Grænbók um net- og upplýsingaöryggi

Stöðumat og valkostir

Samgöngu- og sveitarstjórnarráðuneytið
Stjórnarráð Íslands

Samgöngu- og sveitarstjórnarráðuneytið
Sölvhólsgötu 7 – 101 Reykjavík
545 8200 / srn@srn.is

Mars 2021

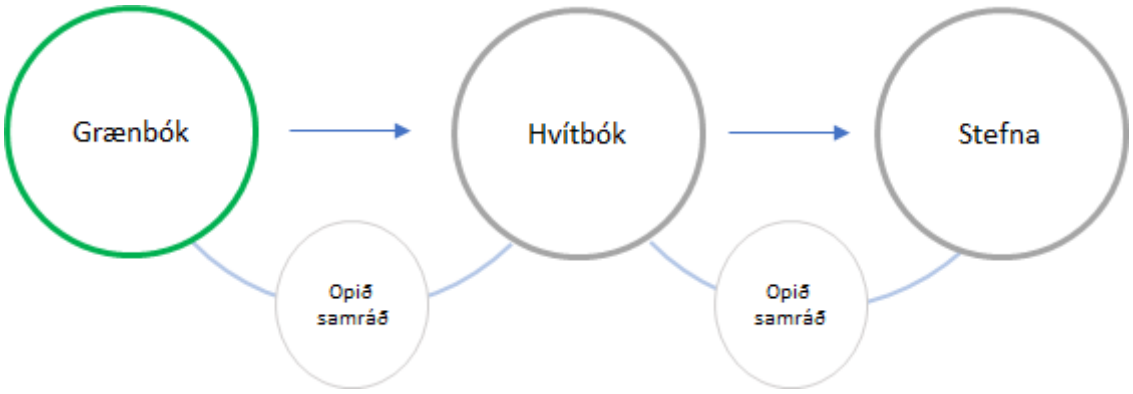
stjornarradid.is

Stöðumat og valkostir

Stöðumat og valkostir (grænbók) er greining á tilteknu viðfangsefni sem stjórnvöld hafa ákveðið að skoða nánar, ýmist sem undanfari stefnumótunar og/eða frumvarpsgerðar. Stöðumatið er hægt að setja í opið samráð á samráðsgáttinni á vef Stjórnarráðsins, þar sem almenningi og hagsmunaaðilum er boðið að taka þátt og setja fram sín sjónarmið um stöðumatið.

Stöðumat og valkostir innihalda upplýsingar um viðfangsefnið og núverandi stöðu þess. Tekin er saman sú tölfræði sem til er um viðfangsefnið, hvort sem hún er innlend eða samanburðar tölfræði við önnur ríki. Stöðumatið gefur gott yfirlit yfir lykilviðfangsefnin fram undan og helstu leiðir eða áherslur við úrlausn þeirra.

Við gerð stöðumats og valkosta er framkvæmdaaðilum, samstarfsaðilum og hagsmunaaðilum jafnan boðið að taka þátt og koma sínum sjónarmiðum og sérþekkingu um málefnið á framfæri.



Stöðumat og valkostir er hluti af stefnumótunarferli stjórnvalda

Að loknu samráði um stöðumat og valkosti eru niðurstöður dregnar saman og mótuð stefna sem inniheldur framtíðarsýn fyrir málefnið og markmið sem marka leiðina ásamt áherslum. Stefnu fylgir yfirleitt aðgerðaáætlun. Stöðumat og valkosti er jafnframt hægt að nota sem grundvöll fyrir frumvarpsgerð.

Þegar stefna eða frumvarp liggur fyrir fá almenningur og hagsmunaaðilar að jafnaði tækifæri til þess að koma á framfæri ábendingum sínum og sjónarmiðum í formlegu samráðsferli áður en endanleg afstaða er mótuð.

Efnisyfirlit

1. Inngangur

1.1 Netöryggi sem þverfaglegt viðfangsefni í samfélaginu

Öryggi tölvu- og hugbúnaðarlausna hefur verið vaxandi viðfangsefni áratugum saman. Þótt áherslan hafi helst verið á tæknilega þætti málsins þá hefur jafnframt verið fjallað um áskoranir í samskiptum fólks og tölva í rúma hálfa öld.

Með gríðarlegri aukningu í notkun (og misnotkun) Netsins hafa öryggisáskoranir aukist að sama skapi. Sé þeim ekki sinnt getur það leitt til illbætanlegs tjóns, traust til netháðrar þjónustu getur hrunið og uppbyggingarstarf komið að litlum notum.

Meðal helstu netöryggisáskorana samtímans er þróun og **notkun hlutanetsins** (e. *Internet of Things* - IoT) því með tilkomu þess getur tölvutengdur búnaður valdið skaða (jafnvel banvænum) án þess að mannshöndin eða mannshugurinn hafi tækifæri til að grípa inn í. Með **notkun gervigreindar** magnast netöryggisþörfin enn frekar, því þá fær tölvubúnaður getu til að taka ákvarðanir og hrinda þeim í framkvæmd. Ein áskorunin sem við blasir snýr svo að því að í dómsmálum þarf að vera unnt að ákvarða hvar lögsaga mála er.

Skipulögð glæpastarfsemi nútímans byggir í æ ríkara mæli á að finna og notafæra sér ekki bara tæknilega veikleika, heldur einnig lagalega og lögsögulega óvissu, siðferðileg álitamál og margt fleira.

Aukin misnotkun á Netinu kallar á að hugað sé sérstaklega að **vernd viðkvæmra hópa, ekki síst barna**. Þar sem þessi misnotkun getur verið margslungin, þá er brýn þörf á samvinnu mismunandi aðila til að viðunandi árangur náist.

Með skammtatölvum mun verða stökkbreyting í reiknigetu og ýmsar öryggislausnir á Netinu verða úreltar. Í alþjóðlegri samvinnu er aukin áhersla á að ríki taki þátt í samstarfi um þær öryggisáskoranir sem fylgja skammtatölvum, t.d. með tilliti til öryggis, flutnings og geymslu trúnaðargagna. Netöryggi hefur því þróast frá því að vera nær eingöngu tæknilegt viðfangsefni tölvusérfræðinga í að vera þverfaglegt viðfangsefni sem krefst víðtækrar samvinnu í samfélaginu[1]. Hér er til mikils að vinna að allir vinni saman, stjórnvöld og atvinnulífið, samtök og einstaklingar. Áhersla á netöryggi skilar sér ekki einungis í minni líkum á skaða (sem getur hlaupið á tug milljarða króna í íslensku samfélagi og fer vaxandi), heldur er framboð á netöryggistækni og þjónustu ört vaxandi atvinnugrein

[1] Sem dæmi um öra þróun má nefna að netöryggisfræði sem þverfagleg fræðigrein var ekki til sem háskólagrein fyrir áratug, breskir háskólar í samvinnu við fleiri hafa því skilgreint ramma fjölþætts netöryggisnámsefnis, sem er jafnframt í boði endurgjaldslaust, sjá: https://www.cybok.org

erlendis.[2] Þeirri nýju stefnu um net- og upplýsingaöryggi (hér eftir nefnd netöryggisstefna til einföldunar) sem hér er í mótun er ætlað að vera grunnur víðtæks samráðs, samhæfingar og samstarfs um netöryggi, sem ekki einungis getur skapað nauðsynlegt öryggi um stafrænar lausnir framtíðar heldur einnig lagt grunn að ábatasömum iðnaði og þjónustu.

1.1 Umgjörð og skipulag stefnumótunar

Settur var á fót stýrihópur sem heldur utan um stefnumótunarverkefnið. Guðrún Ragnarsdóttir, ráðgjafi, stýrir vinnu hópsins og auk hennar eiga Sigurður Emil Pálsson og Arnheiður Ingjaldsdóttir sæti í hópnum af hálfu ráðuneytisins. Að auki vinna Sigríður Rafnar Pétursdóttir og Ottó V. Winther með stýrihópnum. Ragnhildur Hjaltadóttir ráðuneytisstjóri og Guðbjörg Sigurðardóttir skrifstofustjóri voru bakhjarlar verkefnisins. Náið samráð var haft við Netöryggisráð við vinnu verkefnisins.

1.2 Afmörkun viðfangsefnis

Afurð stefnumótunarvinnunnar verður þverfagleg stefna um netöryggismál sem nær til alls samfélagsins, allra verkefna stjórnsýslunnar sem varða netöryggismálin á einhvern hátt og þá um leið verkefna fyrirtækja. Tekið er mið af sambærilegum stefnum ýmissa landa við afmörkun verkefnisins og er sérstaklega litið til sambærilegra stefna á Norðurlöndunum.

1.3 Tilefni endurskoðunar/stefnumótunar

Vorið 2015 kynnti þáverandi innanríkisráðherra ríkisstjórn og Alþingi stefnu um net- og upplýsingaöryggi og í kjölfarið var unnið að innleiðingu hennar. Víðtækt samráð fór fram og voru stefnur grannríkja á sviði netöryggismála á þeim tíma hafðar til hliðsjónar. Alþingi samþykkti í júní 2019 nýja stefnu ríkisins um net- og upplýsingaöryggi, sem birtist sem hluti af stefnu í fjarskiptum fyrir árin 2019-2033[3] og fjarskiptaáætlun fyrir árin 2019-2023[4]. Samhliða samþykkti Alþingi fyrstu heildstæðu lög á Íslandi um netöryggi,[5] að fyrirmynd samevrópsks regluverks.[6] Í þeim er kveðið á um að ráðherra skuli marka stefnu um net- og upplýsingaöryggi, sem endurskoða ber reglubundið. Í stefnu skal m.a. greina frá markmiðum og

[2] Sem dæmi um veltu netöryggisiðnaðar má nefna að í breskri kynningu í janúar 2020kom fram að veltan í Bretlandi væri orðin £8,3 milljarðar og vaxandi. Þetta samsvarar um 7,4 milljörðum íslenskra króna sé veltan heimfærð á Ísland út frá hlutfalli íbúafjölda, https://www.gov.uk/government/news/uks-booming-cyber-security-sector-worth-83-billion.

[3] https://www.althingi.is/altext/149/s/1688.html

[4] https://www.althingi.is/altext/149/s/1687.html

[5] Lög nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða voru samþykkt á Alþingi 25. júní 2019 og tóku gildi 1. september 2020.

[6] Netöryggistilskipun (ESB) 2016/1148 eða NIS1-tilskipunin (sjá m.a. kafla 6.4.1).

ráðstöfunum stjórnvalda í því skyni að stuðla að öryggi og viðnámsþrótti net- og upplýsingakerfa mikilvægra innviða.

Um helmingur er nú liðinn af ætluðum gildistíma fjarskiptaáætlunar, en tímabært þykir að endurskoða stefnuna í ljósi mjög örrar þróunar í netöryggismálum um heim allan, vaxandi netógna og formkrafna sem gerðar eru til netöryggisstefna einstakra ríkja.[7] Þá eru áskoranir í netöryggismálum í auknum mæli þverfaglegar og því þvert á málaflokka Stjórnarráðs Íslands, þær varða í raun nútímasamfélagið allt. Úrlausnir krefjast æ meiri samvinnu og samhæfingar, þar á meðal í stefnumótun og innleiðingu stefnu á þessu sviði.

1.4 Nauðsyn fjölbreytileika: Kynja- og jafnréttissjónarmið

Í umfjöllun um netöryggi í nútímasamfélagi þarf að leggja rækt við þverfagleg gildi og því þarf að huga að fjölbreytileika í hópi þeirra sem að henni koma, t.d. með tilliti til menntunar, kyns, aldurs og menningarlegs bakgrunns[8].

1.4.1 Sóknarfæri til jafnréttis kynja

Karlar hafa lengst af verið fjölmennari en konur í mörgum tæknigreinum, hlutur kvenna í tölvunarfræði hefur hins vegar verið vaxandi. Alþjóðlega er hlutfall kvenna lágt eða nálægt 10-15%. Einnig er kynbundinn launamunur til staðar- þar hallar á konur og margar menningarlegar hindranir verða á vegi kvenna ef þær vilja hasla sér völl innan greinarinnar. Með markvissum aðgerðum er hægt að vinna að úrbótum í skólakerfinu, t.d. með skólastyrkjum, vinnu með staðalmyndir, „mentorum“ og fleiru. Ástæða þess að mikilvægt er að fá fleiri konur að borðinu í netöryggismálum er m.a. sú að þá verða til fjölbreyttari lausnir í þessari vaxandi og brýnu atvinnugrein.

