Málefnasvið 11.2

Fylgiskjal með grænbók

JÚNÍ 2018

Einföld samantekt um stöðu netöryggismála

Vinnuskjal

Yfirlit samantektar

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.

Mótun gildandi stefnu um net- og upplýsingaöryggi

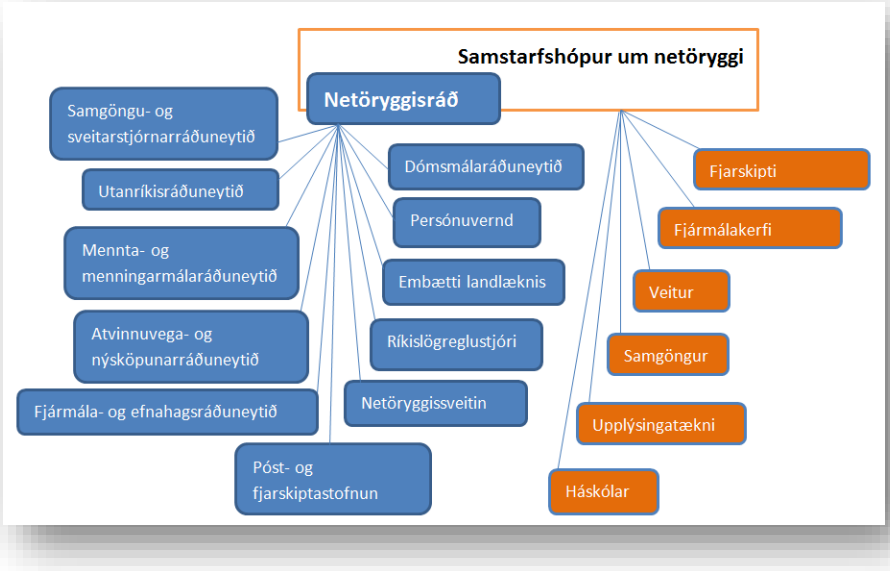
Starf stjórnvalda á sviði netöryggis byggir á stefnu um net- og upplýsingaöryggi sem þáverandi innanríkisráðherra kynnti ríkisstjórn og Alþingi vorið 2015. Stefnunni fylgdi

jafnframt aðgerðaáætlun til þriggja ára[1]. Stefnan var mótuð að undangengnu víðtæku samráði og var einnig höfð hliðsjón af stefnum grannríkja á sviði netöryggismála. Stefnumótunarfundur var haldinn í Þjóðmenningarhúsinu þann 2. júní 2014 og fyrir fundinn var m.a. dreift meðfylgjandi skjali, ***Stefnumótun um NET- OG UPPLÝSINGAÖRYGGI, Umræðuskjal – Drög, maí 2014***. Þótt ör þróun hafi orðið á þessum tíma, þá standa enn ýmsir grunnþættir sem þarna er lýst. Niðurstöður vinnu umræðuhópa má lesa í, ***Samantektir eftir samráðsfund***[2], skjali sem nálgast má á Netinu. Stefnan setur fram sýn um net- og upplýsingaöryggi á Íslandi fram til 2026. Þar kemur fram að stefnt er að því að Íslendingar búi við net sem þeir geti treyst og þar séu í heiðri höfð mannréttindi, persónuvernd ásamt frelsi til athafna, efnahagslegs ávinnings og framþróunar. Stefnan byggir á því að örugg upplýsingatækni sé ein meginstoð hagsældar á Íslandi, studd af öflugri öryggismenningu og traustri löggjöf ásamt því að samfélagið verði vel búið til að taka á netglæpum, árásum, njósnum og misnotkun persónu- og viðskiptaupplýsinga.

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. Skipunartími Netöryggisráðs rann út 1. júní 2018 og hefur verið leitað eftir tilnefningum frá framangreindum aðilum í ráðið. Að auki hefur verið óskað eftir tilnefningum frá forsætisráðuneyti. Netöryggisráð hefur reynst vera góður vettvangur upplýsingamiðlunar, samhæfingar og samstarfs.

[1] Net- og upplýsingaöryggi – Stefna 2015-2026. Innanríkisráðuneytið. Sjá á slóðinni: https://www.stjornarradid.is/media/innanrikisraduneyti-media/media/frettir-2015/Netoryggisstefna_2015_april.pdf

[2] Þetta skjal aðgengilegt á Netinu: https://www.stjornarradid.is/media/innanrikisraduneyti-media/media/frettir-2014/samradsfundur_samantekt---med-frett-28.-november.pdf



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 kennslu 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 (sjá næsta kafla), endurskoðun netöryggisstefnu og mótun nýrrar heildarlöggjafar um netöryggi.

