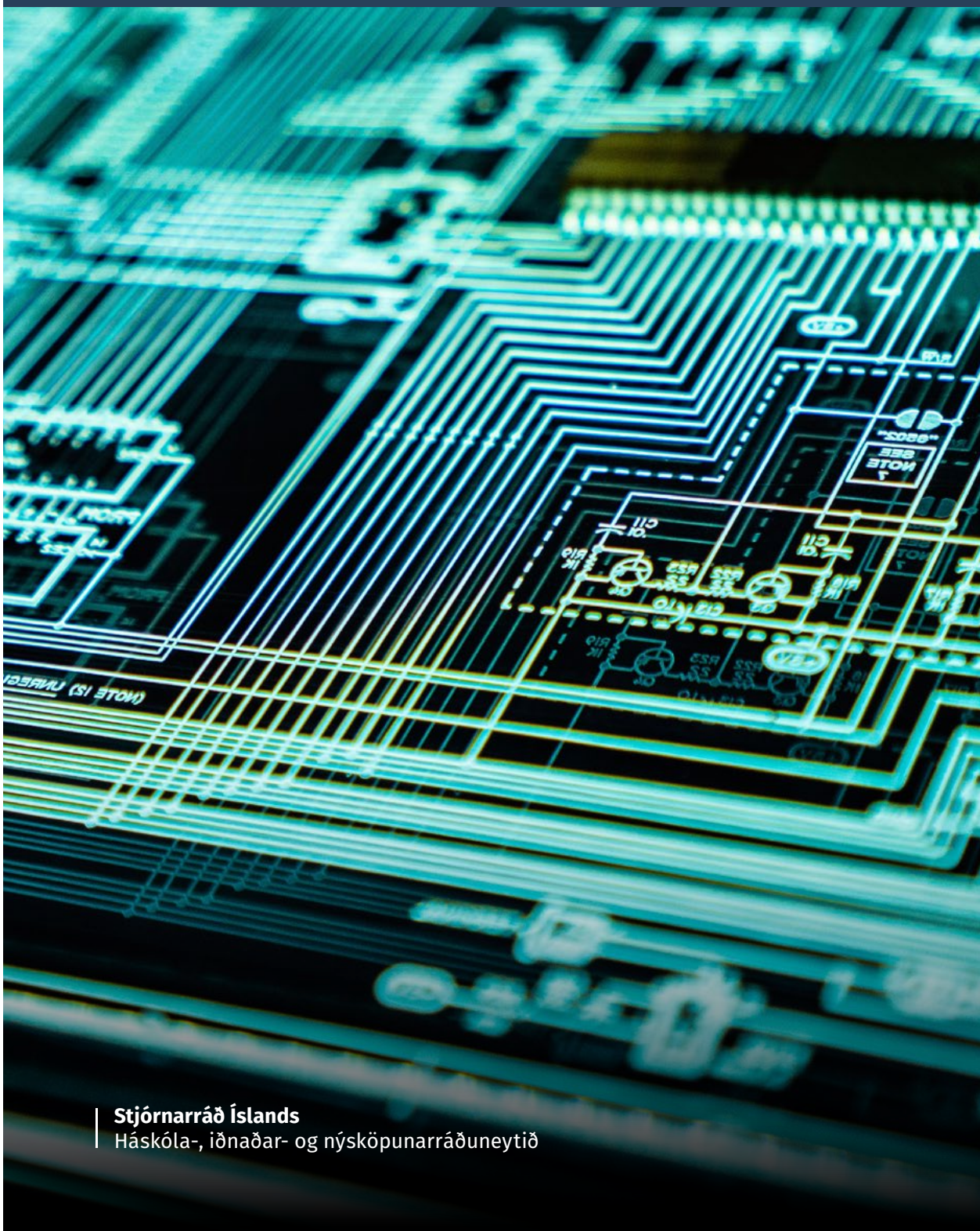
Febrúar 2022

Netöryggisstefna Íslands 2022–2037



Stjórnarráð Íslands
Háskóla-, iðnaðar- og nýsköpunarráðuneytið

Háskóla-, iðnaðar- og nýsköpunarráðuneytið
Lindargötu 1 – 101 Reykjavík
545 9600 | hvin@hvin.is

Febrúar 2022

stjornarradid.is

Efnisyfirlit

1. Inngangur

Í þessari stefnu um netöryggi Íslands er að finna framtíðarsýn og markmið stjórnvalda um stöðu netöryggis í íslensku samfélagi ásamt mælikvörðum og áherslum þar að lútandi til að ná tilsettum markmiðum.

Stefnan leysir af hólmi eldri stefnu frá árinu 2015. Við gerð stefnunnar fór fram opið samráð um drög hennar (hvítbók) sem og mat á stöðu netöryggismála (grænbók). Stefna þessi er samþykkt af ráðherra samkvæmt lögum um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019. Þá er stefnan hluti af fjarskiptaáætlun stjórnvalda.[1]

Með áherslurnar að leiðarljósi er stefnan grunnur að aðgerðum á sviði netöryggismála sem settar verða fram í sérstakri aðgerðaáætlun. Mótun aðgerða á grunni stefnunnar og framkvæmd þeirra er í höndum hinna ýmsu ráðuneyta og stofnana eftir því sem við á. Í stefnunni eru settir fram mælikvarðar til að meta árangur aðgerða.

