Net- og upplýsingaöryggi
Stefnan og aðgerðir í netöryggismálum

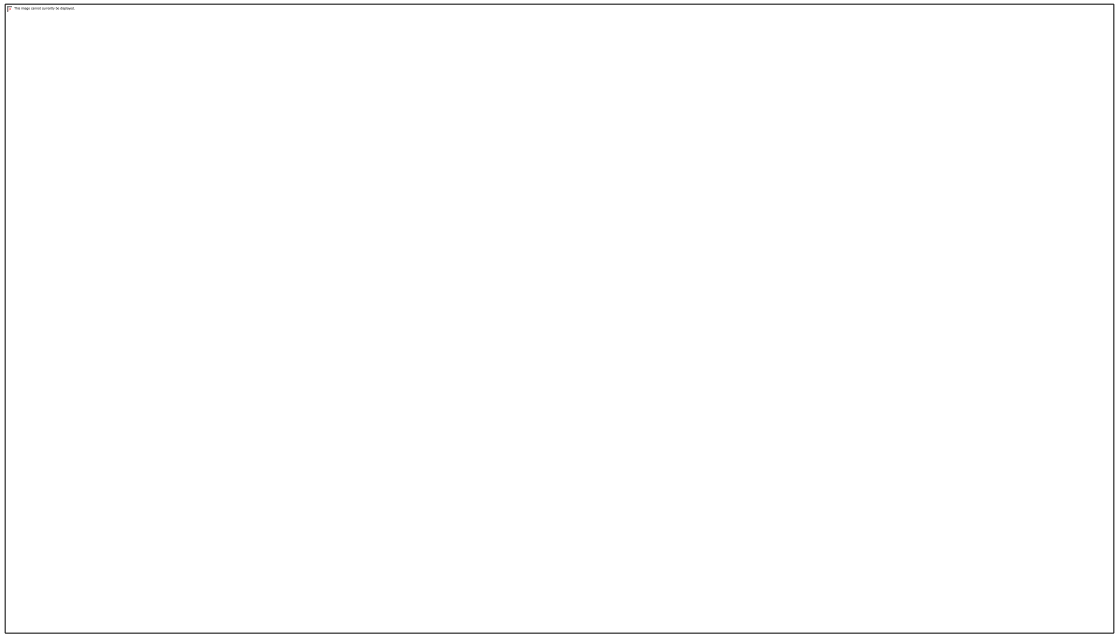
Kynning á UT deginum 2015 – útgáfa til birtingar á vef

Sigurður Emil Pálsson

INNANRÍKISRÁÐUNEYTIÐ

Kynning á vegum Netöryggisráðs

(sjá frétt IRR 5.11.2015)



Anna Borgþórsdóttir Olsen, fulltrúi fjármála- og efnahagsráðuneytis,
Hrafnkell V. Gíslason, forstjóri Póst- og fjarskiptastofnunar,
Ólafur Egill Jónsson, fulltrúi atvinnuvega- og nýsköpunarráðuneytis,
Íva Sigrún Björnsdóttir, fulltrúi mennta- og menningarmálaráðuneytis,
Sigurður Emil Pálsson, sérfræðingur í innanríkisráðuneytinu og formaður ráðsins,
Alma Tryggvadóttir, skrifstofustjóri upplýsingaöryggissviðs Persónuverndar,
Vera Sveinbjörnsdóttir, lögfræðingur í innanríkisráðuneytinu,
Guðbjörg Sigurðardóttir, sérfræðingur í innanríkisráðuneytinu,
Jónas Haraldsson, fulltrúi utanríkisráðuneytis.
Einnig eru í ráðinu þeir **Jón F. Bjartmarz,** fulltrúi ríkislögreglustjóra og **Stefán Snorri Stefánsson**, fulltrúi netöryggissveitar (CERT-IS).

http://www.innanrikisraduneyti.is/frettir/fyrsti-fundur-netoryggisrads-haldinn-i-vikunni

Stefna kynnt í ríkisstjórn, 28. apríl 2015
(sjá frétt á vef IRR sama dag)

Starfshópurinn sem vann að mótun stefnunnar:

- Sigurður Emil Pálsson, sérfræðingur innanríkisráðuneytinu
- Guðbjörg Sigurðardóttir, skrifstofustjóri upplýsingasamfélagsins, innanríkisráðuneytinu
- Páll Heiðar Halldórsson, sérfræðingur, innanríkisráðuneytinu
- Jón F. Bjartmarz, yfirlögregluþjónn, embætti ríkislögreglustjóra
- Ágúst Finnsson, sérfræðingur, embætti ríkislögreglustjóra
- Hrafnkell V. Gíslason, forstjóri Póst- og fjarskiptastofnunar
- Stefán Snorri Stefánsson, hópstjóri CERT-ÍS, Póst- og fjarskiptastofnun
- Jónas Haraldsson, sérfræðingur, utanríkisráðuneytinu.
- Þorsteinn Arnalds, sérfræðingur, Persónuvernd

Net- og upplýsingaöryggi
Hvers vegna?

- Skiptir það máli?
- Fyrir hverja?
- Af hverju?
- Um hvað snýst það?
- Hvers vegna ætti ég að eyða mínum tíma í að gera eitthvað að vandamáli sem er ekki vandamál fyrir mig?
- Ef það er vandamál, er það þá ekki vandamál einhvers annars, ekki mín?

Aukið verðmæti í upplýsingum

- Glæpamenn sækjast eftir upplýsingum, sem oft geta virst ómerkilegar við fyrstu sýn, geta nýst við framkvæmd glæpa
- Samtvinnun ólíkra upplýsinga getur skapað mikil verðmæti
- Með samtengingu geta upplýsingar sem eru einar sér ekki persónugreinanlegar orðið persónugreinanlegar
- Njósnir, t.d. á vegum erlendra ríkja. Mikið af hugverkaauði ríkja getur horfið og skapað efnahagsvanda, gjaldþrot og atvinnuleysi.
- Líkja má árásum/njósnum við **botnvörpuveiðar** annars vegar & **hnitmiðaðar árásir/veiðar** hins vegar

Veislan er búin, nú þarf að borga!

- Alla þjónustu á **Netinu** þarf að greiða með einhverjum hætti.
- Mikið hefur verið fjárfest í fyrirtækjum eins og *Google* og *Facebook*.
- Tekjulind þeirra eru gögn viðskiptavina og viðskiptaskilmálar þeirra hafa leitt til rannsókna og málaferla
- Notendur þurfa að geta tekið upplýsta ákvörðun um hver af þeirra gögnum séu söluvara.

Áfallaþol

Áfallaþol hvers?

- Tækni?
- Þjónustu?
- Trausts?

Ógnir tækninnar

- Stórtækari **söfnun**, **samkeyrsla** og **greining** upplýsinga gefur möguleika á víðtækara eftirliti með fjölda manns en nokkru sinni hefur sést (gera „1984“ að barnagælu og STASI að kórdrengjum).
- Eðlisbreyting á **skipulagðri glæpastarfsemi**
  - **Lénsskipulag mafíunnar** að víkja fyrir **nútíma verkskiptu markaðsskipulagi**, með einyrkjum sem fela sig með dulritunartækni Netsins
- Sé breskt mat á tjóni af völdum tölvutengdra glæpa yfirfært á Ísland og gert ráð fyrir að tjón á íbúa sé það sama, þá ætti tjón hérlendis að nema milljörðum króna á hverju ári.

Samskiptablekking - *(Social engineering)*

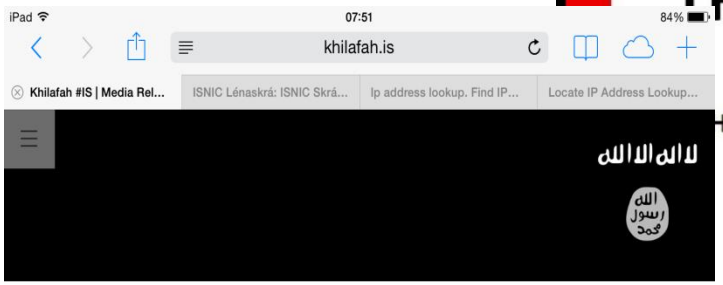
- Öflugt verkfæri tölvuþrjóta – háþróuð iðn
- Megum ekki svipta fórnarlömb sjálfsvirðingu
- Vel skipulagðar hnitmiðaðar árásir geta falið í sér:
  - Greiningarvinnu
  - Velja hentug fórnarlömb
  - Greina fórnarlömbin (fullt af gagnlegum upplýsingum á glámbekk)
  - Búa tii sannfærandi falskt gervi fórnarlamba, fá upplýsingar
  - Setja inn bakdyr og eigin notandaaðgang
  - Bíða í meir en eitt ár
  - Hefja aðgerð, selja upplýsingar eða selja aðgengi að fórnarlambi.