Úttekt Oxford-háskóla á stöðu netöryggis hérlendis

Öryggi er undirstaða þeirrar starfrænu umbyltingar sem nútíma þjóðfélög glíma nú við og til að efling netöryggis skili árangri kallar það á víðtækt samstarf þvert á þjóðfélagið. Greining á stöðu og mat á hvar umbóta sé þörf krefst einnig víðtækrar nálgunar. *Oxford-háskóli* var því 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 netöryggistengd 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.

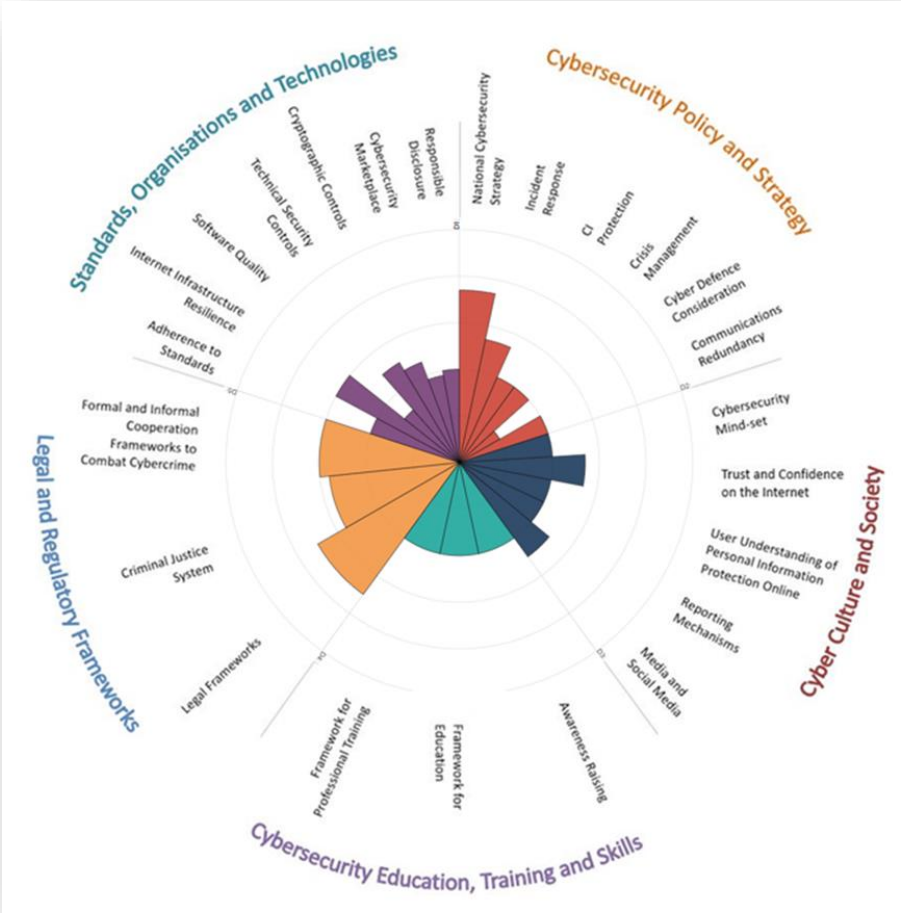
HELSTU NIÐURSTÖÐUR MATS Á STÖÐU NETÖRYGGIS

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

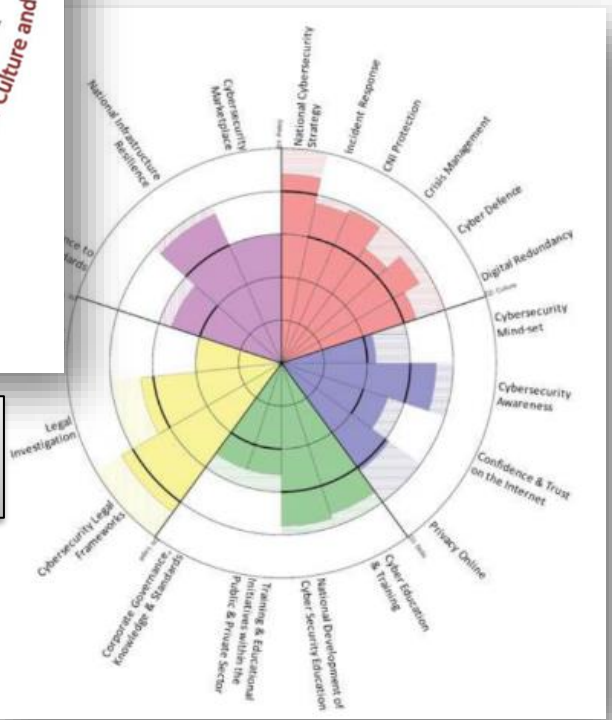
1. *Netöryggisstefna og skipulag* (e. *Cybersecurity Policy and Strategy*)
2. *Netöryggismenning og samfélag* (e. *Cyber Culture and Society*)
3. *Netöryggsmenntun, þjálfun og hæfni* (e. *Cybersecurity Education, Training and Skills*)
4. *Lagalegt umhverfi* (e. *Legal and Regulatory Framework*)
5. *Staðlar,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

Innan hverrar 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 skífuriti 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 *Degi 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 tilsvarandi 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. Þróa reglur um upplýst samþykki notenda vegna söfnunar persónuupplýsinga. Hvetja til notkunar vefstaða 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 - Netöryggsmenntun, þjálfun og hæfni

- Þjóðarátak til betri vitundar um netöryggi, samhæfð dreifing ráðlegginga, stofnun netöryggisgáttar til dreifingar upplýsinga, auk sjálfsnámsgáttar. Fræðsla og ráðleggingar um netöryggi fyrir stjórnsýslu. Sérsniðin 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 víðtæku 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. Þróa 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 örri þróun á þessu sviði.
- Gæta þess að gildi varðandi mannréttindi, vernd barna, neytendavernd og höfundarrétt endurspeglist með viðeigandi hætti í lagaumhverfi og unnt sé að bregðast við örri þróun á þessum sviðum.
- Tryggja að unnt sé að rannsaka flókin netbrot og að rannsakendur hafi hlotið viðeigandi 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, ákærur 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 eflt öryggi mikilvægra innviða.