Stefnuna skal endurskoða eigi sjaldnar en á þriggja ára fresti og skal þá m.a. taka mið af árangri miðað við skilgreinda mælikvarða hennar.

[1] Netöryggisstefnan var samþykkt af samgöngu- og sveitarstjórnarráðherra í nóvember 2021. Við tilfærslu málaflokks netöryggis til ráðuneytis háskóla, iðnaðar og nýsköpunar í febrúar 2022, hefur stefnan verið gefin út að nýju. Stefnan tekur nú til áranna 2022-2037 og er samþykkt af ráðherra.

1.1 Stafrænn heimur

Upplýsingatækni og hvers konar stafrænar lausnir koma við sögu í nánast öllum kimum samfélagsins. Víða í athöfnum daglegs lífs gegnir upplýsingatæknin orðið lykilhlutverki og margs konar þjónusta er háð notkun hennar. En á sama tíma og samfélagið treystir stöðugt meira á stafrænar lausnir er enn að finna veikleika í undirliggjandi tækni. Sú staða er ekki síst komin til vegna Netsins.

Þessari þróun fylgja jafnan aukin lífsgæði og velmegun en henni fylgja einnig neikvæð áhrif. Ný tækifæri skapast og það á einnig við um ógnirnar. Jafnvel má segja að ómögulegt sé að ná markmiðum um efnahagslegan og samfélagslegan ávinning af notkun stafrænna lausna nema áherslur þeirra feli einnig í sér aðgerðir til að bregðast við netöryggisógnum.

Netið býður upp á mikla möguleika fyrir íslenskt samfélag. Áhersla á netöryggi er grunnforsenda þess að nýta megi þessa möguleika. Sú áhersla krefst virkrar þátttöku og samstarfs stjórnvalda, atvinnulífs og almennings. Netöryggismál ná til alls samfélagsins og því er mikilvægt að nýta krafta hinna ýmsu hópa þess. Í umfjöllun um netöryggi þarf að leggja rækt við þverfagleg gildi og huga þarf að fjölbreytileika án aðgreiningar í hópi þeirra sem að henni koma, t.d. með tilliti til menntunar, kyns, aldurs og menningarlegs bakgrunns.

Netöryggi hefur þróast frá því að vera tæknilegt yfir í þverfaglegt viðfangsefni sem krefst víðtækrar samvinnu. Alþjóðleg samvinna er forsenda framfara á þessu sviði og mörg sóknarfæri fólgin í því að nýta erlenda sérfræðinga hérlendis til að tengjast alþjóðlegum straumum. Áhersla á netöryggi skilar sér ekki einungis í minni líkum á skaða, í þeim felast einnig tækifæri til sóknar, svo sem á sviði netöryggistækni og netöryggisþjónustu, sem er ört vaxandi atvinnugrein erlendis.

Árangursrík framkvæmd netöryggisaðgerða stjórnvalda mun ekki aðeins leiða til bættrar stöðu netöryggis á landinu heldur einnig aukinnar netöryggisvitundar almennings sem og tækifæra til þátttöku í þjónustuframboði á þessu sviði.

1.2 Lykilviðfangsefni

1. HÆFNI OG GETA

Auka þarf hæfni og getu með því að efla vitund, menntun, rannsóknir og þróun. Efla þarf getu stjórnvalda og atvinnulífs til að sporna við netárásum og lágmarka skaða þeirra. Nýta þarf þekkingu og tækifæri, innanlands og alþjóðlega.

2. LÖGGÆSLA, ÖRYGGI OG VARNIR

Efla þarf lagaumhverfi og löggæslu innanlands og yfir landamæri til samræmis við alþjóðlegar kröfur og viðmið. Huga þarf sérstaklega að vernd barna á Netinu. Skilgreina þarf betur hvernig tekið er á net- og upplýsingaöryggisáskorunum tengdum öryggis- og varnarmálum.

3. SKIPULAG OG SAMSTARF

Styrkja og formgera þarf samstarf innan stjórnkerfisins og við atvinnulífið, þar sem hlutverkaskipting og ábyrgð er skýr. Tryggja þarf virka samhæfingu opinberra aðgerðaraðila vegna netöryggis.

2. Netöryggi

Netöryggi felst í öryggi stafrænnar þjónustu og lausna og öryggi í notkun þeirra, þar sem Netið kemur við sögu. Með lausnum og aðferðum á sviði netöryggis er spornað við *netöryggisógnum*[2], sem geta orðið að netöryggisatvikum ef þær raungerast.

Netglæpir eru afbrot sem framin eru með því að nýta Netið eða beinast gegn því og í netárás er Netið notað til að skaða virkni tölvukerfa eða fá óleyfilegan aðgang að þeim. Hafa þarf í huga að hefðbundin notkun stafrænna lausna og Netsins til að fremja glæp, svo sem selja ólöglega vöru eða þjónustu, eða beita misnotkun eða ofbeldi telst einnig vera netglæpur.