Þróunin virðist vera í átt að auknum hlut kvenna í hinum ýmsu greinum netöryggis, ef til vill vegna þess að nútímaleg nálgun á netöryggi er sú að hér sé ekki einungis um að ræða tæknigrein, heldur þverfaglega grein sem tekur til margra þátta, ekki síst áhættugreiningar. Sem dæmi má nefna að í Netöryggisráði sem starfar á vegum samgöngu- og sveitarstjórnarráðuneytisins er nú nær jafnt hlutfall karla og kvenna. Alþjóðafjarskiptasambandið (ITU) hefur hrint af stað átaki til að styrkja hlut kvenna í netöryggi og var það m.a. tengt

[7] Sjá t.d. kafla 6.4 (viðauka) í þessari skýrslu.

[8] Í kynningu breska CyBOK verkefnisins (https://www.cybok.org/news/success-at-the-cybok-in-practice) 2. mars 2021 var lögð áhersla á mikilvægi fjölbreytileika (e. diversity) þegar litið væri til þeirra sem þyrftu að koma að netöryggi. Netöryggi væri fjölþætt samfélagsverkefni og t.d eldra fólk með mismunandi reynslu og menningartengsl þyrfti einnig að koma að verkefninu. Svipaða áherslu á nauðsyn fjölbreytileika má einnig finna í eftirfarandi grein: https://www.crest-approved.org/wp-content/uploads/CREST-Closing-the-Gender-Gap-in-Cyber-Security.pdf

netöryggismánuðinum 2020[9]. Hluti dagskrár netöryggismánaðarins hérlendis var málstofa undir stjórn ungra kvenna um hlut kvenna í netöryggismálum og var helsta niðurstaða hennar að auka þyrfti sýnileika starfs kvenna á þessu sviði. Þegar litið er á netnotkun almennt (og ekki einungis netöryggi) eru ýmsir þættir sem þarf að huga að varðandi jafnrétti, t.d. það gildismat sem gervigreind mun byggja á, vaxandi söfnun gagna og lýsigagna, misbeiting samfélagsmiðla, áreiti og ógnir á Netinu auk stafræns kynferðisofbeldis. Hvort sem þessir þættir eru taldir falla undir netöryggi eða ekki, þá er mikilvægt að huga að þeim til að tryggja að umhverfi Netsins sé öruggt og stuðli að jafnrétti.

1.4.2 Sóknarfæri til jafnréttis innflytjenda

Netöryggi er ekki aðeins þverfaglegt í eðli sínu heldur einnig alþjóðlegt. Hugsanlega hefur skortur á tengslum við alþjóðlega strauma hægt á þróun netöryggis hérlendis, því nýir tækni- og menningarstraumar berast iðulega með fólki sem hefur lært og búið erlendis, þar á meðal innflytjendum. Innflytjendur til Íslands hafa að jafnaði mun meiri menntun en innflytjendur í mörgum grannríkjum okkar, en þó virðist vera mun erfiðara fyrir innflytjendur hérlendis en Íslendinga að fá vinnu við hæfi miðað við menntun. Samkvæmt gögnum Hagstofu Íslands er um 50% erfiðara fyrir konur að fá vinnu við hæfi miðað við menntun en karla. Athygli vekur að það er svo um fjórum sinnum erfiðara fyrir innflytjanda að fá vinnu við hæfi miðað við menntun en Íslending.[10] Innflytjendur með góða viðeigandi menntun og reynslu geta verið vannýtt auðlind, ekki einungis í afmörkuðum sérfræðistörfum heldur einnig í stjórnunarstörfum vegna nauðsynlegs tækni- og menningarlæsis. Þar sem netöryggi er nýtt fræðasvið í örri þróun, þá býður það upp á mörg tækifæri til að gefa innflytjendum tækifæri til að leggja sitt af mörkum í þessu brýna samfélagslega verkefni.

[9] Í mörgum ríkjum Evrópu er lögð sérstök áhersla á netöryggi í október ár hvert og það hefur verið gert á Íslandi síðan 2019.

[10] Það hafa ekki verið gerðar ítarlegar rannsóknir á samsetningu og stöðu innflytjenda hér, en samkvæmt nýjustu gögnum Hagstofu Íslands (frá 2017) um stöðu innflytjenda á vinnumarkaði hérlendis þá skiptir mun meira máli hvort viðkomandi er innflytjandi eða Íslendingur en hvort viðkomandi er karl eða kona. Hlutfall starfsfólks sem fær ekki starf miðað við menntun var samkvæmt þessum gögnum 2017 2,8% fyrir íslenska karla og 4,3% fyrir íslenskar konur, en 10,8% fyrir erlenda karla og 16,7% fyrir erlendar konur (eða 1 af hverjum 6). Svipaðar hlutfallstölur voru árin áður, en ögn lægri fyrir alla hópa.

2. Samráð

2.1 Skilgreining framkvæmdaaðila, samstarfsaðila og hagsmunaaðila

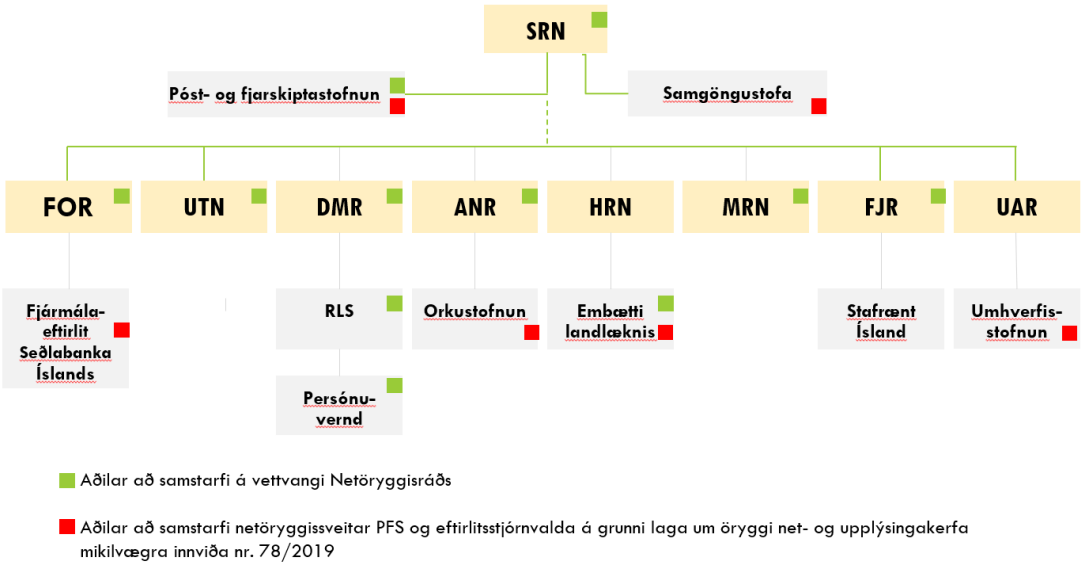
Netöryggi snýst um öryggi og traust þeirrar þjónustu sem veitt er á Netinu og í nútímasamfélagi er nánast öll þjónusta og starfsemi orðin háð Netinu með einum eða öðrum hætti.

Af hálfu stjórnvalda koma margir aðilar að skipulagi og mótun netöryggismála, ýmist með beinum hætti lögum samkvæmt eða óbeint. Fyrirhuguð stefnumótun var kynnt sérstaklega fyrir lykilráðuneytum er fara með málefni tengd netöryggi. Netöryggisráð[11] er formlegur samstarfsvettvangur þeirra ráðuneyta og stofnana sem gegna stóru hlutverki á þessu sviði í stjórnsýslunni og er það mikilvægur samráðsvettvangur í mótun hinnar nýju stefnu. Þessi drög að grænbók verða birt í samráðsgátt stjórnvalda og verða í kjölfarið til umræðu á samráðsfundi sem haldinn verður þann 28. apríl nk. Framkvæmdaaðilar, samstarfsaðilar og ýmsir hagsmunaaðilar verða boðaðir á fundinn (sjá eftirfarandi umfjöllun um þessa aðila).

Stjórnskipan netöryggismála má sjá í eftirfarandi skipuriti. Samgöngu- og sveitarstjórnarráðuneytið (SRN) hefur þar, samkvæmt forsetaúrskurði[12], samhæfingarhlutverk (heiti ráðuneyta og stofnana eru skammstöfuð á myndinni).

[11] Netöryggisráð var sett á stofn í nóvember 2015 sem vettvangur samráðs og samstarfs innan stjórnkerfisins í málefnum er varða netöryggi. Ráðið hefur umsjón með framkvæmd gildandi netöryggisstefnu (sjá nánar hér að aftan), samhæfir aðgerðir og miðlar upplýsingum. Það 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 netöryggissveit hennar. Með lögum um netöryggi sem tóku gildi 1. september 2020 var settur ákveðinn rammi um starf Netöryggisráðs.

[12] Forsetaúrskurður nr. 119/2018 um skiptingu stjórnarmálefna milli ráðuneyta í Stjórnarráði Íslands



Stýrihópurinn hélt reglulega fundi með Netöryggisráði, sem gegnir hlutverki framkvæmdaaðila í stefnumótunarverkefninu. Á vettvangi Netöryggisráðs fór fram mikilvæg umræða og samráð, m.a. var rætt um stöðuna í netöryggismálum í heild, um framgang einstakra verkefna og stöðu mála og þróun í nágrannaríkjum.

Formlegir samstarfsaðilar eru fyrst og fremst stjórnvöld sem falið er hlutverk skv. lögum um netöryggi nr. 78/2019. Að auki hafa ýmsar stofnanir og aðrir aðilar komið að samstarfi um ýmis netöryggismál með virkum hætti.

Til hagsmunaaðila teljast í fyrsta lagi þeir aðilar sem lögum samkvæmt eiga ákveðinna hagsmuna að gæta, einkum mikilvægir innviðir samkvæmt lögum um netöryggi nr. 78/2019 (þ. á m. rekstraraðilar nauðsynlegrar þjónustu), fjarskiptafyrirtæki og opinberar stofnanir. Ennfremur teljast til hagsmunaaðila ýmsir þeir sem veita netöryggisþjónustu, netöryggisháða þjónustu eða eru háðir öryggi Netsins vegna atvinnu sinnar og síðast en ekki síst öll fyrirtæki og almenningur í landinu, því nær öll þjónusta byggir að einhverju leyti á Netinu og stafrænum lausnum og er þar með háð öryggi þjónustunnar.

3. Stöðumat

3.1 Greining á stöðu netöryggis hérlendis

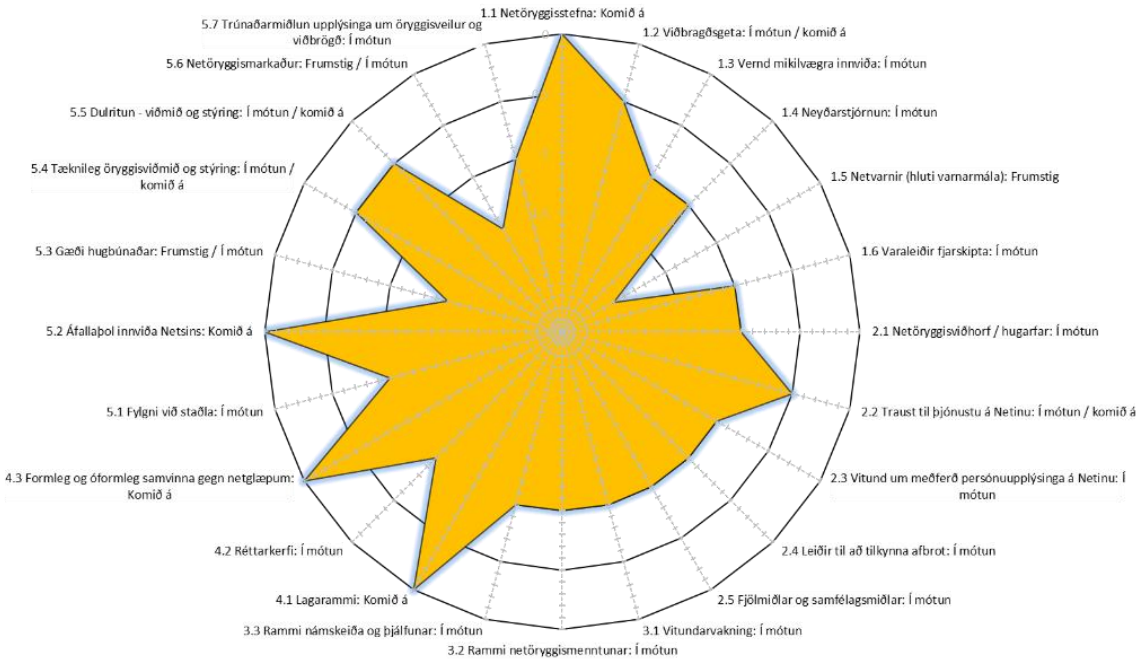
Við eftirfarandi mat á stöðu netöryggismála á Íslandi var ákveðið að nýta úttektir þriggja virtra erlendra aðila sem hafa metið stöðuna hér á landi með sömu aðferðum og þær hafa metið stöðuna í öðrum löndum. Að auki er tekið mið af niðurstöðum tæknilegra úttekta og einnig lagt mat á þætti sem kunnugt er um en ekki hafa verið teknir út í úttektum. Niðurstöður eru síðan teknar saman í lok þessa kafla.