- Greina áfallaþol mikilvægra innviða Netsins á Íslandi í samvinnu við rekstraraðila og greina hvar eru veikir punktar
- Þróa 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). Þróa reglur á þessu sviði og endurmeta þær reglulega.
- Huga að því að styrkja þróun netöryggislausna út frá þörfum íslensks markaðar. Tryggja að þróun hugbúnaðar taki mið af netöryggiskröfum í alþjóðlegum stöðlum og viðmiðum og efla markað með nettryggingar.
- Þróa skipulag varðandi ábyrga miðlun upplýsinga um veikleika. Hvetja hugbúnaðar- og þjónustuveitendur til upplýsingamiðlunar um veilur. Hvetja til miðlunar meðal rekstraraðila mikilvægra innviða um tæknilega eiginleika netveikleika. Birting greiningar á tæknilegum eiginleikum netveikleika.

Þróun í grannríkjum okkar

NORÐURLÖND

Ört vaxandi áhersla er nú á norræna samvinnu á sviði netöryggis, enda er vá á því sviði þegar farin að valda verulegum skaða og árásir gegn mikilvægum innviðum samfélaga veruleiki sem bregðast verður við. Norrænir forsætisráðherrar hafa lagt áherslu á aukna samvinnu og fyrsti sameiginlegi fundur hátt settra norrænna embættismanna um netöryggismál var haldinn í Stokkhólmi, 13. júní 2018. Skipst var á upplýsingum um stöðu uppbyggingar netöryggis og áhersla verður m.a. lögð á miðlun upplýsinga um stefnumótun og innleiðingu stefna sem og á aukna norræna samvinnu á alþjóða vettvangi.

Danir hafa birt nýja netöryggisstefnu[3] (í maí 2018) þar er þrjú meginmarkmið að finna:

1. Öruggt umhverfi
2. Efld hæfni
3. Bætt samvinna.

Danir urðu fyrir verulegu tjóni í kjölfar *NotPetya* netárasarinnar og hafa opinberlega sakað Rússa fyrir að hafa staðið að baki henni. Þótt árásinni hafi væntanlega verið beint gegn Úkraínu, þá var árásartólið hömlulaust í eðli sínu og olli t.d. verulegu tjóni hjá skipafélaginu Maersk. Danir munu á næstu 6 árum verja um 1,5 milljarði danskra króna (nú rúmlega 25 milljarða ISK) til netöryggismála, þar á meðal til netöryggisseturs síns. Miðað við íbúatölu er þetta samsvarandi og ef Íslendingar myndu verja um 1,5 milljörðum ISK til netöryggismála á sama tímabili. Í danska netöryggissetrinu starfa nú um 100 manns en stefnt er að fjölga þeim í 230 á þessu tímabili.

