

Niðurstöður úttektar Oxford-háskóla og efling netöryggis

SAMGÖNGU- OG SVEITASTJÓRNARRÁÐUNEYTIÐ
30. APRÍL 2018

Yfirlit samantektar

Úttekt Oxford-háskóla á stöðu netöryggis hérlendis	1
Helstu niðurstöður mats á stöðu netöryggis.....	2
Helstu ráðleggingar Oxford-skýrslu í kjölfar stöðumats	3
Umgjörð netöryggismála á Íslandi	4
Uppbygging netöryggis – áhersla á undanfögnu ári	5
Alþjóðlegt samstarf	7
Frumvarp um bætt netöryggi	9
Grein samgöngu- og sveitarstjórnarráðherra um vaxandi netógnir	10

Úttekt Oxford-háskóla á stöðu netöryggis hérlendis

Oxford-háskóli var fenginn til að gera úttekt á stöðu netöryggis í íslensku samfélagi sumarið 2017, þar sem beitt var líkani sem háskólinn hefur þróað til að meta slíka stöðu. Fulltrúar Oxford-háskóla áttu fundi með ýmsum aðilum í samfélaginu um netöryggis-tengd málefni. Í kjölfarið skilaði háskólinn skýrslu með ítarlegri lýsingu á stöðu netöryggis í ýmsum þáttum samfélagsins og mati á stöðunni út frá líkani háskólans ásamt 120 ráðleggingum til úrbóta. Ráðuneyti og viðeigandi stofnanir hafa skipt á milli sín ábyrgð á því að bregðast við ráðleggingunum. Það er mikilvægt að þeim sé fylgt vel eftir, enda er rafræna innviði að finna í flestum kimum nútímasamfélags og mikilvægt að tryggja að þjónustan sé sem öruggust og njóti trausts. Fyrirhugað er að Oxford-háskóli endurmeti stöðu síðar, þannig að unnt sé að meta árangur þeirra aðgerða sem ráðist verður í á grunni ráðlegginganna.

Háskólinn í Oxford framkvæmir úttekt á stöðu netöryggismála



Frá fundinum í Safnahúsinu við Hverfisgötu. Fremst f.v., fulltrúar frá netöryggissetrinu í Oxford: María Bada, Michael Goldsmith prófessor og Carolin Weisser. Fyrir aftan eru frá samgöngu- og sveitarstjórnarráðuneytinu f.v. Ragnhildur Hjaltadóttir, Guðbjörg Sigurðardóttir, Vigdís Ósk Háslar Sveinsdóttir og Sigurður Emil Pálsson.

Frétt samgöngu- og sveitarstjórnarráðuneytis frá 23. júní 2017 á vef Stjórnarráðsins um úttekt Oxford-háskóla á stöðu netöryggis hérlendis.

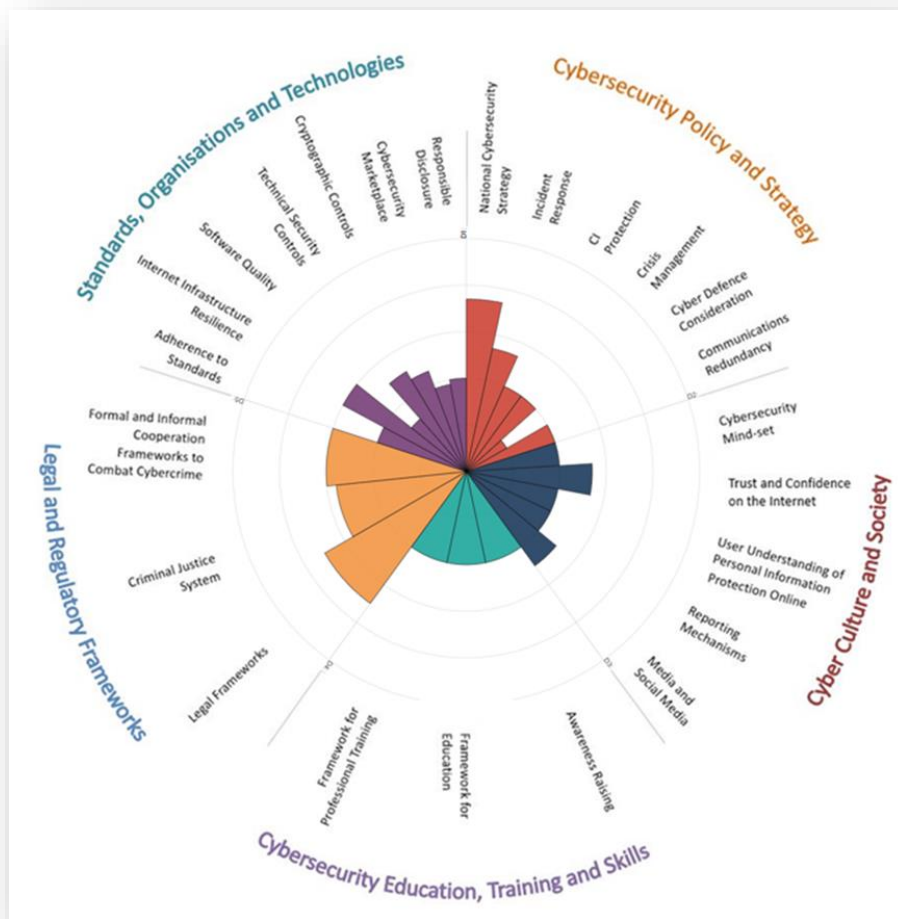
HELSTU NIÐURSTÖÐUR MATS Á STÖÐU NETÖRYGGIS

Í líkani Oxford-háskóla er staða netöryggis metin út frá 5 víddum, en þær eru:

1. *Netöryggisstefna og skipulag* (e. *Cybersecurity Policy and Strategy*)
2. *Netöryggismenning og samfélag* (e. *Cyber Culture and Society*)
3. *Netöryggismenntun, þjálfun og hæfni* (e. *Cybersecurity Education, Training and Skills*)
4. *Lagalegt umhverfi* (e. *Legal and Regulatory Framework*)
5. *Staðlar, skipulag og tækni* (e. *Standards, Organisations and Technologies*)

Innan hversrar víddar eru síðan nokkrir þættir metnir. Ástand getur verið metið sem (a) **Start-up**, að ástand sé á frumstigi; (b) **Formative**, að því hafi miðað á leið en sé þó enn í mótun; (c) **Established**, að ástand sé komið á legg og starfhæft; (d) **Strategic**, að farið sé að forgangsraða þáttum í heildstæðu skipulagi og að lokum (e) **Dynamic**, að skipulag sé kvikt og geti aðlagast skjótt að breyttu umhverfi og nýjum ógnum.

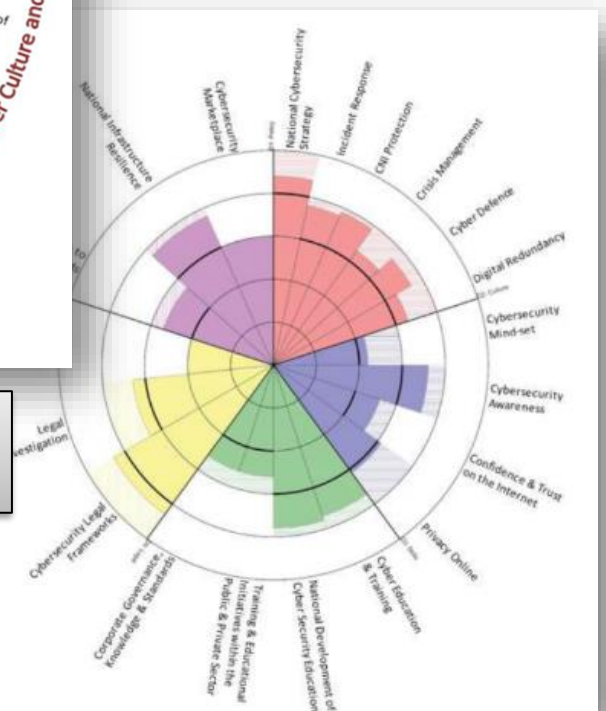
Hér að neðan má sjá í skifuriti niðurstöður fyrir Ísland (vinstra megin) og fyrir Bretland (hægra megin og neðar).



Þeir þættir sem standa best samkvæmt úttekt Oxford eru netöryggisstefnan og lagaumhverfi. Netvarnir sem hluti varnarmála var veikasti þátturinn, en fram kom hjá skýrsluhöfundum að þeir voru í vafa hvort hafa bæri þennan þátt með í ljósi aðstæðna hérlendis. Þátturinn var að lokum hafður með, enda ekki unnt að líta fram hjá ógnum á þessu sviði. Skipulag til að tryggja gæði hugbúnaðar þótti einnig veikt.

Svipað mynstur er í hlutfalli á milli mismunandi þátta í Bretlandi og á Íslandi, en Bretland er í flestum þáttum þrepi ofar.

Sjá má kynningu ritstjóra skýrslunnar, Dr. Maria Bada, á helstu niðurstöðum úttektarinnar á *Deigi upplýsingatækninnar*, 30. nóv. 2017 (Upptökur: [Kynning á aðdraganda verkefnis og á fyrirlesaranum, Mariu Bada, fyrirlestur Mariu Bada](#) (á ensku); [glærur kynningar Mariu Bada](#))



HELSTU RÁÐLEGGINGAR OXFORD-SKÝRSLU Í KJÖLFAR STÖÐUMATS

(Yfirlitið er ekki tæmandi og til að fá glögga mynd af ráðleggingunum verður að lesa þær í samhengi við umfjöllun um tilsvarendi efni í skýrslunni, þessari samantekt er einungis ætlað að gefa yfirlit yfir ráðleggingarnar)

1 - Netöryggisstefna og skipulag

- Tryggja fjárveitingar og eftirfylgni, huga að innri ógnum auk ytri.
- Skilgreina mikilvæga innviði, viðbragðsáætlanir, æfingar
- Efla samvinnu, upplýsingaflæði, leiðbeiningar (t.d. GDPR, NIS, varaleiðir fjarskipta), tilkynningagátt.
- Lagalegar og samningsbundnar skyldur varðandi varnarmál. Efla rannsóknasamvinnu (t.d. með klösum) á sviði netvarna, kanna gildi aukinnar samvinnu v. öndvegissetur Atlantshafsbandalagsins í Tallinn.