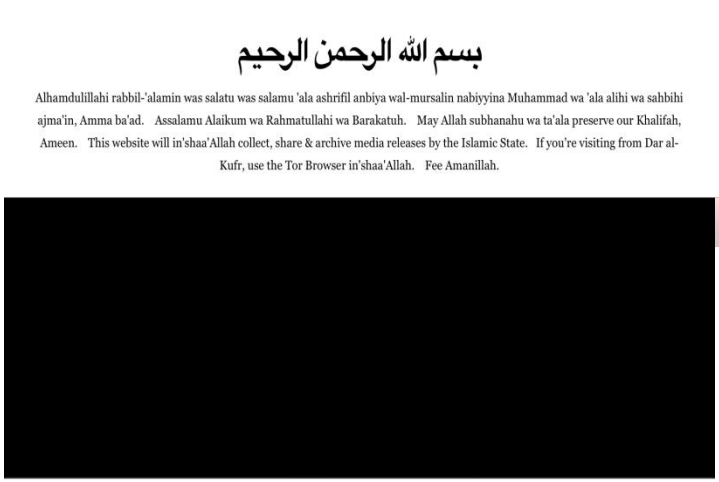
Dæmi um notkun samskiptablekkingar

- Sjarmerandi maður sem labbaði út úr ABN Amro bankanum í Belgíu árið 2007
  með 21 M € virði af gimsteinum – út á persónutöfra eina saman!
- Orðrómur á Twitter 2013 um árás á Hvíta húsið og Obama hefði særst, verðbréf tóku að falla á innan við mínútu og náðu lægð á 3 mínútum (þegar grunur um fals vaknaði)

Staða hérlendis?

- Blómleg nýting – margar góðar afurðir
- Öryggissérfræðingar lengi bent á hættumerki:
  - Lítil öryggistengd menntun
  - Menning: Öryggið aftast í stað þess að vera með frá byrjun
  - Skortur á öryggisvitund, áhættugreiningu og skipulagi
  - Skortur á þekkingu, hjá almennum notendum og stjórnendum
- Þurfum að:
  - Bæta vitund
  - Bæta menntun og þekkingu
  - Bæta löggjöf
  - Geta unnið saman (geta sungið í kór, ekki bara hópur einsöngvara)
  - Hafa samstarfsvettvang
  - Hafa varnir (þ.á.m. löggæslu), viðbúnað og prófanir





Heimsfræg dæmi af íslenskum lénum!

(þótt efni hafi ekki verið íslenskt)

INNANRÍKISRÁÐUN

Til varnar - Eru nýjungar nýjungar?

- Er eitthvað nýtt að við þurfum að taka í notkun varasama tækni?
- Tókum hnífinn í notkun fyrir rúmlega 2 milljónum ára, til góðs og ills.

„Nýir tímar – ný hugsun!“

- Tækni síðustu ára hefur gerbreytt lífi okkar
- Ung kynslóð er nú að vaxa upp sem skynjar heiminn með allt öðrum hætti en sú eldri
- Hún notar tæki sem gera henni mögulegt að framkvæma hluti sem voru áður ógerlegir
- Sá eða sú sem nær ekki tökum á þessari nýju tækni verða brátt eins og ólæs og óskrifandi
- Tími skapandi einstaklinga í þjóðfélagi skapandi greina er runninn upp!

Ofangreindur texti er nútímalegur og gæti átt við netnotkun, hann vísar þó til texta úr ritinu Foto Auge frá 1929, þar sem fúturistar og dadaistar voru að lýsa áhrifum ljósmyndunar og ritvéla á menningu samtímans. Hver tími þarf að glíma við sínar nýjungar!