[2] Annars konar ógnir sem varða upplýsingakerfi geta m.a. falist í félagslegum og efnahagslegum þáttum svo sem mismunun eða glataðri afkomu vegna sjálfvirknivæðingar starfa, sem er ein birtingarmynd fjórðu iðnbyltingarinnar.

Netöryggisatvik geta einnig stafað af völdum manna eða kerfa án þess að um netglæp sé að ræða, svo sem vegna bilana, viðhalds eða mistaka, af gáleysi eða af völdum sið-leysis. Þá geta netöryggisatvik stafað af völdum náttúruafla. Netöryggisatvik geta leitt til óbætanlegs tjóns sem og valdið verulegum skaða á trausti til stafrænna lausna og Netsins, og með því haft hamlandi áhrif á jákvæða þróun og tilsvarandi framfarir.

Til að gæta öryggis við notkun stafrænna lausna er leitast eftir því að um gögn þeirra ríki leynd eftir því sem við á hverju sinni, að réttleiki gagna og kerfa sé tryggður og að gögn og kerfi séu tiltæk, á þann hátt sem til er ætlast af eigendum eða ábyrgðar-aðilum. Stöðug og aukin netöryggisógn beinist að þessum grundvallarþáttum netöryggis stafrænna lausna. Með viðeigandi vörnum, þekkingu og hegðun má auka öryggi við notkun þeirra.

Þegar lagt er mat á öryggi stafrænna lausna er annars vegar horft til þess hvort áhættan sem felst í notkun þeirra sé ásættanleg og hins vegar horft til áfallaþols, svo sem hvort viðbragðsgeta og viðbragðstími til að sporna við slæmum afleiðingum netöryggisatviks sé fullnægjandi. Með því er einnig vísað til þess hversu fljótt sé unnt að veita þjónustu að nýju, jafnvel þótt það sé með breyttum hætti.

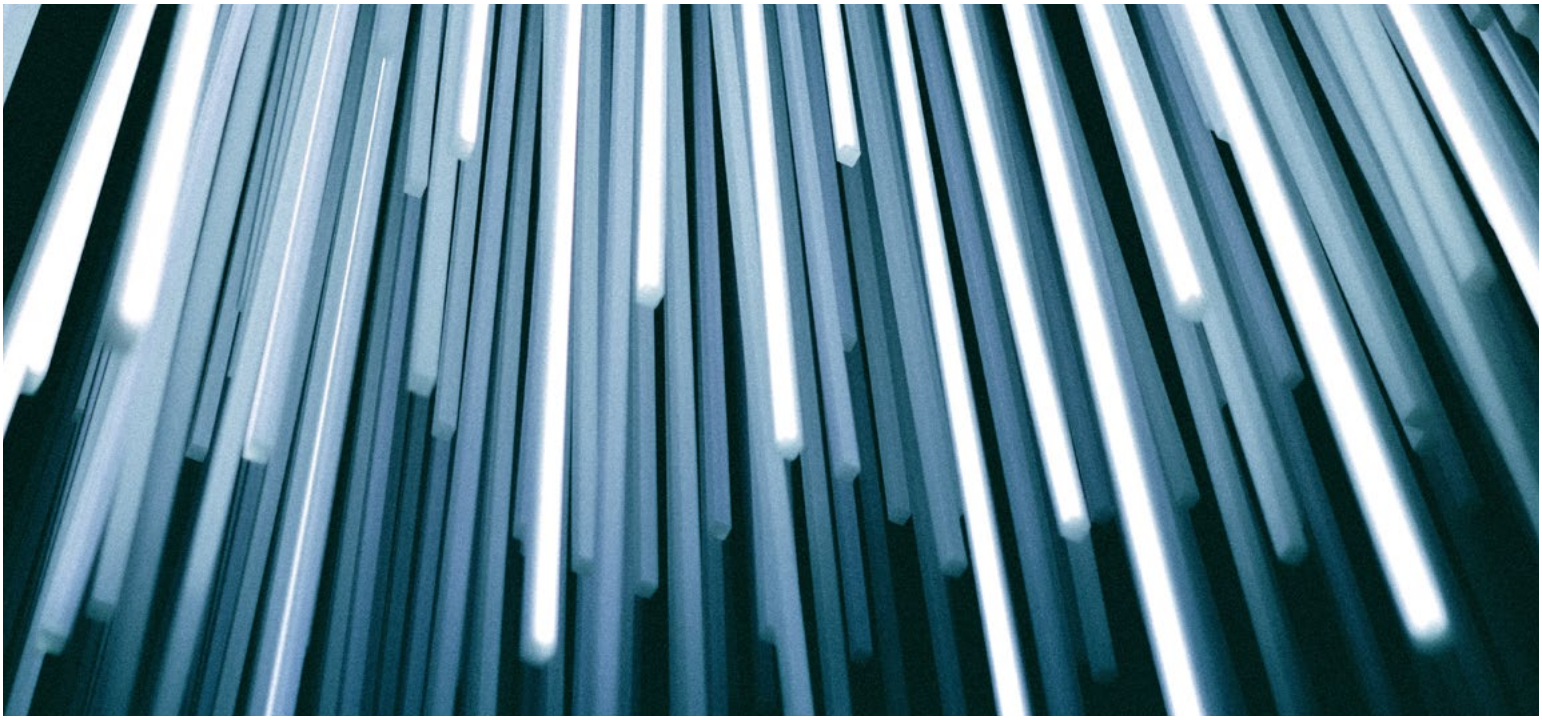
Netglæpir eru orðnir hluti af skipulagðri glæpastarfsemi. Þar er í æ ríkara mæli reynt að finna og notfæra sér lagalega og lögsögulega óvissu eða skapa siðferðisleg álita-mál. Þá mun áframhaldandi tækniþróun skapa áður óþekktar ógnir sem gera þær lausnir og aðferðir sem nú eru notaðar úreltar og ónothæfar. Þannig hefur Netöryggis-stofnun Evrópu ENISA skilgreint gervigreind og notkun skammtatölva sem helstu netöryggisáskoranir komandi ára. Aukning á notkun stafrænna lausna til misnotkunar og ofbeldis kallar á að hugað sé sérstaklega að vernd viðkvæmra hópa, sérstaklega barna.