2 - Netöryggismenning og samfélag

- Vitundarvakning, upplýsingar, hnitmiðuð fræðsla fyrir viðkvæma markhópa.
- Áhersla á persónuvernd í leiðbeiningum, kerfum og þjónustu, persónuvernd sem sjálfgefin eigind. Þjónustuveitendur upplýsi um öryggi þjónustu. Próa reglur um upplýst samþykki notenda vegna söfnunar persónuupplýsinga. Hvetja til notkunar vefstaðla sem verndi notendur. Koma á sameiginlegri tilkynningagátt vegna netatvika og afbrota og stuðla að notkun hennar.
- Stuðla að upplýstri umræðu um netöryggi í fjölmiðlum og samfélagsmiðlum.

3 - Netöryggismenntun, þjálfun og hæfni

- Þjóðaráttak til betri vitundar um netöryggi, samhæfð dreifing ráðlegginga, stofnun netöryggisgáttar til dreifingar upplýsinga, auk sjálfsnámsgáttar. Fræðsla og ráðleggingar um netöryggi fyrir stjórnábyrgð. Sérstök fræðsla fyrir stjórnendur. Árangur metinn reglulega og nýttur til að leggja áherslu á það sem upp á vantar.
- Bætt menntun þeirra sem bera ábyrgð á menntun og fræðslu.
- Stefnt að því að netöryggi verði kennt sem fag á háskólastigi, ekki bara sundurlaus námskeið. Þetta sé gert í samvinnu við erlenda háskóla og jafnframt sé samvinna við þá um að nemendur eigi greiðan aðgang að framhaldsnámi erlendis. Efling þekkingar og áhuga með ýmsum atburðum: Námskeiðum, fyrirlestrum og keppnum. Efling rannsókna (ekki bara bundin við háskóla). Menntastefna á sviði netöryggis sé unnin í viðtæku samráði og tengd netöryggisstefnu.
- Almenn netöryggisnámskeið og þjálfun sé í boði, endurmenntun og síðan samræmd vottunarkerfi fyrir þá þekkingu og hæfni sem aflað hefur verið. Efla atvinnumarkað á sviði netöryggis og halda skrá yfir netöryggissérfræðinga. Próa matskerfi til að meta árangur námskeiða, þjálfunar, fræðslu og fyrirlestra, vefmiðlunar og vottaðrar hæfni.

4 - Lagalegt umhverfi

- Fylgjast með því að lagaumhverfi sé í samræmi við alþjóðlegar kröfur, stefnur og gildi og það dugi til að halda uppi lögum og reglum, einnig í sakamálum sem krefjast alþjóðlegrar samvinnu. Jafnframt að unnt sé að bregðast við örrí þróun á þessu sviði.
- Gæta þess að gildi varðandi mannréttindi, vernd barna, neytendavernd og höfundarrétt endurspeglar með viðeigandi hætti í lagaumhverfi og unnt sé að bregðast við örrí þróun á þessum sviðum.
- Tryggja að unnt sé að rannsaka flókin netbrot og að rannsakendur hafi hlotið viðeigand menntun og þjálfun, m.a. með myndun rannsóknateyma á þessu sviði.
- Efla menntun saksóknara og dómara á sviði netglæpa og persónuverndar. Koma á formlegu skipulagi miðlunar upplýsinga og reynslu á milli saksóknara og dómara.
- Safna og greina reglulega gögn um afbrot tengd Netinu, rannsóknir þeirra, ákæru og dóma.
- Efla óformlegt samstarf löggæslu, Persónuverndar, Póst- og fjarskiptastofnunar (CERT-IS) og netþjónustuveitenda, þannig að samskiptaleiðir séu skýrar.

5 - Staðlar, skipulag og tækni

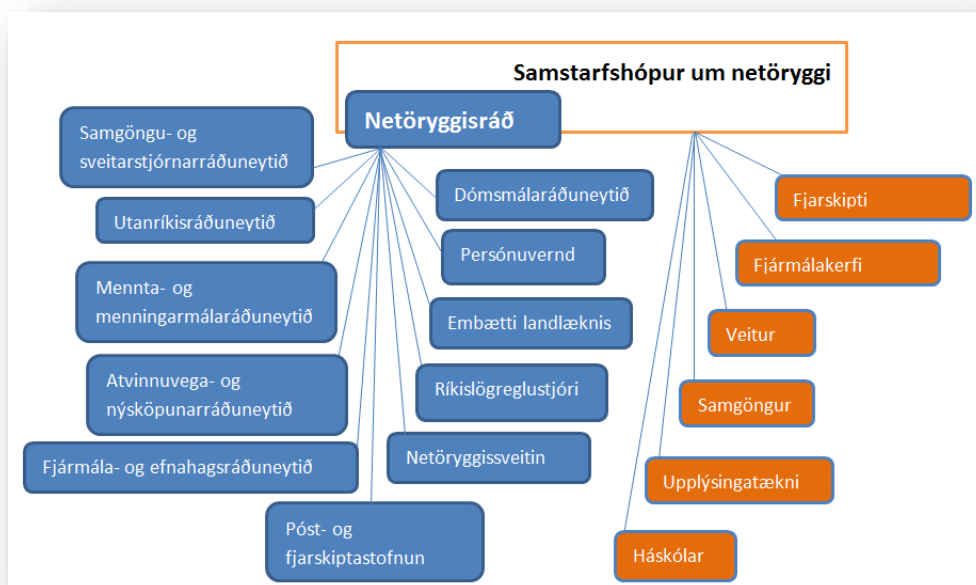
- Koma á viðmiðum (m.a. byggðum á stöðlum) varðandi þróun og kaup hugbúnaðar. Stjórnvaldi sé falið að hafa eftirlit með þessu og meta árangur. Efla umræðu um hvernig slík viðmið geti eftir öryggi mikilvægra innviða.
- Greina áfallaþol mikilvægra innviða Netsins á Íslandi í samvinnu við rekstraraðila og greina hvar eru veikir punktar
- Próa og dreifa lista yfir öruggt tölvu- og netumhverfi og deila með hagsmunaaðilum. Skilgreina gæðakröfur og þar á meðal kröfur um uppfærslur. Leggja áherslu á öruggar lausnir og sem uppfylla alþjóðlega staðla og viðurkennt verklag. Fylgjast með og meta þann hugbúnað sem er í notkun.
- Hvetja til þróunar og notkunar dulritunarlausna til verndar á gögnum í geymslu og flutningi, samkvæmt alþjóðlegum stöðlum og viðmiðum. Efla vitund um örugg samskipti (t.d. dulritaðan tölvupóst) og hvetja til notkunar lausna til að efla öryggi samskipta við netþjóna (t.d. SSL eða TLS). Próa reglur á þessu sviði og endurmeta þær reglulega.
- Hugsa að því að styrkja þróun netöryggislausna út frá þörfum íslensks markaðar. Tryggja að þróun hugbúnaðar taki mið af netörygiskröfum í alþjóðlegum stöðlum og viðmiðum og efla markað með nettryggingar.
- Próa skipulag varðandi ábyrga miðlun upplýsinga um veikleika. Hvetja hugbúnaðar- og þjónustuveitendur til upplýsingamiðlunar um veilir. Hvetja til miðlunar meðal rekstraraðila mikilvægra innviða um tæknilega eiginleika netveikleika. Birting greiningar á tæknilegum eiginleikum netveikleika.