Vandamál lögsögu

- Kemur þjónustuveitandi **til okkar** á Netinu eða **förum við til hans**?
- Ef þjónustuveitandi er í **skýjunum**, hvar á hann þá lögsögu?
- Hvernig ber að túlka þegar gögn eru sótt til annars lands, er **farið inn** í lögsögu þess eða er um **borðtennis** að ræða?

Persónuvernd
og barátta gegn glæpum

- **Persónuvernd** og **öryggi gegn glæpum**, ekki andstæður, tvær mismunandi hliðar sama markmiðs
- Hversu langt er rétt að ganga til að tryggja að til sé **rafræn rekjanleg slóð** svo unnt sé að **rannsaka glæpi**, án þess að það sé nýtt til **víðtæks eftirlits**?
- Viðmið verða að vera almenn og þau þurfa einnig að setja stjórnvöldum takmörk.

Hversu háð erum við tækninni?
Hvernig notum við hana?
Hversu viðkvæm erum við ef hún brestur?

Til hvers er bíllinn?

- Ætlum við að nota bílinn í **staðinn fyrir að ganga**?
- …eða
- Ætlum við að nota bílinn til að **komast lengra**?

Altæk öryggishugsun

- Fólk er ótrúlega duglegt að hrúga lásum á **útidyrnar** - og skilja síðan **gluggana** eftir galopna (ónefndur íslenskur sérsveitarmaður)
- Hvers vegna brjótast inn í tölvukerfi, þegar það er svo miklu einfaldara að láta fólk hleypa sér þangað! (ónefndur alþjóðlegur hakkari)

Stefnan - 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.

Aðgerðir snúast um samvinnu og samhæfingu fyrst og fremst!

Meginmarkmið

- **Efld geta**. Almenningur, fyrirtæki og stjórnvöld búi yfir þeirri þekkingu, getu og tækjum sem þarf til að verjast netógnum.
- **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.
- **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.
- **Traust löggæsla**. Lögregla búi yfir eða hafi aðgang að faglegri þekkingu, hæfni og búnaði til að leysa úr málum er varða net- og upplýsingaöryggi.