Svíar eru einnig með nýlega stefnu, *Nationell strategi för samhällets informations- och cybersäkerhet*[4] og stjórnvöld gáfu sumarið 2017 einnig út tveggja síðna samantekt á ensku[5] um stefnuna.

Norðmenn eru að vinna að nýrri stefnu. Gildandi stefna snýr einkum að hinu opinbera, í hinni nýju verður lögð meiri áhersla á aðila á markaði og einstaklinga og endurspeglar það þá þróun sem víða er að finna, um mikilvægi þess að efling netöryggis sé tekið sem víðtækt samfélagslegt átak. Norðmenn gáfu í árslok 2015 út mjög ítarlega samantekt um hvernig mismunandi geirar samfélagsins væru orðnir háðir netnotkun og þá áhættu sem það skapaði (sjá NOU 2015:13, *Digital sårbarhet – sikkert samfunn*[6]). Þessi opinskáa samfélagsgreining hefur m.a. verið notuð sem grunnur síðari stefnumótunarvinnu.

Finnar eru ekki nú að vinna í endurskoðun á gildandi stefnu, en þeir eru að vinna að endurskoðun aðgerðaáætlunar og með meiri áherslu á árangursmiðaðri rýni og markmiðum.

---

[3] https://www.fm.dk/publikationer/2018/national-strategi-for-cyber-og-informationssikkerhed
[4] https://www.regeringen.se/rattsliga-dokument/skrivelse/2017/06/skr.-201617213/
[5] https://www.government.se/information-material/2017/07/a-national-cyber-security-strategy/
[6] https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

Öll Norðurlönd leggja mikla áherslu á að fylgjast með þeim breytingum sem nú eru að eiga sér stað innan Evrópu á sviði netöryggismála og bregðast við þeim með viðeigandi hætti.

NET- OG UPPLÝSINGAÖRYGGI Í EVRÓPUSAMBANDINU OG VÍÐAR

Þann 13. september 2017 kynnti Evrópusambandið nýja stefnu í netöryggismálum. Samkvæmt henni er lögð áhersla á að efla evrópsku netöryggisstofnunina, ENISA og gefa henni aukið vægi, en þó að settum ákveðnum skorðum þannig að réttindi og skyldur aðildaríkja séu ekki skert. Fulltrúi Samgöngu- og sveitarstjórnarráðuneytis hefur tekið sæti í stjórn stofnunarinnar og ráðuneytið mun því eiga hægara með að fylgjast með þróun þessara mála þar. Jafnframt er unnið að mótun vottunarkerfis netöryggis fyrir nettæki og þjónustu (e. *European Cybersecurity Certification Schemes, ECCS, for Information and Communication Technology, ICT, products and services*). Með þessu er ekki stefnt að þróun nýrra staðla, heldur frekar að aukinni og samræmdri notkun þeirra staðla sem fyrir eru til að unnt sé að skapa skilvirkara markaðssvæði innan Evrópu. Gott yfirlit yfir það sem er á döfinni hjá Evrópusambandinu í netöryggi má finna á vefsíðu sambandsins um það efni[7].

Æ fleiri ríki hafa komið sér upp getu til að ráðast með netárásum á mikilvæga innviði annarra ríkja, til að lama starfsemi þeirra með beinum eða óbeinum hætti. Samhliða þessu hafa kröfur aukist um að vörnum mikilvægra innviða sé sinnt og að reynt sé að veita mikilvæga þjónustu með sem bestum hætti þótt komi til alvarlegrar netárásar. Atlantshafsbandalagið hefur m.a. gert ákveðnar kröfur til aðildarríkja sinna á þessu sviði (e. *Cyber Defense Pledge*[8]) og ríki utan bandalagsins taka einnig mið af þessum kröfum (þar á meðal þau Norðurlanda sem eru ekki í NATO)