Stöðu netöryggis má meta með ýmsum hætti, allt frá því að skoða tæknilega þætti kerfa, öryggisskipulag rekstraraðila og upp í að gera heildstætt mat á samfélaginu í heild. Háskólinn í Oxford bauðst, á grunni óformlegs samstarfs, til að gera heildstæða úttekt á stöðu netöryggis í íslensku samfélagi og var hún framkvæmd í júní 2017. Þótt tæp fjögur ár séu liðin frá úttektinni og staðan hafi batnað á mörgum sviðum, þá standa ýmsir þættir samfélagslegrar lýsingar enn fyrir sínu. Aðrar úttektir sem hér er vísað til hafa verið gerðar af mismunandi aðilum, á mismunandi forsendum og á mismunandi tímum. Slíkt er auðvitað galli, eigi að nota úttektirnar til samanburðar, en sé hugað að forsendunum með viðeigandi hætti þá er það kostur að geta nýtt þessar ólíku úttektir sem taka á mismunandi hliðum netöryggis. Í þessum kafla verður því gerð grein fyrir niðurstöðum hverrar úttektar fyrir sig og niðurstöður dregnar saman í lokin. Jafnframt er í næsta undirkafla, *Mat á árangri gildandi stefna*, fjallað um það sem hefur áunnist á liðnum árum.

3.1.1 Úttekt Háskólans í Oxford 2017

Úttekt Háskólans í Oxford er sú ítarlegasta sem gerð hefur verið á stöðu netöryggis hérlendis, því ólíkt öllum öðrum úttektum byggðist hún á ítarlegum viðtölum við fólk úr mismunandi geirum samfélagsins. Úttektin var gerð með sambærilegum hætti og sami hópur á vegum háskólans hafði gert í öðrum löndum. Hún var framkvæmd 21.-23. júní 2017. Upplýsingar um úttektina, samantekt og úttektarskýrsluna sjálfa má nálgast hér:

https://www.stjornarradid.is/efst-a-baugi/frettir/stok-frett/2018/04/30/Uttekt-Oxford-haskola-a-stodu-netoryggis-og-adgerdir-til-eflingar-thess/



Niðurstöður úttektarinnar eru teknar saman á myndinni hér að framan. Tuttugu og fjórir þættir voru metnir og einkunn gefin fyrir hvern um sig. Hér má sjá dreifingu einkunna frá „á frumstigi“ (næst miðju) til „komið á“ (fjærst miðju) (sjá nánar í viðauka, kafla 6.2.1).

3.1.2 Úttekt ITU 2020

Alþjóðafjarskiptasambandið gerir reglulega úttektir á stöðu netöryggis ríkja út frá matskerfi sem sambandið hefur útbúið. Niðurstöður hvers ríkis eru birtar sem *netöryggisstuðull* (e. *Global Cybersecurity Index*). Í síðustu úttekt sem birt var 2018 var Ísland í 42. sæti af 46 ríkjum Evrópu og í 87. sæti á heimsvísu af 175 ríkjum. Gögnum var safnað án milligöngu stjórnvalda og því hvorki tekið mið af árangri sem ekki var búið að kynna alþjóðlega á þeim tíma né því sem hefur áunnist síðan 2018. Ljóst er að margt má bæta þó talið sé að staðan í dag sé betri en þessar niðurstöður bera með sér.

ITU hóf söfnun gagna vegna næstu úttektar í árslok 2019 og hefur viðeigandi gögnum verið skilað. Þó formleg niðurstaða liggi ekki fyrir má, út frá svörum sem skilað var, m.a. draga eftirfarandi ályktanir varðandi Ísland:

- Æskilegt er að huga að endurmati refsilöggjafar, t.d. hefur verið bent á að lagaumhverfi er ófullnægjandi varðandi auðkennastuld á Netinu (e. *online identiy theft*).
- Þörf er á skipulagðri vitundarvakningu og fræðslu á vegum stjórnvalda. Sérstaklega þarf að huga að vitundarvakningu og viðeigandi upplýsingamiðlun til viðkvæmra hópa (verkefni til að ráða bót á þessu er nú þegar í gangi).

- Stjórnvöldum ber skylda til að tryggja vernd barna og ungmenna á Netinu óháð því hvort frjáls félagasamtök sinna slíkum verkefnum (og án tillits til þess hvort starf þeirra sé unnið skv. samningi við stjórnvöld).
- Framkvæma þarf skipulegar úttektir á netöryggi á landsvísu út frá skilgreindum öryggisviðmiðum (e. *cybersecurity audits performed at a national level*).
- Menntun:
    - Netöryggi þarf að vera tilvísanlegur þáttur í námskrá grunn- og framhaldsskóla. Það þarf einnig að vera í boði á háskólastigi, ef ekki sem heildstæð námsbraut þá a.m.k. sem námsgrein.
    - Stjórnvöld verða að þróa/styðja viðeigandi netöryggisnámskeið fyrir mismunandi geira atvinnulífs og samfélagsins í heild. Sérstaklega þarf að huga að námskeiðum (á landsvísu) fyrir lítil og meðalstór fyrirtæki (e. *SMEs*) og opinberar stofnanir.
    - Netöryggismenntun og hæfni sérfræðinga þarf að vera vottanleg samkvæmt vottunarkerfi.
- Rannsóknir og þróun:
    - Þörf er á að móta áætlun sem miðar að því að styrkja rannsóknir og þróun á sviði netöryggis á landsvísu og auka virkni háskóla og rannsóknastofnana á þessu sviði.
    - Í flóru atvinnuveganna þarf netöryggi að vera til sem atvinnugrein (þ.e. að til séu fyrirtæki sem eru sérhæfð í ýmsum þáttum netöryggis) og stjórnvöld verða að styðja þróun á því sviði.

3.1.3 Eftirfylgni við framkvæmd Búdapest-samningsins

Ísland gerðist nokkuð snemma aðili að samningnum um netglæpi eða *Búdapest-samningnum*[13] eins og hann er oft nefndur. Samningurinn gerir ýmsar kröfur til löggjafar aðildarríkja svo unnt sé að rannsaka netglæpi þvert á landamæri og lögsækja sakamenn eftir því sem við á. Nefnd með fulltrúum aðildarríkja fylgist með hvernig samningnum er framfylgt í aðildarríkjum og gefur út leiðbeiningar um hvernig hann beri að túlka eftir því sem netglæpir þróast. Ísland uppfyllti að mestu kröfur samningsins með því að vísa í hvernig þær væru innleiddar í gildandi lögum. Við úttektir hafa þó komið fram ábendingar sem gefa tilefni til að skoða betur hversu vel ýmis ákvæði íslenskrar refsilöggjafar ná til aðstæðna sem geta komið upp á Netinu. Mikilvægt er að bregðast við þar sem alþjóðleg brotastarfsemi leitar skipulega að veikri löggjöf til að tryggja sér sem best athafnafrelsi.

[13] Sjá: https://www.coe.int/en/web/cybercrime/tcy

3.1.4 Vélræn veikleikaskimun

Þegar *Stýrihópur um netöryggi stjórnsýslunnar,* fyrir hönd ráðuneytanna, gerði samning við Póst- og fjarskiptastofnun (PFS) um netöryggisþjónustu við Stjórnarráðið var það fyrsti samningur sinnar tegundar sem PFS gerði. Í honum var lögð áhersla á að fá aðgang að vélrænni veikleikaskimun sem gerð er alþjóðlega og netöryggissveit PFS hefur aðgang að. Áhersla Stjórnarráðsins á að fá aðgang að slíku mati byggðist bæði á nauðsyn þess að finna veikleika og ráða bót á þeim en einnig á mikilvægi þess að vita hver ásýnd Íslands er í augum þeirra sem geta keypt sér slíkt mat (geta jafnvel verið óheiðarlegir aðilar).

Stöðumat fyrir tímabilið febrúar 2020 – febrúar 2021 sýnir svipaða stöðu á Íslandi og hjá viðmiðunarlöndum (um 3% neðan við Noreg og Bretland) og allir metnir flokkar samfélagslegra mikilvægra innviða[14] á Íslandi hafa betri stöðu (um 20%) en heildarmeðaltal á Íslandi. Þessi staða hefur haldist nokkuð óbreytt, en áfram er unnið að því að gera þetta mat nákvæmara. Sé Ísland í heild borið saman við t.d. Noreg er því ekki mikill munur milli ríkjanna. Séu ákveðnar stofnanir eða fyrirtæki skoðuð má hins vegar sjá veikleika sem bæta þarf úr. Matið er því helst notað við hnitmiðuð umbótaverkefni þar sem ákveðinn flokkur stofnana er tekinn fyrir.

3.1.5 Úttekt á veikleikum í kerfum hjá ríkinu

Ýmsar úttektir hafa verið gerðar á veikleikum í öryggi kerfa hjá ríkinu og hefur stofnunum í kjölfarið verið bent á það sem lagfæra þurfi. Kerfislægur veikleiki í netrekstri ríkisins er hversu margar gáttir eru út á Netið, en það gerir netvarnir mun erfiðari en ella.

Einnig hafa ófullnægjandi öryggisuppfærslur víða verið veikur hlekkur og hafa kannanir leitt í ljós að oftast er um vankunnáttu að ræða. Hafa ábyrgðamenn gagna og kerfa talið að slíkar uppfærslur væru inni í þjónustusamningum við rekstraraðila kerfanna þótt um það hafi ekki verið samið. Meðal aðgerða sem stjórnvöld hafa gripið til er fræðsla og að láta útbúa almennan samningsviðauka sem nær til þessara atriða. Enn fremur hefur fjármála- og efnahagsráðuneytið sett til samráðs í samráðsgátt drög að leiðbeiningum um upplýsingaöryggi og er það hluti verkefnisins um landsarkitektúr fyrir opinber upplýsingakerfi.

3.1.6 Samantekt á stöðumati

Þótt góður árangur hafi náðst hvað snertir marga þætti netöryggis á umliðnum árum (sjá næsta kafla með mati á gildandi stefnu), þá benda niðurstöður úttekta

[14] Hér er átt við fjármálastofnanir, orkufyrirtæki, vatnsveitur, flutningsfyrirtæki, heilbrigðisstofnanir, eftirlitsstjórnvöld og Stjórnarráðið. Fjarskiptafyrirtæki fá lægri einkunn, en það er vegna þess að matið byggist ekki eingöngu á fyrirtækjunum sjálfum heldur að verulegu leyti á viðskiptavinum þeirra.

gjarnan á ákveðin *skipulagsleg atriði og aðgerðir* sem huga þarf að og bæta. Í því samhengi má nefna:

- Skipulega vitundarvakningu og fræðslu, byggða á þarfagreiningu.
- Skipulega greiningu netógna og kynningu á netógnamati.
- Þátttöku (og skipulagningu) innlendra og alþjóðlegra netöryggisæfinga.
- Menntun (á öllum stigum skólakerfis og sérhæfð námskeið fyrir mismunandi hópa).
- Rannsóknir og þróun.
- Regluverk, staðla, kröfur (t.d. varðandi innkaup búnaðar og þjónustu), öryggisvottanir.
- Lagaumhverfi.