3. Netöryggisstefna Íslands

3.1 Framtíðarsýn

Framtíðarsýn í netöryggi Íslands er eftirfarandi:

Íslendingar búa við öryggi á Netinu sem byggir á öflugri öryggismenningu, traustum netvörnum og löggæslu, virku samstarfi, innanlands og alþjóðlega, og traustri löggjöf sem stuðlar að nýsköpun og framþróun í þjónustu á Netinu.

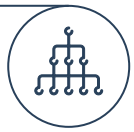


Þetta felur m.a. í sér að Íslendingar búi við sem öruggast umhverfi á Netinu sem þeir geti treyst og að þar séu í heiðri höfð mannréttindi og persónuvernd ásamt frelsi til athafna, efnahagslegs ávinnings og framþróunar. Þá séu örugg upplýsingatækni og örugg þjónusta á Netinu mikilvægar meginstoðir hagsældar á Íslandi, byggðar á traustri samvinnu og studdar af öflugri öryggismenningu, virku alþjóðasamstarfi og traustri löggjöf. Enn fremur að samfélagið sé vel búið til að taka á netglæpum, netárásum, njósnum og misnotkun persónu- og viðskiptaupplýsinga, bæði með eigin getu og alþjóðlegri samvinnu netöryggissveita, lögreglu og öryggis- og varnarsamvinnu.

3.2 Markmið

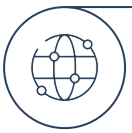
Markmið um netöryggi eru tvö:

1. AFBURÐA HÆFNI OG NÝTING Á NETÖRYGGISTÆKNI



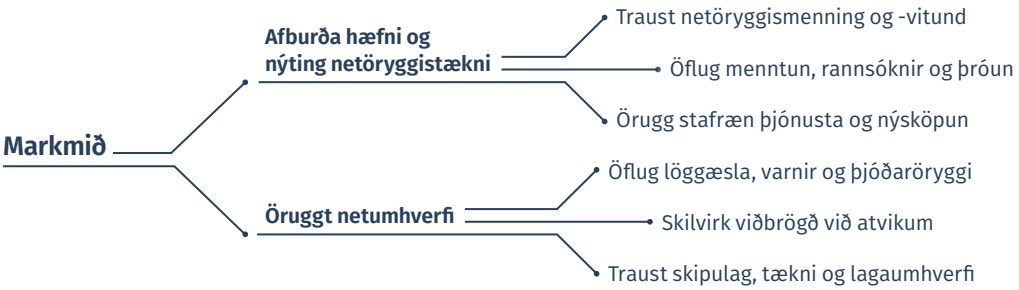
Þekking og hæfni verður efld með aukinni áherslu á almannafræðslu, menntun, rannsóknir, þróun og alþjóðlega samvinnu. Geta til að forðast, bregðast við og lágmarka skaða netárása verður aukin með nýtingu tækni, alþjóðlegra úrræða og bestu fáanlegu lausna.

2. ÖRUGGT NETUMHVERFI



Með öflugri löggæslu á netinu ásamt lagaumhverfi til samræmis við alþjóðleg viðmið verður skapað traust til viðbragða við óviðunandi nethegðun. Lögð verður áhersla á vernd barna á Netinu. Öryggisskipulag, áhættugreining og áfallaþol mikilvægra innviða verður eflt og viðbragðsgeta aukin gegn ógnum á sviði öryggis- og varnarmála.

Hvoru markmiði má skipta í tvo þætti sem sjá má á eftirfarandi mynd:



Árangur aðgerða verður mældur og metinn með tilliti til þeirra mælikvarða sem tilgreindir eru með hvoru markmiði.