Umgjörð netöryggismála á Íslandi

Samgöngu- og sveitarstjórnarráðuneytið fer, samkvæmt forsetaúrskurði, með málefni er varða netöryggi og fór innanríkisráðuneytið áður með þessi mál. Dómsmálaráðuneyti fer með mál er lúta að afbrotum tengdum Netinu og utanríkisráðuneytið fer með formleg tengsl við önnur ríki, t.d. vegna netvarna.

Um fjarskipti gilda lög nr. 81/2003 og Póst- og fjarskiptastofnun fer með framkvæmd fjarskiptamála. Netöryggissveitin, CERT-IS, heyrir undir Póst- og fjarskiptastofnun og á í mjög nánu samstarfi við aðrar norrænar þjóðarnetöryggissveitir. Netöryggissveitin var stofnuð með reglugerð nr. 475 árið 2013, með stoð í lögum um fjarskipti nr. 81/2003. Sveitinni ber lögum samkvæmt að sinna fjarskiptafyrirtækjum og er lagt á þau ákveðið gjald til að standa straum af kostnaði vegna þjónustu sveitarinnar. Sveitinni er heimilt að gera þjónustusamninga við aðra.

Starf stjórnvalda á sviði netöryggis byggir á stefnu um net- og upplýsingaöryggi sem þáverandi innanríkisráðherra kynnti ríkisstjórn og Alþingi vorið 2015. Stefnunni fylgdi jafnframt aðgerðaáætlun til þriggja ára. Stefnan var mótuð að undangengnu víðtæku samráði og var einnig höfð hliðsjón af stefnum grannríkja á sviði netöryggismála. *Netöryggisráð* var sett á stofn í nóvember 2015 og er það skipað fulltrúum ráðuneyta og stofnana sem sinna netöryggistengdum málum. Það hefur umsjón með framkvæmd stefnunnar, samhæfir aðgerðir og miðlar upplýsingum. Ráðið sem slíkt hefur ekki boðvald í netöryggistengdum málum. Í Netöryggisráði sitja nú fulltrúar frá samgöngu- og sveitarstjórnarráðuneyti, dómsmálaráðuneyti, utanríkisráðuneyti, fjármála- og efnahagsráðuneyti, mennta- og menningarmálaráðuneyti, atvinnuvega- og nýsköpunarráðuneyti, ríkislögreglustjóra, Persónuvernd, Embætti landlæknis, Póst- og fjarskiptastofnun og Netöryggissveitinni. Netöryggisráð hefur reynst vera góður vettvangur upplýsingamiðlunar, samhæfingar og samstarfs.



Í stefnunni er jafnframt gert ráð fyrir að starfandi sé *Samstarfshópur um net- og upplýsingaöryggi* og að hann sé skipaður fulltrúum Netöryggisráðs og fulltrúum helstu hagsmunaaðila á þessu sviði. Er þá einkum horft til samstarfs við stofnanir og fyrirtæki á sviði fjármála, orku og veitumála, samgangna, hugbúnaðariðnaðar og þjónustu, heilbrigðisþjónustu og háskóla og aðra sem koma að kenngslu og rannsóknum. Haldinn hefur verið opinn fundur með fulltrúum þessara geira og var það mikilvægt skref fyrir áframhaldandi og skilvirka samvinnu í netöryggistengdum málum. Verið er að byggja upp fulltrúakerfi innan *Samstarfshóps um net- og upplýsingaöryggi* þannig að hópurinn geti átt skilvirka samvinnu við Netöryggisráð og tekið þátt í samstarfi þau verkefni sem getið er í þessari samantekt, t.d. eftirfylgni ráðlegginga Oxford-háskóla, endurskoðun netöryggisstefnu og mótun nýrrar heildarlöggjafar um netöryggi.

