Skýrsla um lagaumhverfi og stjórnsýslu netöryggismála

Lagastofnun Háskóla Íslands
Friðrik Árni Friðriksson Hirst framkvæmdastjóri
Febrúar 2024 (viðauki frá júní 2024)

Efnisyfirlit

1. Inngangur. Skilgreining netöryggis og stefnumörkun

Skýrsla þessi er samin að beiðni háskóla-, iðnaðar- og nýsköpunarráðuneytisins og er tilgangur hennar að veita yfirsýn yfir helstu atriði lagaumhverfis og stjórnsýslu netöryggismála. Skýrslunni er einkum ætlað að varpa ljósi á verkefni ráðuneyta og annarra stjórnvalda sem hafa hlutverki að gegna í málaflokknum, en hann skarast við mörg svið stjórnsýslunnar eins og nánar verður rakið hér á eftir. Í skýrslu þessari er ekki tekin afstaða til þess hvernig skipan netöryggismála er best fyrir komið í stjórnkerfinu, svo sem hvað varðar verkaskiptingu ráðuneyta og stofnana, heldur er það tilgangur skýrslunnar að lýsa gildandi rétti og draga ályktanir af honum til að veita yfirsýn yfir lagalega hlið málaflokksins. Þar sem viðfangsefnið er afar víðfeðmt er eðli málsins samkvæmt ekki um tæmandi úttekt að ræða, heldur almennt yfirlit.

Í þjóðaröryggisstefnunni er m.a. lögð áhersla á að „efla stafrænt fullveldi og auka net- og upplýsingaöryggi á öllum sviðum samfélagsins með samhæfðum aðgerðum, áframhaldandi uppbyggingu á eigin getu og með samstarfi við önnur ríki“.[1] Jafnframt er lögð áhersla á „vernd og órofa virkni mikilvægra innviða og styrkingu áfallaþols samfélagsins gagnvart hvers kyns ógnum.“[2] Í skýringargögnum er m.a. vísað til þess að netið sé burðarás nútímaþjóðfélags og undirstaða daglegs lífs, atvinnu, þjónustu og tæknilegra framfara. Net- og upplýsingaöryggi sé jafnframt þverfaglegt viðfangsefni sem krefst víðtækrar samvinnu og samhæfingar fjölmargra aðila innan og utan stjórnkerfisins. Vakin er athygli á því að mikilvægir samfélagsinnviðir eru í vaxandi mæli sjálfvirkir og samtengdir net- og upplýsingakerfum, sem skapar hættu á netárásum. Þá er bent á að netið sé nú í auknum mæli vettvangur stafrænnar brotastarfsemi. Sameiginlegt einkenni stafrænna brota er að þau eru framin á netinu, í gegnum net- og samskiptamiðla eða fyrir tilstuðlan einhvers konar nettengds búnaðar.[3]

Í íslenskum lögum er ekki að finna almenna skilgreiningu á hugtakinu „netöryggi“ (e. cyber security). Í netöryggisstefnu 2022-2037 er *netöryggi* sagt felast í „öryggi

[1] Skýrslan miðast við réttarástandið eins og það var í febrúar 2024, og í júní 2024 hvað varðar viðauka.
[2] Þjóðaröryggisstefna fyrir Ísland, þingsályktun nr. 26/145, breytt með þingsályktun nr. 7/153 (153. lögþ. 2022–2023, þskj. 577 - 487. mál).
[3] Greinargerð með þingsályktun nr. 7/153. Sjá einnig skýrslu greiningardeildar ríkislögreglustjóra, Tölvu- og netglæpir, 2016, bls. 24.

stafrænnar þjónustu og lausna og öryggi í notkun þeirra, þar sem Netið kemur við sögu“.[4] *Netöryggisógnir* og *netöryggisatvik* vísa almennt til atvika sem ógna eða skerða netöryggi, þar á meðal netglæpa. Hér er bæði átt við atvik af mannavöldum, hvort sem er vilja- eða gáleysisverk eða óhappatilvik, sem og ytri atvik á borð við náttúruhamfarir.[5]

Samkvæmt netöryggisstefnunni eru *netglæpir* „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“. Bent er á í netöryggisstefnunni að „hefðbundin notkun“ stafrænna lausna og netsins til að fremja afbrot, svo sem selja ólöglega vöru eða þjónustu, eða beita misnotkun eða ofbeldi, teljist einnig vera netglæpur.[6]