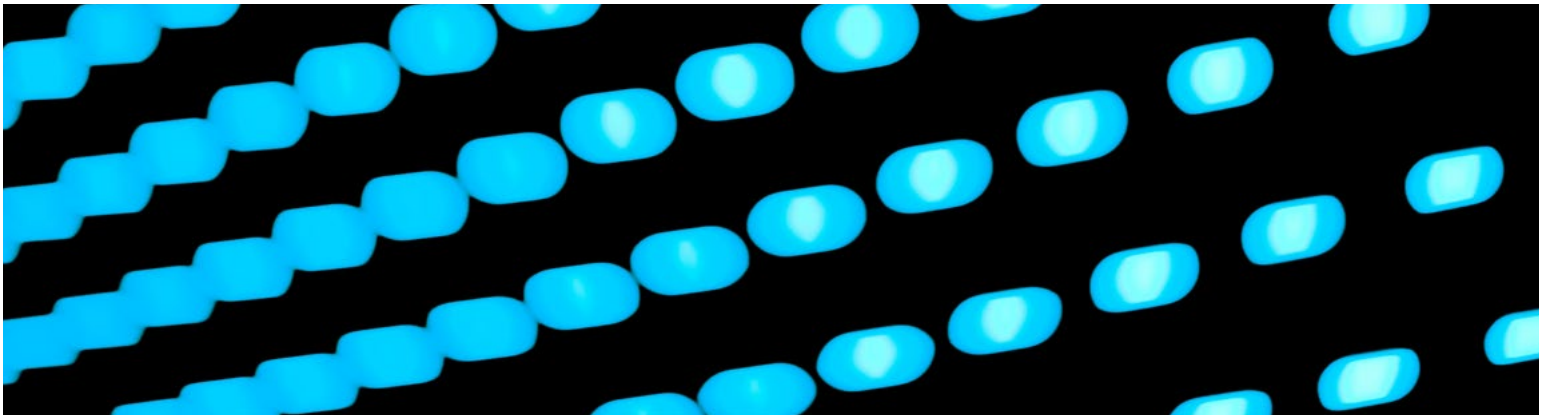
3.2.1 Afburða hæfni og nýting netöryggistækni

Traust netöryggismenning byggir á því að til staðar sé vitund um áhættu sem fylgir notkun Netsins, áhættumat og forgangsröðun aðgerða út frá því. Til að byggja megi upp viðeigandi hæfni og nýtingu netöryggistækni er lykilatriði að aðgengi sé að öflugri og fjölbreyttri menntun sem miðuð sé við mismunandi þarfir og að virk þátttaka sé í rannsóknum. Á því byggir nýsköpun og örugg hagnýting til framtíðar.

Mælikvarðar

	Staða 2021	Staða 2026
Staða skv. matskerfi ITU[3] hvað varðar hæfni og vitund	60%	>90%
Stöðumat skv. Oxford-líkani[4] hvað varðar grunnþætti markmiðs	9 af 32 þáttum uppfylla grunnviðmið	32 af 32 þáttum uppfylli grunnviðmið

[3] Sjá: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[4] Samkvæmt líkani Háskólans í Oxford (https://gcscc.ox.ac.uk/the-cmm#/) er staða þátta netöryggis flokkuð í fimm mismunandi stig. Hér er miðað við að allir þættir uppfylli grunnviðmið sem felst í því að netöryggi á viðkomandi sviði er komið á og það orðið virkt.



Helstu áherslur

a Spornað sé gegn þeim þáttum sem geta rýrt traust á Netinu og þeirri þjónustu sem þar er veitt.

b Vitundarvakning og fræðsla um netöryggismál verði aukin með áherslu á fræðslu við hæfi fyrir þá hópa sem viðkvæmastir eru. Fjölmiðlar og samfélagsmiðlar séu nýttir með markvissum hætti.

c Skilningur á mikilvægi persónuverndar í stafrænni þjónustu verði efldur.

d Greiðar leiðir séu fyrir hendi til að tilkynna netöryggisglæpi.

e Auka framboð og aðgengi að viðeigandi netöryggismenntun og þjálfun fyrir mismunandi hópa, bæði innanlands og í alþjóðlegri samvinnu.

f Hugað sé sérstaklega að þörfum lítilla og meðalstórra fyrirtækja í dreifbýli jafnt sem þéttbýli, m.a. með hliðsjón af leiðbeiningum ENISA þar að lútandi.