Jafnframt er ljóst að huga þarf að fleiri veikleikum sem ekki endurspeglast endilega í mati utanaðkomandi aðila:

- Auka þarf enn frekar áfallaþol og viðbragðsgetu í íslenskri stjórnsýslu, atvinnulífi og innviðum almennt í ljósi vaxandi netógna.
- Tryggja þarf að í allri stefnumótun og ákvarðanatöku sem varðar uppbyggingu netháðrar þjónustu, t.d. í samningum um þróun, rekstur og hýsingu kerfa og gagna verði framkvæmt áhættumat og öryggismálum gerð rækileg skil. Sérstaklega þarf að huga að skýjavinnsluþjónustu.
- Efla þarf samstarf og samhæfingu er varðar netöryggi, innan stjórnkerfisins, atvinnulífsins og á milli þessara aðila.
- Þar sem Ísland er eyja með ákveðna takmörkun tenginga við umheiminn verður áhættumat vegna netháðrar kjarnaþjónustu að taka mið af hugsanlegu sambandsrofi við umheiminn. Hið sama má segja um byggðir úti á landi sem geta lent í fjarskiptarofi. Til viðbótar koma einnig mikilvæg atriði svo sem hvort ákveðin gögn þurfi alltaf að vera tiltækileg í íslenskri lögsögu eða jafnvel að þau megi ekki fara úr íslenskri lögsögu. Skýrt öryggismiðað skipulag byggt á traustum lagagrunni er forsenda þess að unnt sé að nýta skýjalausnir með skilvirkum hætti, þannig að einfalt sé að flokka hvaða gögn megi vista með hvaða hætti og hvar.

3.2 Mat á árangri gildandi stefna

3.2.1 Árangur sem hefur náðst á síðustu árum og með gildandi fjarskiptaáætlun

Umbætur netöryggismála undanfarin tvö ár hafa verið gerðar á grunni gildandi fjarskiptastefnu og áætlunar fyrir 2019 – 2021. Ítarlegasta úttekt sem gerð hefur verið á stöðu netöryggis hérlendis er sú sem Háskólinn í Oxford gerði í júní 2017, þar sem staða fjölmargra netöryggisþátta í samfélaginu var metin. Í kjölfarið var ráðist í margvíslegar umbætur. Í ljósi þess hve ítarleg Oxford-úttektin var hefur árangur umbótaverkefna verið flokkaður eftir þeirri flokkun sem beitt var þá. Hér

að aftan er yfirlit um ýmislegt sem hefur áunnist, nákvæmari lýsing á hvernig einstakir þættir tengjast fjarskiptaáætlun má finna í viðauka (kafla 6.1). Kaflaskipting í upptalningu hér að neðan og tölur í sviga vísa til númers þáttar í Oxford-líkaninu, sbr. mynd á bls. 12 og nánari lýsingu í viðauka, kafla 6.2.1. Að auki er vísað til gildandi fjarskiptaáætlunar þar sem við á. (Í viðauka er fjallað ítarlega um árangur út frá fjarskiptaáætlun, sjá kafla 6.1).

a) Netöryggisstefna (og skipulag)
   - Með nýrri netöryggislöggjöf sem tók gildi 1. september 2020 var komið á lögfestu skipulagi varðandi netöryggi mikilvægra innviða að evrópskri fyrirmynd. Eftirlit með kröfum um viðeigandi umgjörð áhættustýringar í rekstri mikilvægra innviða í skilningi laganna[15] og tilkynningaskyldu um öryggisatvik er falið eftirlitsstjórnvöldum, hverju á sínu sviði.[16] Póst- og fjarskiptastofnun er bæði eftirlitsstjórnvald og falið samhæfingarhlutverk sem stuðla á að samræmdri framkvæmd (þættir 1.2 og 1.3).
   - Netöryggissveit Póst- og fjarskiptastofnunar (CERT-IS) fékk með lögunum miðlægt samhæfandi hlutverk og þjónustuhópur hennar útvíkkaður verulega frá því sem áður var. Sveitin hefur verið efld verulega m.t.t. mannauðs, tækjabúnaðar og samvinna aukin við innlenda sem erlenda aðila. Viðbragðsáætlun hefur verið þróuð í samvinnu við þjónustuhóp sveitarinnar og komið að góðum notum. Ennfremur hefur almannavarnadeild ríkislögreglustjóra þróað viðbragðsáætlun vegna alvarlegra atvika í samvinnu við netöryggissveitina. Til slíkrar áætlunar getur þurft að grípa vegna alvarlegra netavika með víðtæk samfélagsleg áhrif. (þáttur 1.4).
   - Netöryggisráð sem starfað hefur frá 2015 á sér nú stoð í hinni nýju netöryggislöggjöf.
   - Utanríkisráðuneytið hefur eflt ýmis konar starf til að taka á netöryggi sem hluta varnarmála, m.a. í kjölfar skýrslu Björns Bjarnasonar um þróun norræns samstarfs á sviði utanríkis- og öryggismála. Í skýrslunni er fjallað um nauðsyn þess að Norðurlöndin efli varnir og viðbragðsgetu við svokölluðum fjölþáttaógnum, þ.m.t. netógnum. Stofnuð hefur verið ný deild fjölþáttaógna sem mun hafa forgöngu um uppbyggingu þekkingar og getu innan utanríkisráðuneytisins á þessu sviði og halda utan um uppbyggingu samstarfs við hlutaðeigandi stofnanir innanlands og alþjóðasamstarf. Undirbúningur fyrir aðild Íslands að netöryggissetrinu í Tallinn, í

[15] Þ.e. annars vegar svonefndir rekstraraðilar nauðsynlegrar þjónustu og hins vegar veitendur stafrænnar þjónustu.

[16] Fjármálaeftirliti Seðlabanka Íslands t.d. að því er nauðsynlega þjónustu á sviði bankastarfsemi varðar, Samgöngustofu að því er nauðsynlega þjónustu á sviði flutningastarfsemi varðar og embætti landlæknis á sviði heilbrigðisþjónustu.

samræmi við tillögur Háskólans í Oxford (2017), er hafinn og einnig að öndvegissetrinu um fjölþáttaógnir í Helsinki (þáttur 1.5). Aðild að setrunum kemur til með að auka aðgengi hérlendra sérfræðinga að sérhæfðum námskeiðum og vinnustofum umtalsvert frá því sem nú er.

- Ísland hefur verið í forystu varðandi aðgengi að og styrk fjarskiptatenginga,[17] en fjarskiptakerfi hafa takmarkaðan líftíma og rekstur, viðhald og endurnýjun því viðvarandi verkefni allra samfélaga. Unnið hefur verið að eflingu fjarskiptainnviða, t.d. til að geta betur tekist á við náttúruhamfarir en um leið hefur áfallaþol nettenginga aukist (þáttur 1.6).
- Virk samvinna hefur verið við ITU vegna heildrænnar úttektar á netöryggi á landsvísu út frá skilgreindum öryggisviðmiðum líkt og stefnt er að í gildandi fjarskiptastefnu- og áætlun. Samvinna í þessum efnum er mikilvæg og viðvarandi viðfangsefni stjórnvalda, svo og reglulegt árangursmat og eftirfylgni með nauðsynlegum úrbótum.
- Ísland á aðild að nýlegri samevrópskri ráðherrayfirlýsingu um mikilvægi öflugra gagnatenginga innan Evrópu og til annarra heimsálfa (e. *The European Data Gateways Declaration*) fyrir fjölbreytta stafræna þróun í Evrópu.[18]

b) Netöryggismenning og samfélag

- Viðburðir hafa verið skipulagðir til að efla netöryggisvitund (m.a. netöryggismánuður og netöryggiskeppnir, ráðstefnur hafa verið haldnar sem og samhæfð íslensk þátttaka í alþjóðlegum ráðstefnum) (þáttur 2.1).
- Með nýlegri persónuverndarlöggjöf, markvissum undirbúningi Persónuverndar fyrir gildistöku laganna og eftirfylgni með kröfum til vinnslu persónuupplýsinga, ekki síst öryggisráðstafana, hefur mikil vitundarvakning orðið á því sviði (þáttur 2.3).
- Leiðir til að tilkynna um öryggisbresti og netglæpi hafa verið bættar með tilkynningagátt á Netinu[19] (þáttur 2.4).
- Jafnframt hefur lögreglan haldið úti ýmsu forvarnastarfi og almannatengslum á samfélagsmiðlum. Fjármálastofnanir hafa einnig verið virkar á þessu sviði.

---

[17] Á virkum samkeppnismarkaði á sviði fjarskipta hefur uppbygging markaðsaðila á nýjum fjarskiptainnviðum og þjónustu náð til um og yfir 95% þjóðarinnar.

[18] https://www.stjornarradid.is/efst-a-baugi/frettir/stok-frett/2021/03/19/Sigurdur-Ingi-undirritadi-samevropska-radherrayfirlysingu-um-gagnaflutninga/

[19] Tilkynningagáttin um öryggisatvik, https://oryggisbrestur.island.is/, var opnuð í maí 2020. Hún er samvinnuverkefni samgöngu- og sveitarstjórnarráðuneytis, Persónuverndar, Póst- og fjarskiptastofnunar/CERT-IS og Lögreglunnar.

- Fjölmiðlar hafa sýnt netöryggi vaxandi áhuga á undanförnum árum og sjást þess merki í fjölda greina og viðtala um netöryggismál. (þáttur 2.5).

c) Netöryggismenntun, þjálfun og hæfni
   - Unnið er að greiningu á því í hvaða hópum samfélagsins sé mest þörf fyrir vitundarvakningu um netöryggi. Í kjölfarið verður brugðist við með viðeigandi hætti (þáttur 3.1).
   - Samningur hefur verið undirritaður við Norska tækniháskólann (NTNU) og býðst íslenskum stúdentum þar framhaldsnám í netöryggisfræðum, þar á meðal öryggisfræðum sem óvíða annars staðar standa útlendingum til boða. Erlendir kennarar hafa einnig kennt netöryggisnámskeið við íslenska háskóla (þáttur 3.2).
   - Ýmis stutt netöryggisnámskeið og -þjálfun hafa verið í boði innanlands (þáttur 3.3).

d) Lagalegt umhverfi (og löggæsla)
   - Lög nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða eru fyrstu heildstæðu lög sem sett hafa verið um netöryggi á Íslandi og marka tímamót að því leyti.
   - Lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga hafa markað tímamót í kröfum er varða netöryggi og örugga vinnslu upplýsinga.
   - Lögreglumenn hafa í vaxandi mæli sótt sér netöryggismenntun af ýmsu tagi. Að auki eru netöryggistengdar greinar nú meðal námsgreina í lögreglunámi við Háskólann á Akureyri (þáttur 4.2).

e) Staðlar, skipulag og tækni
   - Með nýjum netöryggislögum (sem tóku gildi 1. september 2020) þurfa rekstraraðilar mikilvægra innviða að sýna fram á öryggi sinna kerfa með ýmsum hætti og munu tilvísanir til viðeigandi staðla gegna þar lykilhlutverki (þáttur 5.1).
   - Stórtæk uppbygging stafrænnar þjónustu hins opinbera stendur nú yfir hérlendis á vegum fjármála- og efnahagsráðuneytisins (*Stafrænt Ísland*). Þar er m.a. lögð áhersla á að nota grunnkerfi hönnuð með öryggi í huga (sbr. Straumurinn, „X-Road“) (þáttur 5.3).
   - Ýmis konar framboð á netöryggisþjónustu og vörum hefur aukist jafnt og þétt. Markaður á þessu sviði virðist vera í örri þróun m.a. vegna aukinnar áherslu fyrirtækja á að hafa öryggismálin í lagi, aukins skilnings á mikilvægi öryggisstaðla og hlítni við þá, aukinna öryggiskrafna frá opinberum aðilum og krafna í löggjöf (þáttur 5.6).
   - Vaxandi umræða hefur verið um þörf fyrir ábyrga (trúnaðar)miðlun viðkvæmra upplýsinga m.a. milli viðbragðsaðila og ábyrgðarmanna kerfa, enda mikilvægt að unnt sé að miðla slíkum upplýsingum með skipulegum og ábyrgum hætti (þáttur 5.7).

Þótt enn megi margt bæta og nýjum áskorunum fjölgi með örri þróun nettækninnar, þá er ljóst að brugðist hefur verið við ábendingum um þá þætti þar

sem endurbóta þótti helst þörf og staða netöryggis er því mun betri en niðurstöður úttektar í júní 2017 báru með sér.

Núgildandi fjarskiptaáætlun nær til áranna 2019 – 2023 og miðað við að það tímabil er nú (apríl 2021) um það bil hálfnað hefur framgangur verkefna verið góður og samkvæmt áætlun þegar á heildina er litið. Stórir áfangar náðust með gildistöku netöryggislöggjafar í september 2020 og með eflingu netöryggissveitar PFS ásamt fjölgun starfa í öðrum deildum PFS sem helguð eru netöryggismálum. Nánar er gerð grein fyrir verkefnum áætlunarinnar og framgangi verkefna hennar í viðauka, kafla 6.1.