Í riti Jónatans Þórmundssonar, Afbrot og refsiábyrgð I, tekur höfundur fram að erfitt sé að skilgreina netglæpi á markvissan hátt. Hann greinir milli *netglæpa* og *tölvubrota*, þ.e. tölvubrot séu hrein innanríkisbrot en netglæpir teljist frekar til fjölþjóðabrota (e. transnational crime).[7] Samkvæmt hugtakanotkun netöryggisstefnunnar hér að framan má fella tölvubrot undir netglæpi og verður það lagt til grundvallar hér.[8] Margvíslegar ástæður geta búið að baki netglæpum, t.d. fjárhagslegur ávinningur og pólitísk eða hugmyndafræðileg markmið. Tilgangur netglæpa getur einnig verið að valda tjóni eða grafa undan öryggi eða stöðugleika almennt, t.d. þegar erlent ríki stendur að netárás á mikilvæga innviði.[9] Netglæpir varða ýmist við sértæk refsiákvæði, sjá t.d. tölvubrota-ákvæði 249. gr. a almennra hegningarlaga nr. 19/1940, eða við almenn refsiákvæði í

[4] *Netöryggisstefna Íslands 2022-2037*, bls. 7. Sjá einnig eldri *netöryggisstefnu 2015-2026.*
[5] *Netöryggisstefna Íslands 2022-2037*, bls. 8.
[6] *Netöryggisstefna Íslands 2022-2037*, bls. 7.
[7] Jónatan Þórmundsson, *Afbrot og refsiábyrgð I* (2023), bls. 167-168. Höfundur greinir einnig milli *netháðra* brota (e. cyber-dependent crimes) og *netvirkra* brota (e. cyber-enabled crimes). Í fyrri flokkinn falla brot sem geta eingöngu átt sér stað á netinu og fyrir tilstilli þess, t.d. netinnbrot og netárásir með spilliforritum og tölvuóværum (e. malware), en í síðari flokkinn falla brot sem unnt er að fremja án atbeina netsins en hafa stigmagnast með netinu.
[8] Sjá yfirlit yfir helstu tegundir tölvu- og netglæpa í skýrslu greiningardeildar ríkislögreglustjóra, Tölvu- og netglæpir – áhættu- og ógnarmat (2016), bls. 5 o.áfr.
[9] Greiningardeild ríkislögreglustjóra, *Tölvu- og netglæpir – áhættu- og ógnarmat* (2016), bls. 24-25.

þeim lögum sem eru ekki sérstaklega bundin við tölvur eða netið.[10] Ætla má að stór hluti netglæpa sé ekki kærður til lögreglu og er umfang þeirra lítt þekkt.[11]

Á vettvangi Atlantshafsbandalagsins (NATO) hefur jafnframt verið lögð aukin áhersla á mikilvægi þess að aðildarríki geri ráðstafanir til að efla viðnámsþol sitt (e. resilience), en liður í því er m.a. að tryggja virkni og öryggi mikilvægra innviða. Í grunnstefnu NATO frá 2022 er í þessu sambandi m.a. vakin athygli á mikilvægi þess að aðildarríki dragi úr þýðingarmiklum veikleikum og fækki sviðum þar sem þau eru háð öðrum, þ.m.t. að því er varðar mikilvæga innviði, aðfangakeðjur, orkubirgðir og heilbrigðiskerfi. Þá eru höfð uppi varnaðarorð um að andstæðingar NATO leitist við að nýta sér það að aðildarríkin eru opin, samtengd og stafræn. Mikilvægt sé að verjast ógnum sem felast m.a. í skaðlegri íhlutun óvinveittra aðila í mikilvæga innviði og aðrar samfélagslegar undirstöður í aðildarríkjunum.[12]

2. Lagaumhverfi netöryggis

2.1. Almennt

Gildandi regluverk um netöryggi samanstendur af ákvæðum ýmissa laga og stjórnvaldsfyrirmæla. Það sem e.t.v. kemst næst heildarlögum um netöryggi eru lög nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða (NIS-lögin), sem innleiða netöryggistilskipun ESB 2016/1148 (NIS 1-tilskipunin).[13] Lög nr. 78/2019 gilda um netöryggi rekstraraðila sem teljast til mikilvægra innviða í skilningi laganna, þ.m.t. rekstraraðila nauðsynlegrar þjónustu sem nánar verður vikið að hér á eftir. Með stoð í

[10] Ýmis ákvæði hegningarlaga eru eðli málsins samkvæmt ekki orðuð með rafræn viðskipti eða stafræna miðla í huga, m.a. ákvæði um auðgunarbrot. Um skýringarvafa af þeim toga, sjá t.d. *H 184/2011*. Á það skortir að ákvæði almennra hegningarlaga hafi verið endurskoðuð með hliðsjón af netglæpum og stafrænni tækni almennt og kunna ákvæðin því að vera gloppótt eða endasleppt í því tilliti, sem bitnar á netöryggi. *H 184/2011* er þó til marks um að dómstólar kunni að skýra ákvæði hegningarlaga rúmt í takt við nútímatækni. Ekki er þó hægt að gefa sér að rúm lögskýring refsiákvæða sé tæk í öllum tilvikum.