Uppbygging netöryggis – áhersla á undanfögnu ári

Eitt brýnasta verkefni ráðuneytisins á sviði netöryggismála hefur verið *efling Netöryggissveitarinnar* og það er einnig lykilatridi í frumvarpi að sérstökum lögum um net- og upplýsingaöryggi sem er í mótun. Þar til ný lög hafa verið samþykkt og taka gildi verður að byggja á núgildandi lögum, sem miða við að Netöryggissveitin þjóni einkum fjarskiptafyrirtækjum en að aðrir geti þó gert þjónustusamninga við sveitina. Almenn form slíkra samninga var þróað á grunni sambærilegra samninga í Noregi og kynnt fulltrúum fjármálafyrirtækja og orku- og veitufyrirtækja. Fyrsti samningur á þessum grunni var hins vegar undirritaður við stjórnsýsluna og er hann mikilvægt skref til að efla Netöryggissveitina og munu væntanlega aðrir samningar fylgja í kjölfarið. Annað mikilvægt skref, sem hefur verið stigið á undanfögnu ári til að styrkja sveitina, er flutningur starfstöðvar hennar í sama húsnaði og hýsir tölvu- og netrannsóknir þeirra lögregluembætta sem vinna að rannsóknum á þessu sviði. Jafnframt hefur verið komið upp öruggri aðstöðu til móttöku og miðlunar trúnaðarupplýsinga á milli Netöryggissveitarinnar og norrænna systurstofnana, en það er lykilatridi í því norræna samstarfi sem sveitin á í.

Auk almennra aðgerða sem nýtast við að *bæta netöryggi stjórnsýslunnar*, þá var myndaður seint á síðasta ári *stýrihópur um netöryggi stjórnarráðsins*. Hópurinn starfar á vegum samgöngu- og sveitastjórnarráðuneytis, en í honum eru einnig fulltrúar forsætisráðuneytis og fjármála- og efnahagsráðuneytis. Til stendur að fulltrúi utanríkisráðuneytis bætist einnig við hópin. Stýrihópurinn stóð að gerð fyrrgreinds samnings á milli stjórnsýslunnar og Póst- og fjarskiptastofnunar um svokallaða GovCERT þjónustu Netöryggissveitarinnar. Samningurinn við stjórnsýsluna var undirritaður 26. janúar 2018 og er sem fyrr segir sá fyrsti sem nýtir lagaheimild til að gera þjónustusamning vegna þjónustu Netöryggissveitarinnar.

Samið um þjónustu Netöryggissveitarinnar við stjórnarsýsluna



Hrafnkell V. Gíslason og Sverrir Jónsson undirrituðu samninginn. Með þeim á myndinni eru Sigurður Emil Pálsson og Guðbjörg Sigurðardóttir.

Í dag var undirritaður fyrsti þjónustusamningur sem gerður hefur verið um þjónustu Netöryggissveitar Póst- og fjarskiptastofnunar. Samninginn undirrituðu fulltrúar fjármála- og efnahagsráðuneytisins og Póst- og fjarskiptastofnunar.

Markmið samningsins er að styrkja stjórnarsýsluna til að verjast öryggisatvikum og takast á við netárásir og hliðstæðar ógnir með sérhæfðri þjónustu Netöryggissveitarinnar.

Stefnt er að því að leggja fram *haustið 2018 frumvarp til laga um net- og upplýsingaöryggi*. Með því verða innleidd í íslensk lög ákvæði *tilskipunar Evrópuþingsins og ráðsins (ESB) 2016/1148 varðandi ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum í öllu Sambandinu*. Oftast er vísað til þessarar tilskipunar sem NIS-tilskipunarinnar (e. *NIS Directive*, NIS vísar til *network and information systems*). Markmiðið með tilskipuninni og lagafrumvarpinu er að styrkja með samræmdum hætti netvarnir þeirra sem veita nauðsynlega stafræna þjónustu, s.s. orkuveitur, bankaþjónustu, fjármálamarkaði, heilbrigðisþjónustu, vatnsveitur og stafræn grunnvirki. Gildissvið fyrirhugaðrar löggjafar er umfangsmikið og samráð er hafið við hagsmunaaðila. Samkvæmt tilskipuninni skal netöryggissveit með miðlægt hlutverk vera starfandi í hverju ríki sem tilskipunin nær til. Efling Netöryggissveitarinnar er því mikilvægt skref til að uppfylla þær kröfur. Innleiðing NIS-tilskipunarinnar kemur í kjölfar innleiðingar nýrrar *persónuverndarreglugerðar* í íslensk lög, sem unnið er að á vegum dómsmálaráðuneytisins. Strangar kröfur eru þar um tilkynningaskyldu og háar sektir geta legið við brotum á ákvæðum reglugerðarinnar. Fyrirhugað er að þróa, undir forystu samgöngu- og sveitastjórnarráðuneytis, tilkynningagátt fyrir öryggisatvik til að auðvelda að tilkynna netatvik sameiginlega og með samræmdum hætti eftir því sem við á, til Netöryggissveitar, Persónuverndar og lögreglu.