3.2.2 Alþjóðleg staða

Utanríkisráðuneytið hefur í vaxandi mæli tekið þátt í alþjóðlegum verkefnum og fundum um netöryggismál[20]. Með samningi sem samgöngu- og sveitarstjórnarráðuneytið gerði við Norska tækniháskólann (NTNU) býðst Íslendingum þátttaka í alþjóðlegu rannsókna- og þróunarsamstarfi sem þar fer fram.

Samkvæmt alþjóðlegum úttektum hefur Ísland verið í fararbroddi þegar kemur að fjarskiptainnviðum og nýtingu Netsins. Slíkar úttektir hafa hins vegar ekki sýnt jafn góða stöðu fyrir Ísland þegar kemur að netöryggi. Að hluta til er skýringin sú að um mat á ásýnd en ekki stöðu hefur verið að ræða. Gagna hefur þá ekki verið aflað í samvinnu við hlutaðeigandi innlenda aðila, heldur byggt á því efni sem finna má á Netinu. Dæmi um slíka úttekt á Íslandi má finna í viðauka, kafla 6.3.

3.3 Netöryggi sem hluti utanríkis-, öryggis- og varnarmála

Öryggisumhverfi ríkja hefur tekið stakkaskiptum síðastliðin ár og áratug. Helstu einkenni breytts öryggisumhverfis eru óskýrari skil á milli borgaralegs öryggis og hernaðarlegs öryggis, svo og á milli þess sem telst til innanríkismála, utanríkismála og alþjóðamála. Ör tækniþróun og aukinn hraði í upplýsingamiðlun eykur flækjustigið og kröfur um og þörf fyrir aukinn viðbragðshraða eykst.

Utanríkisráðuneytið fer með varnarmál og ber samkvæmt varnarmálalögum að hafa yfirsýn um þær ógnir og hættur sem steðjað geta að íslenskri þjóð og forráðasvæði og eiga upptök sín í hinu alþjóðlega umhverfi. Mikilvægi netöryggis og -varnarmála hefur vaxið í allri umræðu um þjóðaröryggi innanlands sem og í umræðum á vettvangi alþjóðastofnana og í tvíhliða samstarfi.

Atlantshafsbandalagið hefur skilgreint netheima sem eitt af aðgerðasviðum bandalagsins (e. *domain of operations*) til jafns við aðgerðasvið í lofti, láði og legi. Þótt netöryggi og netvarnir séu fyrst og síðast á ábyrgð aðildarríkjanna sjálfra

[20] Sjá kafla 3.2.1 að framan og næstu kafla hér á eftir.

hafa þau skuldbundið sig til að gera allt sem í þeirra valdi stendur til að efla varnir innviða og netkerfa (e. *Cyber Defence Pledge*) og hafa þar til hliðsjónar grundvallarviðmið um viðnámsþol borgaralegra fjarskiptakerfa (e. *Baseline Requirements for Resilient Civil Communication Systems*). Lögð er áhersla á að fjarskipta- og netkerfi geti staðið af sér hættuástand og að forgangsaðgengi stjórnvalda að öflugum og öruggum fjarskiptakerfum á hættutímum sé tryggt.

Gott samráð innanlands, öflug samræming, samvinna og uppbygging þekkingar, ferla og viðbragðskerfa skiptir miklu máli fyrir öryggi og varnir landsins. Í alþjóðlegu samhengi hefur slíkt áhrif á orðspor og ímynd Íslands. Netöryggi er ekki síður mikilvægt fyrir samkeppnisstöðu og trúverðugleika Íslands í margvíslegu samhengi, t.d. fyrir atvinnulíf, hagkerfið allt og fjármálastöðugleika.

Öryggisumhverfi nútímans krefst samstarfs þvert á ráðuneyti og stofnanir. Ljóst má vera að það að tryggja viðeigandi netöryggi í íslensku samfélagi er viðvarandi áskorun og samfélagsleg ábyrgð allra. Samvinna innlendra aðila hefur verið góð en reglulegt endurmat m.t.t. hlutverka- og ábyrgðarskiptingar ólíkra aðila er mikilvægt, frá einum tíma til annars.

3.4 Þróun í nágrannalöndum og áskoranir Íslands

Norðurlöndin hafa unnið að því að efla samráð á vettvangi norræna varnarsamstarfsins (NORDEFCO), í samstarfi NB8 ríkjanna auk þess sem utanríkisráðherrar Norðurlandanna hafa aukið samráð um netöryggismál á vettvangi N5 samstarfsins. Þá eiga norrænir sérfræðingar og embættismenn á ýmsum stigum stjórnsýslunnar reglulegt samráð um netöryggismál. Netöryggismál eru og í auknum mæli viðfangsefni í tvíhliða samræðum ríkja um öryggis- og varnarmál. Bretland og Bandaríkin hafa á umliðnum árum lagt stóraukna áherslu á netöryggis og -varnarmál í stefnum sínum og endurspeglast þetta í samskiptum þeirra við önnur ríki, þ.m.t. Ísland. Þá eru netöryggismál, eðli málsins samkvæmt, æ stærri þáttur í störfum öryggisþjónusta nánustu vina- og bandalagsríkja Íslands með áherslu á þverfaglegt og alþjóðlegt samstarf.

Netöryggisstofnun Evrópu (ENISA) gegnir vaxandi hlutverki í evrópsku netöryggissamstarfi í kjölfar ákvörðunar um að útvíkka starfssvið hennar 2019.[21]

Á vettvangi Atlantshafsbandalagsins hefur Ísland lýst viðleitni og vilja til að efla varnir netkerfa, en bandalagið gerir ráð fyrir því að ríki geti greint, varist og

[21] Meðal nýlegra skýrslna stofnunarinnar má nefna: ENISA AI Threat Landscape Report Unveils Major Cybersecurity Challenges https://www.enisa.europa.eu/news/enisa-news/enisa-ai-threat-landscape-report-unveils-major-cybersecurity-challenges (15. desember 2020) Updated ENISA 5G Threat Landscape Report to Enhance 5G Security https://www.enisa.europa.eu/news/enisa-news/updated-enisa-5g-threat-landscape-report-to-enhance-5g-security (14. desember 2020) New Guidelines for Telecom and 5G Security https://www.enisa.europa.eu/news/enisa-news/new-guidelines-for-telecom-and-5g-security (10. desember 2020)

brugðist við netógnum með viðunandi hætti. Til þess að sú verði raunin þarf að efla viðnámsþol og getu til að verjast ógnum og árásum. Bandalagið leggur til mikilvæg viðmið og veitir stuðning en slíkt kemur ekki í stað varna og góðrar samhæfingar aðila innanlands.

Á vettvangi Öryggis- og samvinnustofnunar Evrópu (ÖSE) hafa verið samþykktar aðgerðir, sem ætlað er að draga úr hættu á átökum sem stafa af notkun upplýsinga- og samskiptatækni. Unnið hefur verið að því að styrkja hlutverk stofnunarinnar í þessum efnum.

Þótt margt hafi áunnist á sviði netöryggis innan Evrópu, t.d. Búdapest-samningurinn, NIS (1 og 2) og margvíslegt starf ENISA, þá er ekki unnt að horfa fram hjá því að ríki heims hafa ekki komið sér saman um alþjóðlegt regluverk að því er varðar netöryggi eða mögulegt gildissvið þess. Allsherjarþing Sameinuðu þjóðanna hefur viðurkennt að Netið, upplýsingatækni og notkun hennar hafi áhrif á alþjóðasamfélagið í heild. Einnig að skilvirkni í málaflokknum aukist með alþjóðlegri samvinnu. Gera má ráð fyrir að þörf fyrir og krafan um alþjóðlega samvinnu komi til með að aukast á komandi árum.

Alþjóðlega er aukin áhersla lögð á mikilvægi borgaralega innviða og viðnámsþols sem hluta af vörnum ríkja. Alþjóðlegar skuldbindingar Íslands á sviði netöryggis og -varnarmála gera kröfur um nauðsynlegar varnir og trausta innviði og frekari eflingu þeirra. Ísland þarf vera í stakk búið til þess að geta varist, aðlagast og mætt netógnum og -árásum. Því til grundvallar þarf að liggja reglulegt mat og greining á áhættu og veikleikum, einkum með tilliti til þeirra innviða og kerfa sem teljast mikilvæg vegna þjóðaröryggis og alþjóðlegra skuldbindinga Íslands.

3.4.1 Stefnumörkun á vettvangi ESB

Hin íslensku netöryggislög, lög nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða, sem tóku gildi 1. september 2020 taka að verulegu leyti mið af kröfum svonefndrar NIS-tilskipunar (NIS1), sem birt var 2016 en tafist hefur að taka upp í EES-samninginn og hefur því enn ekki öðlast formlega gildi í EFTA-ríkjunum innan Evrópska efnahagssvæðisins. Ákveðin kaflaskil urðu í netöryggismálum um miðjan desember 2020 þegar nýr netöryggispakki ESB, *Cybersecurity package*,[22] var birtur á vef ESB. Lykilatriði í honum eru ný netöryggisstefna ESB[23] og tillaga um endurnýjaða útgáfu NIS tilskipunarinnar, NIS2.[24] Í gildandi tilskipun (NIS1) eru gerðar tilteknar kröfur til útfærslu netöryggisstefnu sérhvers ríkis og í nýju NIS2 tillögunni er lagt til að gerðar verði

[22] Sjá: https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en

[23] Sjá: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade

[24] Sjá: https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union
Beinn hlekkur á texta draga að NIS 2: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166

enn frekari kröfur í þeim efnum, sem verða væntanlega bindandi fyrir Ísland. Sjá nánar í viðauka (kafla 6.4.1). Í NIS2-tillögunni er einnig lagt til að fleiri svið samfélagsins verð felld undir tilskipunina, **gildissvið hennar verði** með öðrum orðum víðtækara en á við um NIS1.

Að auki má nefna að eitt meginverkfæra Evrópusambandsins við nýsköpun hinnar stafrænu Evrópu er *Digital Europe Programme* (DEP).[25] Ísland getur tekið þátt í þessari samstarfsáætlun, m.a. verkefnum sem tengjast netöryggi, beint sem óbeint og þar eru tækifæri til að afla styrkja til slíkra verkefna. Meðal verkefnaflokka í boði eru verkefni sem tengjast helstu netöryggisáskorunum nánustu framtíðar, gervigreind og skammtatölvum auk almennra netöryggisverkefna. Einnig er nú (í apríl 2021) í undirbúningi að stofna evrópskt netöryggissetur í Búkarest (í Rúmeníu)[26] og ætlunin er að það verði m.a. miðpunktur samvinnu netöryggissetra í öllum aðildarríkjum sambandsins og stuðli m.a. að samvinnu í rannsóknum og þróun á sviði netöryggis.

3.5 Þróun fjárheimilda

Stofnanir ríkisins og ráðuneytin fjármagna verkefni sem varða net- og upplýsingaöryggi af sinum fjárheimildum. Með gildistöku laga nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða urðu tímamót í fjármögnun þessa málefnis hjá samgöngu- og sveitarstjórnarráðuneytinu. Árið 2020 nam netöryggisframlagið til Póst- og fjarskiptastofnunar 125 m.kr. og í ár nemur það 285 m.kr. Miðað er við að fullri fjármögnun til netöryggismála hjá Póst- og fjarskiptastofnun verði náð 2023 og þá verði framlagið yfir 400 m.kr.

Einnig hafa ýmis önnur framlög úr ríkissjóði þó tengst net- og upplýsingaöryggismálum beint, enda er oft miðað við erlendis að um 15% fjármagns sem varið er til uppbyggingar stafrænnar þjónustu þurfi að fara í verkefni til að tryggja öryggi hennar. Má þar sérstaklega nefna framlag fjármála- og efnahagsráðuneytis til verkefna sem varða netöryggi innan verkefnisins Stafrænt Ísland. Utanríkisráðuneytið hefur fengið framlög vegna stofnunar fjölþáttaógnadeildar og hugsanlegrar aðildar Íslands að netöryggissetrinu í Tallinn og öndvegissetrinu um fjölþáttaógnir í Helsinki.

[25] Sjá: https://ec.europa.eu/digital-single-market/en/europe-investing-digital-digital-europe-programme

[26] Sjá t.d. fréttatilkynningu frá 16. apríl 2021, *The European Cybersecurity Competence Centre and Network moves forward: future Governing Board meets for the first time*, https://digital-strategy.ec.europa.eu/en/news/european-cybersecurity-competence-centre-and-network-moves-forward-future-governing-board-meets og á einnig tilkynningu frá 8. apríl 2021, *Proposal for a European Cybersecurity Competence Network and Centre* https://digital-strategy.ec.europa.eu/en/policies/european-cybersecurity-competence-network-and-centre

3.6 Lykilviðfangsefni til næstu ára

Lykilviðfangsefni næstu ára eru í grófum dráttum þrenns konar.