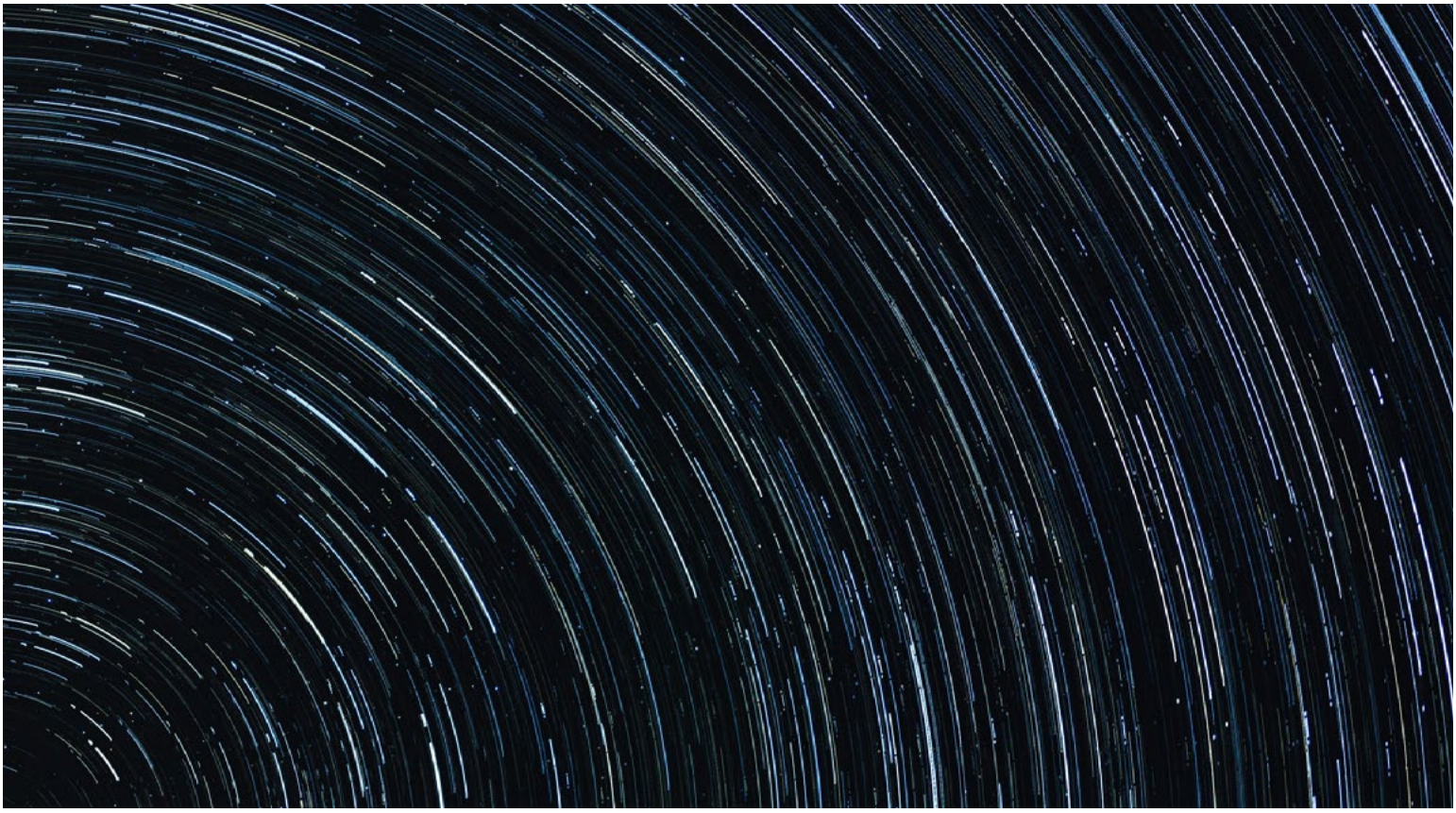
g Rannsóknir og nýsköpun byggðar á skýrri stefnu verði efldar, m.a. í alþjóðlegri samvinnu og með alþjóðlegu klasasamstarfi.

h Hugbúnaður og þjónusta standist vaxandi öryggiskröfur og sé í samræmi við alþjóðlega öryggisstaðla og -viðmið. Gerðar verði ríkar öryggiskröfur við innkaup og þróun hugbúnaðar og hvers kyns þjónustu á sviði stafrænna lausna. Útbúnar verði leiðbeiningar þessu til stuðnings. Skýr viðmið verði sett fyrir hið opinbera um öryggiskröfur varðandi innkaup, þróun og þjónustu stafrænna lausna.

i Til staðar séu áreiðanlegar og öruggar lausnir til rafrænnar auðkenningar- og traustþjónustu.

j Netöryggismarkaður þjónustu og tækjabúnaðar verði efldur, bæði innlendur og til útflutnings. Netöryggisþjónusta og búnaður byggi á skýrum viðmiðum og vottunum eftir því sem við á, þar á meðal er varðar stýringu öryggis.

k Gætt verði sérstaklega að ógnum og öryggisáskorunum sem geta falist í útvistun og nýtingu aðkeyptrar þjónustu (þar á meðal skýjavinnsluþjónustu), t.d. vegna lögsögu, birgjakeðju og eignarhalds.



3.2.2 Öruggt netumhverfi

Íslendingar treysta á að til staðar sé öflugt netöryggisskipulag sem getur með skilvirkum hætti brugðist við netöryggisatvikum, sem ógnað geta þjóðaröryggi, mikilvægum innviðum og réttindum einstaklinga. Sérstök áhersla sé á vernd þeirra sem minna mega sín, sérstaklega barna.

Ör þróun netöryggismála og síbreytilegar aðstæður krefjast lagaumhverfis sem stuðlar að vernd einstaklinga, atvinnulífs og samfélagsins í heild og að því sé fylgt eftir með löggæslu þar á meðal með viðeigandi samfélagslegri samvinnu.