Eðli nauðsynlegrar *vitundarvakningar* hefur verið að taka breytingum undanfarið ár. Umfjöllun fjölmiðla hefur aukist verulega um árásir, veilur og aðra misnotkun Netsins og flestir átta sig á að þar kunni að leynast hættur. Stefnt er að því að auka samvinnu um upplýsingamiðlun og vitundarvakningu á þessu sviði, bæði á vettvangi Netöryggisráðs og með ýmsum hagsmunaaðilum í þjóðfélaginu, á vettvangi *Samstarfshóps um net- og upplýsingaöryggi*.

Nemendum við íslenska háskóla býðst nú að fara í *framhaldsnám í netöryggisfræðum* við erlenda háskóla. Viðræður við Tækniháskólann í Noregi (NTNU) leiddu til þess að fulltrúar háskólans komu hingað til lands og héldu kynningarfundir fyrir nemendum í tölvunarfræði í Háskóla Íslands og Háskólanum í Reykjavík. Kynnt var meistaranám í netöryggisfræðum sem er í boði við NTNU og í kjölfarið innrituðu sig 4 nemendur til náms. Stefnt er að því að endurtaka kynninguna næsta haust og viðræður standa yfir um þátttöku fleiri háskóla, t.d. Oxford-háskóla. Þetta er mikilvægt skref, bæði til að fá sérfræðinga á sviði netöryggis sem brýn þörf er á og til að efla vitund nemenda og margra í háskólasamfélaginu um nauðsyn þess að netöryggi verði viðeigandi hluti margra námsgreina, eins og Oxford-háskóli hefur nú þegar gert.

Alþjóðlegt samstarf

Netið er alþjóðlegt í eðli sínu og því byggir mikið af uppbygginu netöryggis á alþjóðlegu samstarfi, bæði við einstök ríki og samtök. Norrænt samstarf hefur gengt lykilhlutverki í þessu sambandi, bæði hjá ráðuneytum og stofnunum þeirra, ekki síst hjá Póst- og fjarskiptastofnun og Netöryggissveitinni, enda gegnir náið norrænt samstarf lykilhlutverki í starfsemi sveitarinnar. Jafnframt hefur verið gott samstarf á þessu sviði við ýmis grannríki og stofnanir þeirra.

Fulltrúi samgöngu- og sveitastjórnarráðuneytisins hefur nú tekið sæti í stjórn ENISA, evrópsku netöryggisstofnunarinnar, sem ætlað er aukið hlutverk í skipulagi netöryggismála álfunnar. Ýmislegt alþjóðlegt samstarf tengt netöryggi er fyrir milligöngu *utanríkisráðuneytisins*. Öllum aðildarríkjum Atlantshafsbandalagsins ber að viðhafa vissar lágmarksráðstafanir til að verja eigin innviði og gera grein fyrir því gagnvart bandalaginu. Þá hefur bandalagið skilgreint netöryggi sem fjórðu vídd sameiginlegra varna (ásamt vörnum á lofti, láði og legi). Netöryggi er viðfangsefni funda á vegum Norðurlanda og Eystrasaltsríkja og hafa fulltrúar utanríkisráðuneytis og samgöngu- og sveitastjórnarráðuneytis tekið þátt í þeim. Netöryggismál ber æ oftast á góma í ýmsum alþjóðlegum nefndum og ráðum og hefur verið leitast við (t.d. á vettvangi Netöryggisráðs) að miðla upplýsingum og samhæfa afstöðu og aðgerðir, eftir því sem við á. Óformleg tengsl hafa einnig verið við *Öndvegissetur Atlantshafsbandalagsins á sviði netöryggis (NATO Cooperative Cyber Defence Centre of Excellence)* sem hefur m.a. gefið út fræðirit og greiningar á lagalegum hliðum átaka á Netinu og ber þar hæst endurbætta útgáfu svokallaðrar Tallinn-handbókar, sem gefin var út vorið 2017. Fulltrúar utanríkisráðuneytis munu heimsækja setrið að nýju vorið 2018 og kanna möguleika á nánari tengslum. Nýtt öndvegissetur í Helsinki um varnir gegn blönduðum ógnum (e.

hybrid threats) var heimsótt sumarið 2017. Slíkar ógnir geta verið af ýmsum toga, en eiga þó margar sameiginlegt að byggja á notkun Netsins, beint eða óbeint. Þetta málefni var tekið til umræðu innan Netöryggisráðs og var samstaða um að ráðið geti tekið slík mál til umfjöllunar og til að samræma aðgerðir þeirra sem að lausn slíkra mála kunna að koma, ef sá aðili sem ber ábyrgð á úrlausn málsins óskar eftir því.

Dómsmálaráðuneytið og stofnanir þess fara með ýmis mál sem tengjast netglæpum, sem geta ýmist verið framdir með því að nýta Netið eða beinst gegn því. Ísland á aðild að Samningi Evrópuráðsins um tölvubrot (Convention on Cybercrime) og samvinna innan Europol skiptir miklu fyrir löggæsluna.