1. Skipulagsleg. Það þarf að halda áfram að styrkja og formgera samstarf innan stjórnkerfisins og við atvinnulífið, þar sem hlutverkaskipting og ábyrgð er skýr og tilvísanleg.
2. Hæfni og geta. Það þarf að halda áfram að byggja upp getu, efla vitund, menntun, rannsóknir og þróun. Nýta þarf þekkingu og tækifæri innanlands og erlendis m.a. með virku alþjóðlegu samstarfi.
3. Löggæsla og öryggi. Efla þarf lagaumhverfi og löggæslu innanlands og yfir landamæri til samræmis við alþjóðlegar kröfur og viðmið, þannig að fólk njóti verndar réttarríkisins á Netinu ekki síður en í raunheimum. Jafnframt þarf að skilgreina betur hvernig tekið er á netöryggisáskorunum tengdum öryggis- og varnarmálum.

4. Valkostir, framtíðarsýn og áherslur til umræðu

4.1 Valkostir – leiðir

Við val á leiðum þarf að líta til þess hvort þær henta viðfangsefninu, eru líklegar til árangurs, eru pólitískt fýsilegar, tæknilega fýsilegar og leiða til jákvæðra efnahagslegra áhrifa, til lengri og skemmri tíma.

4.2 Drög að framtíðarsýn

Íslendingar búi við öruggt umhverfi á Netinu sem þeir geti treyst og þar séu í heiðri höfð mannréttindi og persónuvernd ásamt frelsi til athafna, efnahagslegs ávinnings og framþróunar.

Örugg upplýsingatækni og örugg þjónusta á Netinu sé ein meginstoð hagsældar á Íslandi, studd af öflugri öryggismenningu, virku alþjóðasamstarfi og traustri löggjöf.

Jafnframt sé samfélagið vel búið til að taka á netglæpum, árásum, njósnum og misnotkun persónu- og viðskiptaupplýsinga, bæði með eigin getu og alþjóðlegri lögreglu-, öryggis- og varnarsamvinnu.

4.3 Áherslur

Það er gagnlegt að nota alþjóðlegan ramma við að móta ramma fyrir áherslur í nýrri netöryggisstefnu, því það gerir samanburð, eftirfylgni og úttektir mun skilvirkari og einfaldari. Hér er því höfð hliðsjón af þeim fimm meginstoðum sem eru í netöryggislíkani Háskólans í Oxford sem áður hefur verið lýst. Áherslur innan hverrar stoðar eru aðlagaðar að íslenskum aðstæðum. Tillögur um áherslur eru eftirfarandi:

1. Samhæft stjórnskipulag netöryggis
    a. Samvinna og samhæfing er varðar netöryggistengda þætti verði efld innan stjórnsýslunnar, byggt á skýrri verkaskiptingu, þar á meðal er varðar vernd barna, byltingarkennda nýtækni, t.d. hlutanetið (IoT), gervigreind og skammtatölvur. Jafnframt verði þróaður áfram vettvangur fyrir upplýsingamiðlun og samstarf við atvinnulífið.
    b. Greining netógna verði styrkt og skipulagi komið á varðandi miðlun ógnamats. Samhæfing við almannavarnaskipulag verði aukin, m.a. með æfingum.
    c. Netöryggi verði gert að viðeigandi hluta almannaöryggis-, utanríkis-, öryggis- og varnarmála.
2. Netöryggismenning og traust
    a. Spornað sé við þeim þáttum sem geta rýrt traust á Netinu og þeirri þjónustu sem þar er veitt.

3. Vitund, þekking og hæfni
    a. Aukin vitundarvakning og fræðsla um netöryggismál.
    b. Aukið framboð og aðgengi að netöryggismenntun fyrir mismunandi hópa, bæði innanlands og í alþjóðlegri samvinnu.
    c. Efldar rannsóknir og nýsköpun, m.a. í alþjóðlegri samvinnu og með alþjóðlegu klasasamstarfi.
4. Varnir gegn afbrotum
    a. Bætt refsilöggjöf m.t.t. afbrota sem tengjast Netinu. Byggt verði m.a. á kröfum í Búdapest-samningnum.
    b. Áhersla verði lögð á vernd barna gegn misnotkun á Netinu, með skýrri löggjöf og ábyrgð á framkvæmd og eftirfylgni. Einnig verði hugað að öðrum hópum sem kunna að þarfnast aukinnar verndar með svipuðum hætti.
    c. Efld samvinna gegn netglæpum milli löggæslu, atvinnulífs og annarra hagsmunaaðila, og virk þátttaka í alþjóðlegu samstarfi á þessu sviði.
5. Uppbygging og nýting netöryggistækni
    a. Áhersla á að hugbúnaður og þjónusta standist vaxandi öryggiskröfur og sé í samræmi við alþjóðlega öryggisstaðla og önnur öryggisviðmið. Gerðar verði miklar öryggiskröfur við innkaup og þróun hugbúnaðar og hvers kyns þjónustu.
    b. Viðeigandi eftirlit verði með áreiðanleika og áfallaþoli grunnkerfa ríkisins og atvinnulífsins.
    c. Tekið verði með viðeigandi hætti á öryggisáskorunum vegna útvistunar og nýtingar aðkeyptrar þjónustu (þ. á m. skýjalausna), t.d. vegna lögsögu, birgjakeðju og eignarhalds.
    d. Netöryggismarkaður verði efldur, bæði innlendur og til útflutnings. Netöryggisþjónusta byggi á skýrum viðmiðum og vottunum eftir því sem við á.
    e. Komið verði á skilvirku skipulagi til að auðvelda tilkynningar um bresti í net- og hugbúnaðarkerfum og stafrænni þjónustu með ábyrgum hætti.

5. Hver er þín skoðun?

Netöryggi er viðfangsefni sem snertir alla í samfélaginu en þó með mismunandi hætti og enginn einn getur haft yfirsýn yfir allar hliðar þess. Markmið þessa skjals er að hvetja til umræðu um stöðu, framtíðarsýn og helstu áherslur í væntanlegri stefnu um netöryggismálin. Margt hefur verið gert nú þegar af hálfu stjórnvalda, atvinnulífs, ýmissa samtaka og einstaklinga en verkefnum á þessu sviði lýkur ekki í fyrirsjáanlegri framtíð og margt er ógert. Einnig er mikilvægt að svara því hvernig samvinnu ólíkra aðila þurfi að vera háttað til þess að mannafli og fé skili sem mestum árangri?

- Stöðumat og lykilviðfangsefni. Leitað er svara og álits frá hagsmunaaðilum um hvort matið sé rétt sett fram, hvort lykilviðfangsefnin séu rétt skilgreind og hvort bæta þurfi við efnisatriðum sem ekki koma fram í þessu skjali.
- Framtíðarsýn. Í umræðu um áherslur eru hagsmunaaðilar og aðrir þátttakendur hvattir til að benda á nýjar áherslur eða aðrar áherslur sem þykja skipta mestu máli til framtíðar.
- Áherslur og forgangsröðun. Í samráðsferlinu er einna mikilvægast að fá ábendingar og tillögur varðandi þær áherslur sem birtast í nýrri stefnu og verða í framhaldinu útfærðar í aðgerðaráætlunum.

Að lokum er vakin athygli á því að í samráðsferlinu býðst dýrmætt tækifæri fyrir hagsmunaaðila til að hafa áhrif á stefnuna og þær aðgerðir sem ráðist verður í á sviði netöryggismála.

6. Viðaukar

6.1 Árangur gildandi fjarskiptaáætlunar

Núgildandi fjarskiptaáætlun nær til áranna 2019 – 2023 og miðað við að það tímabil er nú (apríl 2021) um það bil hálfnað, þá hefur framgangur verkefna verið góður og samkvæmt áætlun þegar á heildina er litið.

Í áætluninni fjallar markmið nr. 2 um örugg fjarskipti, þar á meðal netöryggi.

Eftirfarandi fimm verkefni voru skilgreind og staða þeirra við mitt gildistímabil áætlunarinnar (í apríl 2021) er jafnframt tilgreind:

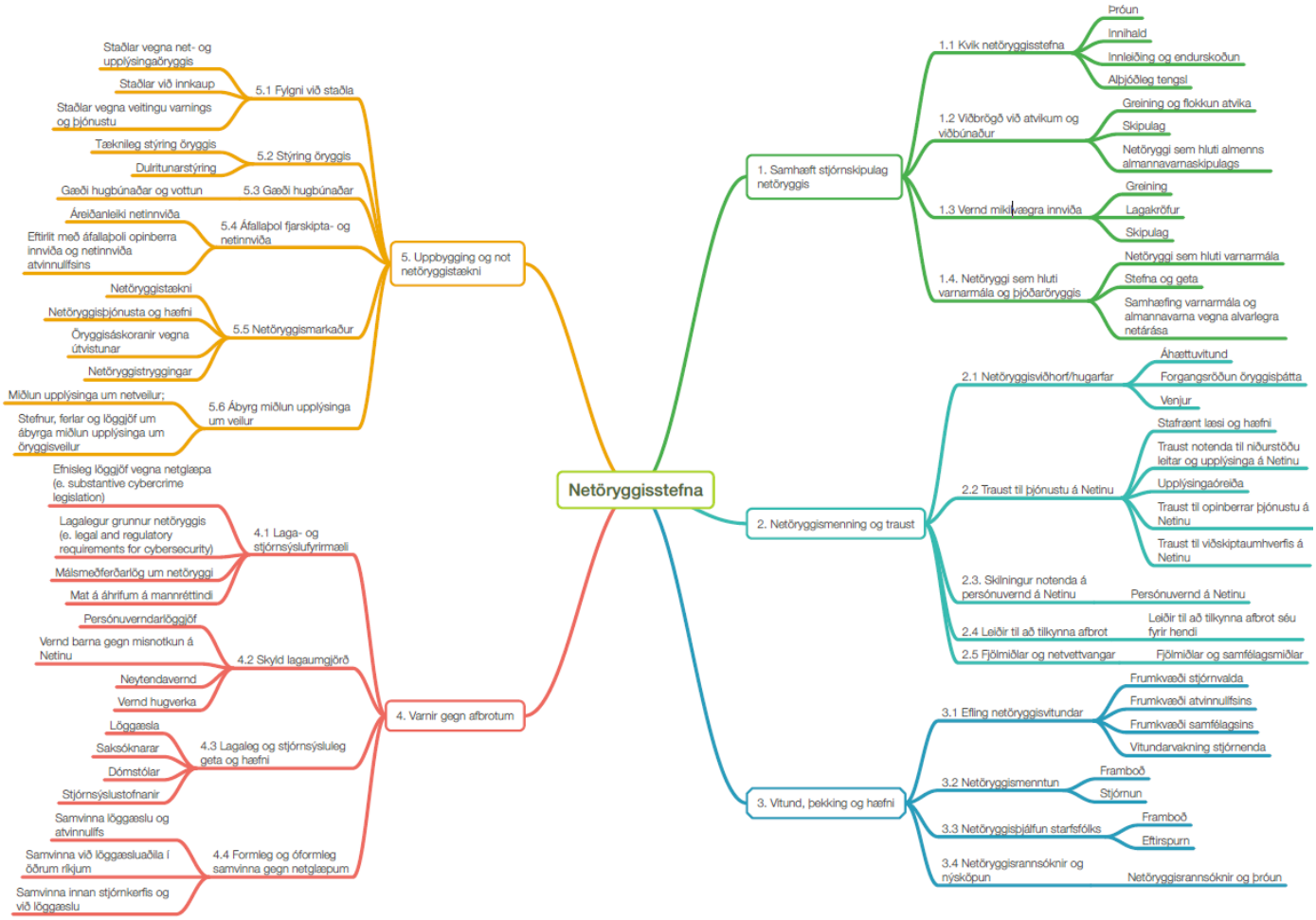
1. *Mótuð verði úttektarstefna og áætlun til að stuðla að viðunandi öryggi fjarskiptaneta.*
   Staða: Er í mótun.
2. *Greining og viðbragðsgeta vegna netógna standist alþjóðlegan samanburð.*
   Staða: Unnið hefur verið að eflingu netöryggissveitar Póst- og fjarskiptastofnunar, hún er orðin aðili að FIRST og hefur sótt um vottun samkvæmt TF-CSIRT-SIM3.
3. *Lög verði sett um íslenska landslénið .is.*
   Staða: Frumvarp hefur verið lagt fram á Alþingi og er þess vænst að það verði samþykkt á vorþingi (2021).
4. *Við innkaup, þróun, rekstur og viðhald á opinberum kerfum og netum verði öryggiskröfur í forgangi. Netöryggisráð verði nýtt sem samvinnuvettvangur stjórnvalda vegna netöryggismála eftir því sem við á og leitað verði samstarfs við fyrirtæki og stofnanir. Fjölbreytt menntun á sviði netöryggis standi til boða, allt frá einföldum námskeiðum til framhaldsnáms á háskólastigi, hérlendis eða í samstarfi við erlenda aðila. Netöryggisvitund verði efld með fræðslu, viðburðum og keppnum hérlendis og með þátttöku í alþjóðlegum viðburðum.*
   Staða: Hlutverk Netöryggisráðs sem samvinnuvettvangs stjórnvalda hefur farið vaxandi og því var gefið skilgreint hlutverk í netöryggislögum sem tóku gildi 1. september 2020. Niðurstöður úttektar Háskólans í Oxford (2017) voru rýndar innan ráðsins og nýttar við skipulagningu aðgerða samkvæmt gildandi fjarskiptaáætlun. Úttekt Alþjóðafjarskiptasambandsins (ITU) á stöðu netöryggis á liðnu ári, var nýtt til eigin mats á stöðu netöryggis og hvar úrbóta væri þörf. Boðið hefur verið upp á ýmis konar fræðslu og fundi fyrir fyrirtæki og stofnanir og meira samstarf er á döfinni á grunni nýrrar netöryggislöggjafar, alþjóðlegra samninga og annarrar samvinnu sem Íslandi stendur til boða. Unnið er að greiningu á hvaða hópar í samfélaginu þurfa helst á fræðslu og vitundarvakningu að halda. Aðgerðir hefjast þegar greiningin liggur fyrir. Samningur hefur verið undirritaður við Norska tækniháskólann (NTNU) og býðst íslenskum stúdentum þar framhaldsnám í netöryggisfræðum, þar á meðal öryggisþáttum sem óvíða annars staðar