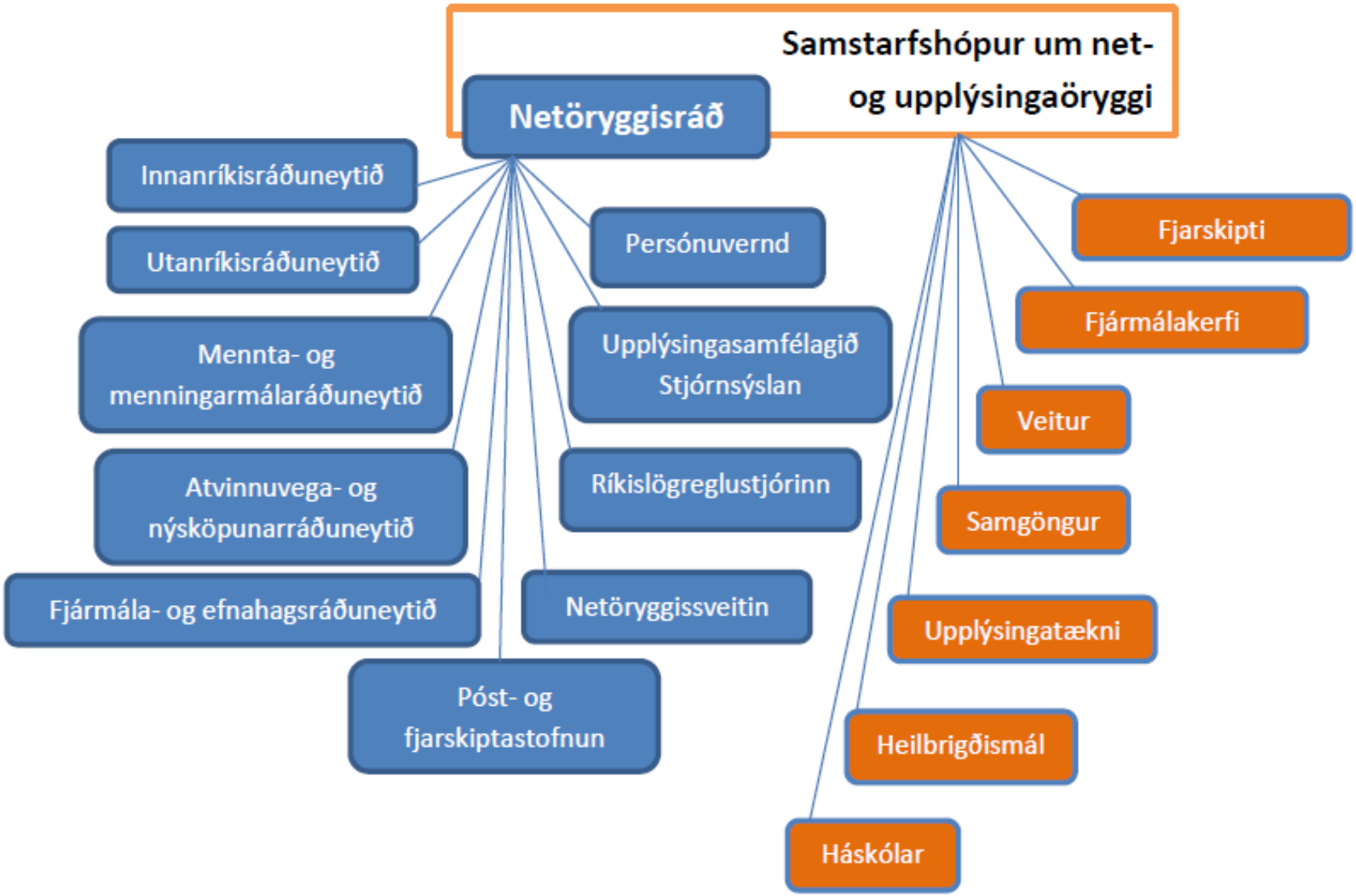
Netöryggisráð og samráðshópur

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.


Samstarfshópur um net- og upplýsingaöryggi
Netöryggisráð
Innanríkisráðuneytið
Utanríkisráðuneytið
Mennta- og menningarmálaráðuneytið
Atvinnuvega- og nýsköpunarráðuneytið
Fjármála- og efnahagsráðuneytið
Póst- og fjarskiptastofnun
Persónuvernd
Upplýsingasamfélagið Stjórnsýslan
Ríkislögreglustjórinn
Netöryggissveitin
Fjarskipti
Fjármálakerfi
Veitur
Samgöngur
Upplýsingatækni
Heilbrigðismál
Háskólar

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.

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.

Staða Eistlands

- Hafa verið leiðandi hlutverki vinnu á grunni samnings Evrópuráðsins gegn netglæpum (*Convention on cybercrime*), helsta alþjóðlega samnings á þvi sviði
- Hýsa þekkingasetur NATO á sviði net- og upplýsingaöryggis.
- Hafa þróað rafrænt skjalaumhverfi fyrir opinbera stjórnsýslu („X-Road“) sem aðrar þjóðir (t.d. Finnar, Bretar) eru að eða hafa tekið upp

- **Eru ein sparsamasta þjóð Evrópu samkvæmt hagtölum, af hverju eyða svona miklu fé í net- og upplýsingaöryggi, þar á meðal kerfi fyrir örugga rafræna umsýslu opinberra gagna?**
- **Svar: Af því þeir hafa ekki efni á að gera það ekki!**

Með öryggi til sóknar!

- Reisum skýjakjúfa, ekki bara skýjaborgir!
- Gerum öryggi að forgangskröfu í hönnun og notkun hugbúnaðar
- „Security by design“ og „Privacy by design“
- Tækniþekking og rekjanlegt öryggi eru stoðir sem ýmsar grannþjóðir okkar ætla að byggja efnahagslega sókn á (þetta eru þættir sem ráðgjafafyrirtæki líta til, t.d. við val á staðsetningu gagnavera)
- Góð samvinna á grunni starfs Upplýsingasamfélagsins
- Það er öfundsverð auðlegð að því fyrir önnur lönd að hafa marga lykilfulltrúa opinberra stofnana saman í einum sal!