Áhersla í netöryggismálum á komandi ári

Brýnustu umbætur á komandi eru að ljúka við áður nefnt frumvarp um bætt netöryggi (sem er nauðsynlegt vegna innleiðingar NIS-tilskipunar) og leggja það fyrir haustþing 2018 til samþykktar. Það kallar m.a. á viðtækt samstarf og því er nú unnið að því að byggja upp innviði *Samstarfshóps um net- og upplýsingaöryggi* með öflugum fulltrúakerfi. Samhliða þessu þarf að endurskoða gildandi netöryggisstefnu og móta nýja aðgerðaáætlun innan ramma *heildarstefnu í fjarskiptum, netöryggismálum og póstmálum* (vinna hófst 2017, lýkur 2018). Fylgja þarf eftir ráðleggingum skýrslu Oxford-háskóla, sumar þeirra geta krafist víðtæks samstarfs. Umbætur í netöryggismálum þarf að vera unnt að meta og rýna út frá mælikvarða óháðs aðila (sbr. lánshæfismat). Búið er að gera samning við matsfyrirtæki sem gerir úttektir á tæknilegum veikleikum netkerfa landa og gefur tölulegt mat á stöðunni (skýrsla Oxford-háskóla gefur hins vegar mat á samfélagslegum þáttum og háskólinn er reiðubúinn til að greina stöðu á ný til að unnt sé að meta árangur aðgerða). Halda þarf áfram að efla menntun og rannsóknir, jafnframt þarf að benda hagsmunaaðilum á þá auðlind sem gott rannsókn- og menntaumhverfi getur verið.

Þótt mörgu hafi miðað vel þá þarf að leggja enn ríkari áherslu á netöryggismál en gert hefur verið, því örugg nýting Netsins er ein helsta áskorun nútímasamfélaga, án öryggis mun öll uppbygging á þessu sviði hrynja að lokum og traust á tækni og netþjónustu þverra, eins og nú þegar er farið að sjást merki um í ýmsum greinum.

Frumvarp um bætt netöryggi

Í undirbúningi er frumvarp um heildarlöggjöf um net- og upplýsingaöryggi og er henni m.a. ætlað að ná til þeirra sem veita nauðsynlega stafræna þjónustu. Meginmarkmið löggjafarinnar er að auka öryggi net- og upplýsingakerfa og bæta viðbrögð við öryggisatvikum. Hún byggir á því að áreiðanleiki og öryggi net- og upplýsingakerfa sé grundvöllur efnahags- og samfélagslegrar starfsemi. Og þar með að netöryggi sé mikilvægt fyrir trúverðugleika þeirrar þjónustu sem um ræðir, bæði innanlands og utan. Með löggjöfinni er meðal annars vegar að koma til móts við kröfur fyrrnefndrar NIS tilskipunar, en meginmarkmið tilskipunarinnar eru þrjú:

- I. Að auka hæfni ríkisins
 - Ríki skuli setja sér stefnu um net- og upplýsingaöryggi sem skal innihalda skilgreind markmið, áhættumat og reglur um viðeigandi ráðstafanir til að bæta öryggi.
 - Fela skuli ákveðnum aðila innan stjórnáslunnar eftirlit með fylgni við löggjöfina og samskipti við önnur ríki.
 - Netöryggisveit skuli starfa. Hún skuli fylgjast með og bregðast við öryggisatvikum sem verða innanlands, greina áhættu og vinna með netöryggisveitum annarra aðildarríkja.
- II. Að bæta samvinnu ríkja
 - Samstarfshópur ríkja verði settur á fót. Með það að markmiði að styðja samstarf ríkja, styrkja upplýsingamiðlun þeirra á milli og byggja upp gagnkvæmt traust.
 - Netöryggisveitir ríkja skuli mynda samstarfsnet netöryggisveita sem skiptast á upplýsingum og samræma viðbrögð.
- III. Að styrkja öryggi net- og upplýsingakerfa
 - Undir gildissvið NIS-tilskipunarinnar falla tveir flokkar innviða, rekstraráðilar nauðsynlegrar þjónustu og veitendur stafrænnar þjónustu. Öryggi net- og upplýsingakerfa þeirra þarf að vera tryggt.

Mikilvægt er að gott samstarf takist um þetta verkefni á milli ríkisins og hagsmunaaðila, þannig að nýta megi sem best þau sóknarfæri sem felast í samhæfingu öryggiskrafna til net- og upplýsingakerfa í Evrópu. Einn liður í fyrirhuguðu samstarfi er fundur í *Samstarfshópi um net- og upplýsingaöryggi*, sem haldinn verður þann 17. maí n.k.

Grein samgöngu- og sveitarstjórnarráðherra um vaxandi netógnir

Samgöngu- og sveitarstjórnarráðherra ritaði grein sem birtist í Viðskiptablaðinu þann 8. febrúar s.l. um vaxandi netógnir og ýmsar þær aðgerðir til varnar sem að framan hefur verið lýst. Grein ráðherra má lesa hér að neðan.

SKOÐUN

Vaxandi ógn

Sigurður Ingi Jóhannsson



Net- og tölvuárásir eru vaxandi ógn sem veldur fjárhagslegum og tilfinnanlegum skaða hjá einstaklingum, fyrirtækjum og stofnunum. Varlega er áætlað að kostnaður af völdum netglæpa hér á landi hlaupi á hundruðum milljóna króna og gæti jafnvel numið milljörðum. Skaðinn er mikill – skortur á netöryggi skerðir trúverðuleika ríkja og þar með samkeppnisstöðu þeirra á ýmsum sviðum.