standa útlendingum til boða. Erlendir kennarar hafa einnig kennt netöryggisnámskeið við íslenska háskóla og ýmis styttri námskeið og þjálfun hefur verið í boði.

5. *Vernd mikilvægra innviða verði aukin með fræðslu, löggjöf, samvinnu um skipulag netöryggis, úttektum, æfingum og prófunum. Tekið verði mið af alþjóðlegum skuldbindingum Íslands, þar á meðal á sviði varnarmála. Árangur verði metinn reglulega og nauðsynlegum umbótum fylgt eftir.*
   Staða: Vernd mikilvægra innviða var aukin með netöryggislöggjöf sem tók gildi 1. september 2020 og reglugerðum byggðum á henni, enda skilgreinir löggjöfin tiltekna mikilvæga innviði og þá lagalegu umgjörð netöryggis sem þarf um þá. Þetta myndar síðan umgjörð um annað starf til eflingar netöryggis mikilvægra innviða með samvinnu, úttektum, fræðslu og æfingum. Þess skal jafnframt getið að ýmsir mikilvægir innviðir hafa átt gott samstarf á þessu sviði í mörg ár. Utanríkisráðuneytið hefur eflt netöryggisþátt starfsemi sinnar verulega, meðal annars á sviði varnarmála. Náin samvinna hefur verið við erlenda úttektaraðila (Háskólann í Oxford, ITU) og stefnt er að samvinnu við fleiri aðila.
6. *Brugðist verði við ráðleggingum í skýrslu Oxford-háskóla um stöðu netöryggis hérlendis og staðan endurmetin.*
   Staða: Brugðist hefur verið við ráðleggingum í skýrslu Háskólans í Oxford með ýmsum hætti (sjá nánar í kafla 3.3.1).

6.2 Líkön (2017 og 2021) Háskólans í Oxford til að meta stöðu netöryggis

Þær áherslur sem fjallað er um hér byggja á nýju líkani Háskólans í Oxford til að meta stöðu netöryggis í samfélögum. Fulltrúar frá háskólanum komu hingað til lands í júní 2017 og gerðu úttekt á stöðu netöryggis hérlendis, í kjölfarið var ítarlegri skýrslu skilað með stöðulýsingu og fjölda ráðlegginga til úrbóta. Sú úttekt var byggð á líkani skólans frá 2016. Þann 25. mars sl. (2021) kynnti háskólinn uppfært líkan, þar sem tekið er mið af reynslunni af fyrra líkaninu til úttekta og þeirri öru þróun sem hefur verið í netöryggismálum undanfarin ár. Í líkaninu er tekið heildstætt á netöryggisáskorunum samfélagsins, óháð því hvort þær snúi að stjórnvöldum, atvinnulífi eða einstaklingum. Líkanið byggir sem fyrr á 5 meginstoðum eða áhersluflokkum sem fela samtals í sér 23 áherslur. Þeir skiptast síðan í áhersluþætti, 61 alls. Í leiðbeiningum með líkaninu eru áhersluþættir skýrðir og hvernig skuli meta stöðu netöryggis fyrir hvern um sig[27]. Fyrirhugað er setja hina nýju stefnu þannig upp að hún fylgi skipulagi hins nýja Oxford-módels í þeim tilgangi m.a. að auðvelt verði að meta árangurinn með atbeina sérfræðinga þaðan. Það fylgja því einnig margir kostir að velja áherslur sem alþjóðlega eru taldar skipta mestu máli og eru fram settar í kerfi með leiðbeiningum um hvernig standa megi að rýni á stöðunni.



[27] Sjá upplýsingar á vef Háskólans í Oxford https://gcscc.ox.ac.uk/the-cmm#/ , þar má einnig nálgast lýsingu nýja líkansins sem gagnvirkt PDF skjal: https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

6.2.1 Úttekt Háskólans í Oxford 2017

Líkanið sem var notað árið 2017 er svipað því sem er notað nú og byggir á 5 stoðum (hér kallaðar „víddir“) og greinar eru svipaðar þótt einstaka hafi verið fluttar á milli stofna. Í greiningunni voru 24 þættir netöryggis metnir og þeir voru flokkaðir í 5 víddir. Staða hvers þáttar var metin og miðað var við 5 þroskastig. Miðstigið (að viðunandi ástandi sé komið á) er það lágmark sem stefna ber að, allt þar umfram er hins vegar til bóta. Nokkrir þættir hérlendis höfðu náð miðstiginu, aðrir voru lakari:

1. Frumstig (e. *start-up*), sýnt með rauðleitum lit í töflu hér fyrir neðan.
2. Í mótun (e. *formative*), sýnt með daufgulum lit.
3. Komið á (e. *established*), sýnt með skærgrænum.
4. Framsækin (e. *strategic*),
5. Kvik aðlögun (e. *dynamic*).

Í töflunni hér á eftir má sjá þær 5 víddir (D1-D5) sem voru skoðaðar og þá þætti innan hverrar víddar sem voru metnir. Einkunn var stundum á milli þroskastiga og er það á táknað með eftirfarandi litum:

1-2 Á milli „frumstigs“ og „í mótun“, sýnt með sterkum gulum lit.
2-3 Á milli „í mótun“ og „komið á“, sýnt með daufgrænum lit.

Flokkar (víddir) og þættir sem metnir voru í úttektinni

D1 - Netöryggisstefna *(e. Cybersecurity Policy and Strategy)*	
1.1	**Netöryggisstefna** (Þróun, skipulag, innihald)
1.2	**Viðbragðsgeta** (Hvort miðlægur aðili hafi umboð og getu til samhæfingar, hér er þessi aðili netöryggissveit PFS CERT-IS)
1.3	**Vernd mikilvægra innviða** (Hvort það hafi verið greint hverjir þeir eru og mikilvægi upplýsinga þeirra, hvert formlegt samband þeirra við stjórnvöld er, er netöryggi hluti áhættugreiningar?)
1.4	**Neyðarstjórnun** (Viðbragðsáætlun sem prófuð er með æfingum)
1.5	**Netvarnir (hluti varnarmála)** (Eru netvarnir hluti varnaráætlunar landsins? Er til skipulagt samstarf opinberra og einkaaðila verði gerð alvarleg árás á mikilvæga innviði landsins)
1.6	**Varaleiðir fjarskipta** (Er unnt að halda uppi boðskiptum á milli mikilvægra innviða þótt einn strengur í netinu bresti, jafnvel þótt skipulag boðskipta verði með öðrum hætti en venjulega)
D2 - Netöryggismenning og samfélag *(e. Cyber Culture and Society)*	
2.1	**Netöryggisviðhorf/hugarfar** (Mat á netöryggisvitund stjórnvalda, einkaaðila og almennings)
2.2	**Traust til þjónustu á Netinu** (Er unnið að því að viðhalda og efla traust til þjónustu á Netinu? Traust til opinberrar þjónustu á Netinu og þjónustu einkaaðila)
2.3	**Vitund um meðferð persónuupplýsinga á Netinu** (Er skilningur hjá almenningi og notendum á hversu viðkvæmar persónuupplýsingar á Netinu geta verið?)
2.4	**Leiðir til að tilkynna afbrot** (Greiðar leiðir séu fyrir hendi og þekktar til að tilkynna netsvindl og önnur brot)
2.5	**Fjölmiðlar og samfélagsmiðlar** (Umfjöllun fjölmiðla og samfélagsmiðla um netöryggi, hvert hefur hlutverk verið?)

D3 - Netöryggismenntun, þjálfun og hæfni *(e. Cybersecurity Education, Training and Skills)*	
3.1	**Vitundarvakning. (a) Í þjóðfélaginu** (Er samhæft skipulag fyrir vitundarvakningu um netöryggi í þjóðfélaginu?) **(b) Hjá stjórnendum** (Hversu langt hefur vitundarvakning um netöryggi náð meðal stjórnenda, þar á meðal stjórnenda opinberra stofnana og einkafyrirtækja sem og menntastofnana?)
3.2	**Rammi netöryggismenntunar** (Framboð á menntun, t.d. á háskólastigi, sem kallast á við þarfir þjóðfélagsins og viðeigandi framboð á hæfum kennurum. Heildarskipulag slíkrar fræðslu)
3.3	**Rammi námskeiða og þjálfunar** (Framboð á námskeiðum, endurmenntun og nýting innan fyrirtækja og stofnana, t.d. hvort gerð sé krafa um ákveðna menntun?)
D4 - Lagalegt umhverfi *(e. Legal and Regulatory Frameworks)*	
4.1	**Lagarammi** (Fjallað er um ýmsa þætti er snerta netöryggi, net- og fjarskiptamál, persónuvernd, vernd barna gegn misnotkun, neytendavernd, vernd hugverka, hegningarlög)
4.2	**Réttarkerfi**: (Hvort löggæsluaðilar, saksóknarar og dómarar hafi fengið menntun og þjálfun til að eiga við mál þar sem vinna þarf með og meta rafræn sönnunargögn og sönnunargögn á Netinu?)
4.3	**Formleg og óformleg samvinna gegn netglæpum** (Með formlegri samvinnu er m.a. átt við hversu skilvirk samvinna er við rannsókn netglæpa, t.d. á milli innlendra aðila og alþjóðlega, þ.á.m. á grunni réttarbeiðna; með óformlegri samvinnu er átt við ýmsa samvinnu opinberra aðila og einkaaðila til að gera rannsókn netbrota skilvirkari).
D5 - Staðlar, skipulag og tækni *(e. Standards, Organisations, and Technologies)*	
5.1	**Fylgni við staðla** (Eru staðlar nýttir af rekstraraðilum mikilvægra innviða, við innkaup og við þróun hugbúnaðar?)
5.2	**Áfallaþol innviða Netsins**. (Hversu traustir eru innviðir Netsins í landinu? Hversu góð samvinna er á milli opinberra aðila og einkaaðila þar sem það á við? Hversu góða stjórn hafa stjórnvöld á eigin netinnviðum og úthýsingu?)
5.3	**Gæði hugbúnaðar** (Gæði þróunar og stefna varðandi uppfærslur og öryggi út frá áhættumati og mikilvægi þjónustu).
5.4	**Tæknileg öryggisviðmið og stýring** (Nýting staðla og viðmiða, sbr. *SANS top 20* og *GESG 10 steps to cybersecurity*)
5.5	**Dulritun – viðmið og stýring** (T.d. SSL og TLS, rafrænar undirskriftir og önnur notkun, uppfærslur?)
5.6	**Netöryggismarkaður** (Framboð á innlendri jafnt sem erlendri þjónustu, t.d. tækni en einnig tryggingar)
5.7	**Trúnaðarmiðlun upplýsinga um öryggisveilur og viðeigandi viðbrögð** (Rammi um miðlun slíkra upplýsinga?)

