starfsemi sveitarinnar mun hún skipuleggja vernd innviða innan þess ramma sem gildandi lög heimila.
Mælikvarði:	Skipulag samvinnu við skilgreinda aðila mikilvægra innviða samfélagsins liggi fyrir og sé orðið virkt 1. september 2015. Endurskoðað skipulag byggt á nýjum lögum sé orðið virkt 1. mars 2016.

Aðgerð 14 – Viðbragð

Markmið:	Viðbragðsáætlanir vegna netógna verði þróaðar og prófaðar með æfingum, með sérstakri áherslu á mikilvæga innviði samfélagsins.
Eigandi:	Almannavarnadeild ríkislögreglustjóra
Ábyrgð:	Netöryggissveitin
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Netöryggisráð, Samstarfshópur um net- og upplýsingaöryggi.
Lýsing:	Almannavarnadeild ríkislögreglustjóra hefur unnið viðbragðsáætlun vegna alvarlegra netárása þar sem reynsla er nýtt af atburðum sem hafa reynt á innviði samfélagsins. Útvíkka þarf áætlun þannig að hún taki til allt frá smáum atvikum sem Netöryggissveitin hefur fengist við til stórra og alvarlegra atvika þar sem reynsla almannavarnadeildar er mikil.
Mælikvarði:	Frumútgáfa viðbragðsáætlana verði þróuð frekar og þeirri endurskoðun lokið í júní 2015. Þær verði endurskoðaðar/yfirfarnar á ný fyrir árslok og eftir það fari fram endurskoðun eigi sjaldnar en árlega. Prófun með æfingum fari fram eigi sjaldnar en árlega.

Meginmarkmið 3 – Bætt löggjöf

Aðgerð 15 – Bætt löggjöf

Markmið:	Íslensk löggjöf verði endurskoðuð þannig að tryggt sé að hún sé í samræmi við alþjóðlegar skuldbindingar og geri það mögulegt að glíma við netógnir með sambærilegum hætti og tíðkast í grannlöndum okkar. Jafnframt sé löggjöfin þannig úr garði gerð að hægt sé að glíma við netógnir með sambærilegum hætti og aðrar ógnir í samfélaginu, eftir því sem við á.
Eigandi:	Innanríkisráðuneytið
Ábyrgð:	Innanríkisráðuneytið
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Netöryggisráð, Samstarfshópur um net- og upplýsingaöryggi.
Lýsing:	Meðal þess sem þarf að rýna með tilliti til hugsanlegra breytinga á íslenskri löggjöf er samningur gegn tölvubrotum (Cybercrime convention), Evrópusambandstilskipun (NIS directive) og huga þarf að viðeigandi tilkynningarskyldu öryggisatvika (þannig að aðilar sjái sér hag í því að tilkynna jafnframt því að vera skuldbundnir til þess), nýtingu skýjatækni og túlkun alþjóðlegrar lögsögu á Netinu.
Mælikvarði:	Drög að frumvarpi/frumvörpum verði tilbúin til kynningar fyrir ráðherra í árslok 2015. Lagabreytingar taki gildi eigi síðar en 2016.

Meginmarkmið 4 – Traust löggæsla

Aðgerð 16 – Löggæsla

Markmið:	Hæfni lögreglu til að fást við glæpi tengda net- og upplýsingaöryggi verði bætt með aukinni þekkingu, reynslu ásamt efldri innlendri og alþjóðlegri samvinnu og þeim búnaði sem til þarf.
Eigandi:	Innanríkisráðuneyti
Ábyrgð:	Ríkislögreglustjóri
Verkefnastjórn:	(Ákveðið af ábyrgðaraðila að höfðu samráði við lykilaðila)
Aðrir lykilaðilar:	Netöryggisráð, Samstarfshópur um net- og upplýsingaöryggi.
Lýsing:	Mótuð verði „endurmenntunaráætlun“ til a.m.k. tveggja ára þar sem skipulagt er hvernig uppbygging þekkingar eigi að fara fram. Hún feli í sér hvers konar námskeið, æfingar, kynnisferðir og beina ráðgjöf/leiðsögn fyrir þann „kjarnahóp“ innan lögreglunnar sem bera mun hitann og þungann af verkefnum á þessu sviði. Við mótun þessarar endurmenntunaráætlunar verði tekið mið af löggæsluáætlun þannig að aðgerðin falli einnig að þeirri áætlun.
Mælikvarði:	Endurmenntunaráætlun verði útbúin eftir samhæfingu við aðra menntun lögreglunnar, áætlun verði tilbúin eigi síðar en í júní 2015. Árleg endurskoðun áætlunar í ljós reynslunnar fari fram 15. janúar 2016.