Uppbygging netöryggis – áhersla á undanförnu ári

Eitt brýnasta verkefni ráðuneytisins á sviði netöryggismála hefur verið *efling Netöryggissveitarinnar* og það er einnig lykilatriði 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. Almennt 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 undanförnu ári til að styrkja sveitina, er flutningur starfstöðvar hennar í sama húsnæði og hýsir tölvu- og netrannsóknir þeirra lögregluembætta sem vinna að rannsóknum á þessu sviði. Jafnframt hefur verið komið

[7] https://ec.europa.eu/digital-single-market/en/cyber-security
[8] Texta þessarar skuldbindingar má finna hér:
https://www.nato.int/cps/su/natohq/official_texts_133177.htm

upp öruggri aðstöðu til móttöku og miðlunar trúnaðarupplýsinga á milli Netöryggissveitarinnar og norrænna systurstofnana, en það er lykilatriði 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 stjórnsýslunnar*. 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 hópinn. 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.

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*.

Kennsla í netöryggisfræðum fer vaxandi við íslenska háskóla og nemendum þaðan 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 kynningarfundi fyrir nemendur 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. Þátttaka hefur einnig verið í alþjóðlegum styrkumsóknum og verkefnum á sviði netöryggis og netöryggistengt frumkvöðlastarf hefur vakið athygli erlendis. Þetta er ánægjuleg þróun, en betur má ef Ísland á að verða í fremstu röð á þessu sviði.

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,* bæði norrænt eins og fyrr er getið og alþjóðlegt. Öllum aðildarríkjum Atlantshafsbandalagsins ber að viðhafa vissar lágmarksráðstafanir til að verja eigin innviði og gera grein fyrir því gagnvart bandalaginu[9]. 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 oftar 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 fjölþáttaógnum (eða 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.

[9] Samanber áðurnefnda skuldbindingu, *Cyber Defence Pledge*: https://www.nato.int/cps/su/natohq/official_texts_133177.htm

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 ári eru að ljúka við áðurnefnt 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 það gerir einnig eftirfylgni við ráðleggingar Oxford-háskóla. Það er því nú unnið að því að byggja upp innviði *Samstarfshóps um net- og upplýsingaöryggi* með öflugu fulltrúakerfi, helst er horft til í byrjun þeirra sem munu falla undir ákvæði NIS-tilskipunarinnar. Samhliða þessu þarf að endurskoða gildandi netöryggisstefnu og móta nýja aðgerðaáætlun innan ramma *heildarstefnu í fjarskiptum, netöryggismálum og póstmálum* (vinna hófst 2017, lýkur 2018). 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 rannsókna- 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. Menntun, rannsóknir og nýsköpun eru lykilþættir í eflingu netöryggis, án þeirra mun það ekki ná að standa á styrkum stoðum.

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 verið 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 stjórnsýslunnar eftirlit með fylgni við löggjöfina og samskipti við önnur ríki.
   - Netöryggissveit 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.
   - Netöryggissveitir ríkja skuli mynda samstarfsnet netöryggissveita sem skiptast á upplýsingum og samræma viðbrögð.

III. Að styrkja öryggi net- og upplýsingakerfa
   - Undir gildissvið NIS-tilskipunarinnar falla tveir flokkar innviða, rekstraraðilar 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.

Uppbygging samstarfs um net og upplýsingaöryggi

Á næstu síðu má sjá drög að kortlagningu þess samstarfs sem miðað er við að *Samstarfshópur um net- og upplýsingaöryggi* byggi á. Til vinstri er Netöryggisráð og þeir opinberu aðilar sem eiga aðild að því. Hægra megin ofarlega má sjá þá aðila sem gætu fallið undir ákvæði NIS-tilskipunarinnar og samsvarandi eftirlitsstofnanir. Neðar má sjá aðra aðila sem einnig gegna mikilvægu hlutverki í því samstarfi sem byggja þarf upp. Rétt er að ítreka það að endanleg ákvörðun á hvaða aðilar muni falla undir NIS-tilskipunina mun byggjast á lögfræðilegu mati og verður þá einnig tekið mið af túlkun tilskipunarinnar í grannlöndum okkar. Skýringarmyndinni er því einungis ætlað að gefa mynd af hugsanlegri uppbyggingu samstarfs, ekki nákvæmum hlutverkum hvers og eins. Allar ábendingar eru þó vel þegnar.

(Mynd sleppt fyrir birtingu með grænbók á samráðsgátt þann 27.9.2018, þar sem skipulagið sem myndin lýsir er í þróun og hefur breyst að hluta frá því sem myndin lýsir og var miðað við fyrri hluta júní 2018).