6.3 Mat á ásýnd (en ekki stöðu)

NCSI - kvarði eistneskrar netöryggisstofnunar

NCSI – kvarði eistneskrar netöryggisstofnunar, sjá https://ncsi.ega.ee/ncsi-index/. Mat stofnunarinnar er endurskoðað eftir því sem ný gögn berast og einkunnagjöfin getur því verið kvik. Unnt er að fá einkunn hækkaða um leið og umbætur hafa verið staðfestar (t.d. með því að vísa stofnuninni á birtar heimildir á vef).

Ísland var sl. haust í 62. sæti af 160 ríkjum sem matið tekur til og með 47% af mögulegum stigum. Matið á stöðu Íslands byggist á opinberum gögnum sem voru aðgengileg á Netinu og stofnunin safnaði og birti 7. apríl 2018. Matið tekur því ekki, frekar en mat ITU, mið af árangri sem ekki var búið að kynna alþjóðlega á þeim tíma né því sem hefur áunnist síðan. Nýtt mat var gert af hálfu stofnunarinnar þann 25. janúar 2021 og hækkaði þá Ísland upp í að vera með 56% af mögulegum stigum og fór Ísland upp í 46. sæti sem er umtalsverður árangur.

Í síðari könnuninni eru það einkum eftirfarandi þættir sem voru ófullnægjandi og drógu Ísland niður (ekkert land fær þó fullt hús stiga):

- Áætlun um innleiðingu stefnu skorti.
- Greining netógna og árleg birting á netógnamati skorti.
- Alvarlegur skortur á netöryggismenntun á öllum stigum.
- Fagsamtök netöryggissérfræðinga skorti.
- Ísland hýsir enga alþjóðastofnun á sviði netöryggis.
- Ísland veitir enga þróunaraðstoð á sviði netöryggis.
- Netöryggisviðmið skortir fyrir hið opinbera (e. public sector).
- Reglubundið eftirlit skortir með netöryggi mikilvægra innviða (lagast með framkvæmd nýju netöryggislöggjafarinnar).
- Kröfulýsingu til dulritunarkerfa skortir.
- Tímastimplun (e. Timestamping) ófullnægjandi.
- Rafræn skráð flutningsþjónusta ófullnægjandi (e. electronic registered delivery service).
- Viðbragðsáætlanir skortir.

Rétt er að ítreka að þetta mat endurspeglar mat á ásýnd Íslands út frá auðfengnum gögnum á Netinu án þess að leitað hafi verið gagna með beiðni eða í samstarfi við innlenda aðila. Staða einstakra þátta er því metin lakari en hún er í reynd ef stöðulýsing er ekki aðgengileg. Hér er því ekki um stöðumat að ræða. Ásýnd getur haft áhrif á viðhorf, traust og viðskipti og skiptir því einnig máli þótt hún þurfi ekki að endurspegla raunverulega stöðu. Eitt af forgangsverkefnum ársins 2021, nú þegar vinna vegna úttektar ITU er að baki, er að sjá til þess að þessi mælikvarði og aðrir svipaðir geti nýtt sér viðeigandi gögn þannig að ásýnd endurspegli stöðu í reynd.

6.4 Kröfur til netöryggisstefnu; leiðbeiningar og stefnur annarra ríkja

Þegar netöryggisstefna er mótuð verður að huga að ýmsum kröfum og samræmi við netöryggisstefnur annarra landa, þetta er ekki síst mikilvægt þar sem Netið er alþjóðlegt. Netöryggisstefna lands er ásýnd þess gagnvart umheiminum, til dæmis varðandi hversu traust það virðist vera vegna viðskipta eða samvinnu þegar um netháð málefni er að ræða. Netöryggisstefnur ríkja eru því iðulega rýndar og metnar af öðrum ríkjum, samtökum og jafnvel fyrirtækjum.

Við mótun netöryggisstefnu þarf því bæði að huga að ýmsum formkröfum sem stefnu þarf að uppfylla og jafnframt væntingum um ákveðna samhæfingu sem grannríki hafa.

Hér á eftir er fyrst lýst kröfum í NIS1-tilskipuninni sem og síðan hvernig þær kröfur hafa verið útvíkkaðar í tillögu að endurnýjaðri NIS-tilskipun (NIS2). Hafa verður hugfast að netöryggisstefna þarf að spanna mun fleiri þætti en eru bein viðfangsefni NIS1-tilskipunarinnar og fyrirliggjandi tillögu að NIS2, en brýnt er að stefna uppfylli m.a. kröfur þeirra[28]. Í næsta undirkafla er fjallað um almennar leiðbeiningar Netöryggisstofnunar Evrópu (ENISA) um gerð stefna og er þá tekið mið af fleiri þáttum. Að lokum eru gefin dæmi um stefnur nokkurra grannríkja okkar.

6.4.1 NIS1-tilskipunin og NIS2-tillagan

Netöryggistilskipun ESB 2016/1148 (NIS1-tilskipunin) mælir fyrir um að öll ríki á Evrópska efnahagssvæðinu setji sér netöryggisstefnu (sjá ennfremur 1. mgr. 4. gr. laga nr. 78/2019).[29] Í 7. gr. NIS1 eru gerðar eftirfarandi kröfur til útfærslu netöryggisstefnu.[30]

[28] Nú er unnið að undirbúningi upptöku NIS 1 í EES-samninginn. Hlutverk Eftirlitsstofnunar EFTA (ESA) er að tryggja að EFTA ríkin innan EES (Ísland, Noregur og Liechtenstein) innleiði og fylgi hinum sameiginlegu reglum. Ef EFTA ríkin innleiða ekki nýjar EES reglur í landsrétt innan tímamarka eða með tilhlýðilegum hætti grípur ESA til aðgerða. Sama á við ef EES löggjöf er ekki rétt framkvæmd í EFTA ríkjunum.

[29] Með netöryggisstefnu er í NIS1-tilskipuninni átt við ramma sem kemur á fót stefnumótandi markmiðum og forgangsröðun varðandi öryggi net- og upplýsingakerfa á landsvísu (sjá 3. tölul. 4. gr.). Lög nr. 78/2019 byggja á NIS1-tilskipuninni og er 1. mgr. 4. gr. þeirra svohljóðandi: „Ráðherra skal marka stefnu um net- og upplýsingaöryggi, sem endurskoðuð skal reglubundið. Í stefnu skal m.a. greina frá markmiðum og ráðstöfunum stjórnvalda í því skyni að stuðla að öryggi og viðnámsþrótti net- og upplýsingakerfa mikilvægra innviða“.

[30] Netöryggisstofnun Evrópu (ENISA) hefur útfært nánari leiðbeiningar um slíka stefnumótun.

NIS1-tilskipunin

NIS1-tilskipunin hefur verið þýdd á íslensku[31] en tilvitnaður hluti hennar er hafður hér óþýddur á ensku til að auðvelda samanburð við samsvarandi kröfur í NIS2-tillögunni hér að aftan:

> *Article 7* ***National strategy on the security of network and information SYSTEMS***
>
> *1. Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at least the sectors referred to in Annex II and the services referred to in Annex III. The national strategy on the security of network and information systems shall address, in particular, the following issues:*
>
> *(a) the objectives and priorities of the national strategy on the security of network and information systems;*
>
> *(b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;*
>
> *(c) the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;*
>
> *(d) an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems;*
>
> *(e) an indication of the research and development plans relating to the national strategy on the security of network and information systems;*
>
> *(f) a risk assessment plan to identify risks;*
>
> *(g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.*
>
> *2. Member States may request the assistance of ENISA in developing national strategies on the security of network and information systems.*
>
> *3. Member States shall communicate their national strategies on the security of network and information systems to the Commission within three months from their adoption. In so doing, Member States may exclude elements of the strategy which relate to national security.*

[31] https://www.stjornarradid.is/library/02-Rit--skyrslur-og-skrar/NIS_drog_thyding_SRN.pdf

NIS2-tillagan

Tillaga að endurnýjaðri netöryggistilskipun ESB (NIS2-tillagan), sem leysa mun af hólmi þá gildandi (NIS1) var birt í desember 2020.[32] Með henni er lagt til að gerðar verði enn ríkari kröfur til útfærslu landsbundinnar netöryggisstefnu. Þar sem þessar kröfur verða væntanlega bindandi fyrir Ísland eru þær birtar hér óþýddar í heild sinni, en ákvæðið getur tekið breytingum enda hefur tillagan ekki enn verið samþykkt sem ESB-gerð. Hér er einungis birt grein 5 sem snýr beint að stefnunni, aðrar greinar sem fjalla um ýmsar hliðar netöryggismála snerta hana einnig óbeint.

Article 5 ***National cybersecurity strategy***

1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:

- *a) a definition of objectives and priorities of the Member States' strategy on cybersecurity;*
- *b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 and the roles and responsibilities of public bodies and entities as well as other relevant actors;*
- *c) an assessment to identify relevant assets and cybersecurity risks in that Member State;*
- *d) an identification of the measures ensuring preparedness, response and recovery to incidents, including cooperation between the public and private sectors;*
- *e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;*
- *f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council38 [Resilience of Critical Entities Directive] for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks.*

2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies:

- *a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services;*
- *b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement;*
- *c) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6;*
- *d) a policy related to sustaining the general availability and integrity of the public core of the open internet;*

[32] Sjá: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166

e) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives;
f) a policy on supporting academic and research institutions to develop cybersecurity tools and secure network infrastructure;
g) a policy, relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between companies in compliance with Union law;
h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats.

3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. Member States may exclude specific information from the notification where and to the extent that it is strictly necessary to preserve national security.

4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon request, in the development of a national strategy and of key performance indicators for the assessment of the strategy.

6.4.2 Leiðbeiningar varðandi gerð netöryggisstefnu

Netöryggisstofnun Evrópu (ENISA) hefur tekið saman ýmsar leiðbeiningar og stoðefni fyrir ríki til notkunar við eigin stefnumótun á sviði netöryggismála.. Á vefsíðu helgaðri mótun á netöryggisstefnum[33] má finna ýmsar leiðbeiningar. Þeirra á meðal er ritið *National Cyber Security Strategies*[34] sem stendur enn fyrir sínu þótt það sé komið til ára sinna, því þótt tæknin og viðfangsefnin taki örum breytingum, þá breytast ýmsar grunnforsendur hægar.

6.4.3 Dæmi um stefnur nokkurra grannríkja

Allar neðangreindar stefnur eru enskar útgáfur og er jafnframt ætlað að kynna framsækin viðhorf viðkomandi ríkis. Þótt megináherslur geti virst mismunandi, þá er innihaldið þegar kemur að einstökum aðgerðum að jafnaði svipað.

- Noregur: National Cyber Security Strategy for Norway (2019)[35] List of measures – National Cyber Security Strategy for Norway (aðgerðaáætlun, 2019)[36]
- Finnland: Finland´s Cyber Security Strategy 2019[37]
- Danmörk: Danish Cyber and Information Security Strategy 2018-2021[38]
- Svíþjóð: A national cyber security strategy (Skr. 2016/213)[39] & Comprehensive cyber security action plan 2019–2022 (2019)[40]
- Eistland: Cybersecurity Strategy 2019–2022[41]
- Holland: National Cybersecurity Agenda (2018)[42]
- Írland: The National Cyber Security Strategy 2019 – 2024[43]

[33] https://www.enisa.europa.eu/topics/national-cyber-security-strategies

[34] https://www.enisa.europa.eu/publications/cyber-security-strategies-paper

[35] https://www.regjeringen.no/en/dokumenter/national-cyber-security-strategy-for-norway/id2627177/

[36] https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/list-of-measures--national-cyber-security-strategy-for-norway.pdf

[37] https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/

[38] https://en.digst.dk/policy-and-strategy/danish-cyber-and-information-security-strategy/

[39] https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213

[40] https://rib.msb.se/filer/pdf/28898.pdf

[41] https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

[42] https://english.ncsc.nl/topics/national-cybersecurity-agenda/documents/publications/2019/juni/01/national-cyber-security-agenda

[43] https://www.skillnetireland.ie/publication/national-cyber-security-strategy-2019-2024/