Mælikvarðar

	Staða 2021	Staða 2026
Staða skv. matskerfi ITU[5] hvað varðar lagalegt umhverfi, tækni og skipulag	86%	>90%
Stöðumat skv. Oxford-líkani[6] hvað varðar grunnþætti markmiðs	14 af 30 þáttum uppfylla grunnviðmið	30 af 30 þáttum uppfylli grunnviðmið

[5] Sjá https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[6] Samkvæmt líkani Háskólans í Oxford (https://gcscc.ox.ac.uk/the-cmm#/) er staða þátta netöryggis flokkuð í fimm mismunandi stig. Hér er miðað við að allir þættir uppfylli grunnviðmið sem felst í því að netöryggi á viðkomandi sviði er komið á og það orðið virkt.

Helstu áherslur

a Lagalegt umhverfi uppfylli alþjóðleg viðmið og væntingar. Þannig verði unnt að taka á misnotkun og glæpsamlegri notkun Netsins með ekki síðri hætti en í nágrannalöndum okkar, m.a. með mati á hversu vel skilyrði Búdapest-samningsins séu virt, og að varnir séu gegn auðkenna- og gagnaþjófnaði.

b Stuðlað sé að öflugu öryggisskipulagi byggðu á virkri áhættugreiningu viðeigandi innviða og eflingu áfallaþols.

c Öryggisskipulag mikilvægra innviða endurspegli bestu framkvæmd með tilliti til leiðbeininga Netöryggisstofnunar Evrópu, ENISA. Einnig sé tekið mið af ögnum innan frá.

d Vernd barna gegn misnotkun á Netinu verði tryggð með stefnu, skýrri löggjöf og ábyrgð á framkvæmd og eftirfylgni. Einnig verði hugað að öðrum hópum sem kunna að þarfnast aukinnar verndar með svipuðum hætti.

e Samvinna löggæslu, atvinnulífs og annarra hagsmunaaðila gegn netglæpum verði efld sem og virk þátttaka í alþjóðlegu samstarfi á þessu sviði.

f Eftirlit verði aukið með áreiðanleika og áfallaþoli mikilvægra innviða og kerfa hins opinbera og atvinnulífsins. Stuðlað verði að uppbyggingu og rekstri stjórnkerfa um upplýsingaöryggi byggt á alþjóðlegum stöðlum.

g Netöryggi verði gert að viðeigandi hluta almannaöryggis og utanríkis-, öryggis- og varnarmála.

h Lögregla, saksóknarar, dómstólar og stjórnsýslustofnanir séu í stakk búin til að takast á við afbrot sem tengjast Netinu og því alþjóðlega samstarfi sem það kann að kalla á.

i Eftirlitsstofnanir og viðbragðskerfi séu í stakk búin til að bregðast við alvarlegum netöryggisatvikum sem ógnað geta réttindum einstaklinga, mikilvægum innviðum og samfélaginu í heild.

j Greining netógna verði styrkt og skipulagi komið á varðandi miðlun ógnamats. Einnig verði ógnamat birt reglulega opinberlega.

k Til staðar sé skilvirkt skipulag til að auðvelda ábyrgar tilkynningar um bresti í net- og hugbúnaðarkerfum og stafrænni þjónustu. Netöryggissveit Fjarskiptastofu verði tengill ábyrgrar miðlunar upplýsinga um öryggisveilur.

3.3 Samvinna

Mikilvægur þáttur og í reynd forsenda þess að ná megi markmiðum stefnunnar er að styrkja og formgera frekar samstarf innan stjórnkerfisins , við atvinnulífið og almenning, með skýrri hlutverkaskiptingu og ábyrgð. Þá þarf að tryggja virka samhæfingu opinberra aðgerðaraðila. Víðtækt samráð, samhæfing og samvinna um netöryggi skapar ekki eingöngu nauðsynlegt öryggi stafrænna lausna framtíðar, heldur leggur einnig grunn að ábatasömum iðnaði og þjónustu.

Helstu áherslur

a. Samvinna og samhæfing er varðar netöryggistengda þætti verði efld innan stjórnsýslunnar og við atvinnulíf, byggt á skýrri verkaskiptingu, þar á meðal er varðar vernd barna og byltingarkennda nýtækni, t.d. hlutanetið (e. IoT), gervigreind og skammtatölvur.

b. Tryggð verði virk samhæfing opinberra aðila vegna netöryggis stafrænnar þjónustu þeirra.

c. Þróaður verði vettvangur um víðtækt samstarf stjórnvalda, atvinnulífs og annarra haghafa, þar á meðal er varðar upplýsingamiðlun og hlutverk aðila. Stjórnvöld og atvinnulíf vinni saman, m.a. að því að leiðbeina um net- og upplýsingaöryggismál.

d. Lögð sé áhersla á fjölbreytileika og samheldni, að netöryggi sé fyrir alla og byggi á að öllum sé gert kleift að taka þátt. Hugað verði sérstaklega að aukinni þátttöku kvenna í þessu sambandi.

e. Netöryggisþekking og -menning verði efld og gerð fjölbreyttari með því að auðvelda aðkomu innflytjenda með viðeigandi menntun, reynslu og alþjóðlegt tengslanet.

f. Varnir og viðbúnaður taki mið af kviku, alþjóðlegu samstarfi á sviði netöryggis- og varnarmála.