Fjallað hefur verið um ýmiss konar netvá í fjölmiðlum undanfarið og ekki að ástæðulausu. Netöryggi er eitt brýnasta mál allra ríkja í okkar heimshluta þegar kemur að uppbyggingu samfélagsins. Á sama tíma og netið gerir okkur kleift að nýta tölvutæknina með fjölbreyttum hætti þá fylgir notkun þess ýmsar ófyrirséðar áskoranir sem við verðum að takast á við og getum ekki lokað augunum fyrir. Æ algengara er að veillar í netkerfum og tölvubúnaði séu nýttar skipulega til afbrota, njósna eða einfaldlega til að valda tjóni. Skaðsemi slíkra árása getur verið mikil en umræðan fer jafnan ekki hátt.

Eins og staðan er í dag sjá öll lönd fram á skort á sérfræðingum á þessu sviði en nú stendur yfir átak á vegum ráðuneytisins til að efla menntun í netöryggismálum. Við-

ræður við Tækniháskólann í Norgei (NTNU) hafa leitt til þess að sérfræðingar frá skólanum koma hingað til lands síðar í þessum mánuði og munu þeir kynna nám á framhaldsstigi á sviði netöryggis sem hentar einstaklingum sem lokið hafa grunnprófi í tölvunarfræði. Þessi heimsókn er í samvinnu við Háskóla Íslands og Háskólann í Reykjavík. Auk þessarar kynningar verður rætt um mögulegt samstarf skólanna þriggja á þessu sviði.

Bætt netöryggi

Þó að ýmislegt hafi verið gert til að efla net- og upplýsingaöryggi hér á landi er brýnt að halda áfram eftir því sem tækninni fleygir fram. Ein brýnasta aðgerð til að bæta netöryggi er mótun frumvarps um heildarlöggjöf um net- og upplýsingaöryggi en jafnframt er unnið að endurskoðun á stefnu um netöryggi og nýrri aðgerðaáætlun.

Markmiðið með frumvarpinu er að ná til þeirra sem veita nauðsyn-

lega stafræna þjónustu, s.s. orkuveitur, bankþjónusta, fjármála- markaði, heilbrigðisþjónusta, vatnsveitur og stafræn grunnvirki. Mikilvægt er að tryggja að slíkir aðilar geti veitt þessa þjónustu þvert á landamæri með samræmdum öryggiskröfum og þar með aukið samkeppnishæfni og dregið úr óþarfa kostnaði vegna mismunandi krafna og lagaumgjörðar. Gildissvið fyrirhugaðrar löggjafar er umfangsmikið og samráð er hafið við hagsmunaaðila, auk þess sem farið verður í opið samráð á netinu. Miðað er við að leggja umrætt frumvarp fram á komandi haustþingi og að það taki gildi um næstu áramót.

Samkvæmt NIS-tilskipuninni sem frumvarpið byggist á ber netöryggisveit að vera starfandi í hverju ríki sem tilskipunin nær til. Netöryggisveit Póst- og fjarskiptastofnunar, sem er ein af stofnunum ráðuneytisins, greinir netvá og á að sinna ýmsum samþæfingarverkefnum innanlands og jafnframt að taka virkan þátt í samstarfi evrópskra netöryggisveita. Efling Netöryggisveitarinnar er því mikilvæg. Stórum áfanga var nýverið náð þegar undirritaður var þjónustusamningur sveitarinnar við stjórnsluna um netöryggisþjónustu. Þetta er fyrsti þjónustusamningurinn sem hefur verið undirritaður og munu aðrir væntanlega fylgja í kjölfarið. Samningur Netöryggisveitarinnar við orku-geirann er t.d. langt kominn.

Markmið samningsins við stjórnsluna er að verjast öryggis-

atvikum og takast á við netárásir og hliðstæðar ógnir. Hann er til marks um aðgerðir sem samgöngu- og sveitarstjórnarráðuneytið hefur beitt sér fyrir til að efla netöryggi.

Ábendingar frá Oxford

Auk tæknilegra þátta þarf einnig að huga að þeim samfélagslegu. Samgöngu- og sveitarstjórnarráðuneytið fékk Háskólann í Oxford til að gera skýrslu um stöðu netöryggis á Íslandi sem skilað var nýlega. Í skýrslunni eru ýmsar ráðleggingar til úrbóta og er verið að vinna að mótun aðgerða byggðum á ráðleggingunum. Skýrslan, ásamt tillögum um aðgerðir, verður bráðlega kynnt opinberlega.

Ljóst er að mikil þróun er nú í öllu skipulagi netöryggismála hjá grannríkjum okkar og sér ekki fyrir endann á því. Viðtæk innleiðing nettækni hefur róttæk áhrif á samfélög okkar sem bregðast verður við. Ráðuneytið hefur fylgst náið með þessum breytingum og átt gott samstarf við grannríki okkar, ekki síst Norðurlönd. Nýja persónuverndarreglugerðin (GDPR) hefur verið mikið til umræðu undanfarið, nú mun NIS-tilskipunin bættast við og fleiri breytingar á stjórnskipun netöryggismála eru fyrirsjáanlegar. Með efldu netöryggi byggðu á góðu samstarfi getum við öll nýtt þau tækifæri sem netnotkun getur boðið upp á, styrkt samkeppnisstöðu okkar og bætt lífsgæði í vinnu og einkalífi.

Höfundur er samgöngu- og sveitarstjórnarráðherra.



Viðtæk innleiðing nettækni hefur róttæk áhrif á samfélög okkar sem bregðast verður við.