g. Samhæfing við almannavarnaskipulag verði aukin, m.a. með auknu samráði þvert á ráðuneyti og stofnanir sem og við atvinnulífið, með auknu samstarfi og æfingum.

h. Aukin þátttaka:

   i. Í alþjóðlegu samstarfi um netöryggi, þar á meðal með setu í stjórnum og nefndum sem hafa slíkt samstarf til umfjöllunar.

   ii. Í alþjóðlegu samstarfi um netöryggismenntun, samstarfi á milli háskóla, svo sem að fá erlenda kennara til landsins og að stuðla að því að íslenskir nemendur fari til útlanda í nám.

   iii. Í netöryggisvitundarverkefnum, þar á meðal keppnum fyrir ungmenni.

   iv. Í alþjóðlegum rannsókna- og þróunarverkefnum, m.a. byggðum á klasasamstarfi.

3.4 Áhrif á íslenskt samfélag

3.4.1 Alþjóðleg

Netöryggismál eru án landamæra og Ísland er virkur þátttakandi í alþjóðlegu samstarfi, m.a. um menntun, rannsóknir, verkefni og samhæfingu stjórnskipulags. Slíkt samstarf mun gera Íslandi kleift að verða í fremstu röð í nýtingu stafrænnar tækni með öruggum hætti.

Með virkri þátttöku Íslands í alþjóðlegum samvinnuverkefnum verður hægt að byggja upp framúrskarandi netöryggishæfni og þekkingu. Sú hæfni og þekking mun m.a. nýtast í nýsköpun og þróun á sviði stafrænnar þjónustu og netöryggis og auka möguleika á samkeppnisforskoti.

Ákveðnir þættir netöryggis eru hluti öryggis- og varnarmála hérlendis og styrkja þátttöku Íslands í alþjóðlegu varnar- og öryggissamstarfi. Með traustu lagaumhverfi gegn netglæpum og getu til að bregðast við þeim má forða því að Ísland verði talið auðveld bráð í stafrænum heimi. Jafnframt verður stafrænt orðspor Íslands betra, samkeppnishæfni þess eykst og gerir landið að vænlegri fjárfestingarkosti.

3.4.2 Landshlutar

Með aukinni samhæfingu netöryggismála opinberra aðila geta sveitarfélög nýtt til fulls möguleika stafrænnar tækni og um leið veitt borgurum og lögaðilum skilvirkari og betri þjónustu, t.d. fjarheilbrigðisþjónustu, af fullnægjandi öryggi, óháð búsetu þeirra. Með samvinnu sveitarfélaga má nýta mun betur takmarkaðar auðlindir á sviði netöryggis, sem byggja á æ víðtækari þekkingu og reynslu. Áhersla á þarfir lítilla og meðalstórra fyrirtækja um land allt jafnar aðstöðu fyrirtækja og auðveldar t.d. störf án staðsetningar.

3.4.3 Atvinnulíf

Netöryggismál eru samstarfsverkefni stjórnvalda og atvinnulífs með áherslu á að efla notkun stafrænnar tækni sem byggir á traustum grunni netöryggis. Með auknu samstarfi og netöryggi er traust almennings á stafrænum lausnum líklegt til að aukast og notkunin um leið.

Kröfur atvinnulífsins um afburða netöryggishæfni fara stöðugt vaxandi enda er það grundvöllur þess að hægt verði að innleiða stafrænar lausnir í hvaða atvinnugrein sem er. Með fjölbreytileika í menntun og fræðslu á sviði netöryggismála á öllum skólastigum og á vegum atvinnulífsins næst framþróun þekkingar og hæfni sem er nauðsynleg hérlendis og í alþjóðlegri samkeppni.

Með umbótum í löggæslu á Netinu verða leiðir lítilla og meðalstórra fyrirtækja í þéttbýli og dreifbýli til að tilkynna afbrot, fá ráðgjöf og leita réttar síns jafnframt gerðar greiðari.

3.4.4 Almenningur

Meiri samvinna gefur samfélaginu möguleika á að efla þróun netöryggis svo almenningur geti nýtt sér þau fjölmörgu tækifæri sem liggja í stafrænum lausnum. Hlutverk stjórnvalda felst í fyrirbyggjandi aðgerðum sem og viðbragði þegar hætturnar steðja að. Þannig byggist upp traust almennings á netöryggi landsins og þeirri stafrænu þjónustu sem er veitt. Á grunni vitundarvakningar og fræðslu getur almenningur áttað sig betur á ábyrgð sinni við notkun Netsins. Með áherslu á fjölbreytileika og samheldni verður lögð áhersla á að allir geti bæði notið netöryggis og orðið virkir þátttakendur í að skapa það. Sérstaklega er hugað að þörfum einstakra hópa, t.d. barna, og samvinnu við eldri borgara. Með umbótum í löggæslu á Netinu verða leiðir almennings til að tilkynna afbrot og leita réttar síns jafnframt gerðar greiðari.

Allir munu geta fundið í verki að verndar laga og réttar gæti einnig á Netinu.

Stjórnarráð Íslands
Háskóla-, iðnaðar- og nýsköpunarráðuneytið