[11] Greiningardeild ríkislögreglustjóra, *Tölvu- og netglæpir – áhættu- og ógnarmat* (2016), bls. 26. Á bls. 24 í þeirri skýrslu er einnig bent á að það líða að meðaltali 200 dagar frá því að utanaðkomandi aðili getur hagnýtt sér veikleika tölvukerfis þar til að upp kemst um öryggisrofið og veikleikar eru lagfærðir.

[12] *Grunnstefna NATO 2022* (NATO 2022 Strategic Concept).

[13] Tilskipun ESB 2016/1148 varðandi ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum í Sambandinu. NIS stendur fyrir „network and information systems“. Sjá einnig NIS 2 tilskipun ESB 2022/2555 sem verður innleidd hér á landi á næstunni og mun víkka út gildissvið reglnanna svo þær nái yfir talsvert fleiri tegundir rekstraraðila, sem skipt er í tvo flokka, þ.e. nauðsynlega og mikilvæga aðila.

þeim lögum hefur verið sett reglugerð nr. 866/2020 um öryggi net- og upplýsingakerfa rekstraraðila mikilvægrar þjónustu, auk reglugerðar nr. 1255/2020 um öryggi net- og upplýsingakerfa veitenda stafrænnar þjónustu, sbr. einnig auglýsingu nr. 1331/2023 sem geymir skrá yfir rekstraraðila nauðsynlegrar þjónustu hér á landi.

Í lögum nr. 70/2022 um fjarskipti er fjallað um skyldur fjarskiptafyrirtækja á sviði netöryggis. Á grundvelli eldri laga um fjarskipti nr. 81/2003 voru settar reglur nr. 1221/2007 um vernd upplýsinga í almennum fjarskiptanetum og reglur nr. 1222/2007 um virkni almennra fjarskiptaneta, en þær reglur njóta nú lagastoðar í gildandi fjarskiptalögum og kveða nánar á um skyldur fjarskiptafyrirtækja á sviði netöryggis.[14] Þá hafa lög nr. 75/2021 um Fjarskiptastofu að geyma ákvæði um netöryggi, einkum netöryggissveit (CERT-IS), en um sveitina er einnig fjallað í ákvæðum laga nr. 78/2019 og 70/2022, auk reglugerðar nr. 480/2021, sbr. nánari umfjöllun hér á eftir.

Í næstu köflum verður gefið almennt yfirlit yfir efnisreglur laga nr. 78/2019 og laga nr. 70/2022. Í framhaldi af þeirri umfjöllun verður gerð grein fyrir verkefnum einstakra stjórnvalda á sviði netöryggis, einkum netöryggissveitar Fjarskiptastofu.

2.2. Lög um öryggi net- og upplýsingakerfa mikilvægra innviða

2.2.1. Gildissvið – mikilvægir innviðir

Áður var vikið að lögum nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða, sem fela í sér innleiðingu á netöryggistilskipun ESB 2016/1148 (NIS 1). Í 24. tölul. 6. gr. laganna er *öryggi net- og upplýsingakerfa* skilgreint svo: „Geta net- og upplýsingakerfis til að standast, með tilteknu öryggisstigi, hvers konar aðgerðir sem stofna í hættu aðgengi að sannvottuðum uppruna, réttleika eða trúnaði um vistuð, send eða unnin gögn eða tengda þjónustu sem boðin er eða er aðgengileg um þessi net- og

[14] Ákvæði til bráðabirgða I. laga nr. 70/2022 um fjarskipti.

upplýsingakerfi.“[15] Öryggi net- og upplýsingakerfa snýst m.ö.o. um að tryggja leynd, rekjanleika, réttleika og tiltækileika þeirra gagna og upplýsinga sem um ræðir.[16]

Eins og heiti laga nr. 78/2019 ber með sér miðast gildissvið þeirra við net- og upplýsingakerfi aðila (einkaaðila og opinberra aðila) sem skilgreindir eru sem *mikilvægir innviðir*.[17] Þeir greinast í tvo meginflokka og gilda að sumu leyti ólíkar kröfur til netöryggis í hvorum flokki um sig:

- *Rekstraraðilar nauðsynlegrar þjónustu*, á sviði bankastarfsemi og innviða fjármálamarkaða, flutninga, heilbrigðisþjónustu, orku- og hita- og vatnsveitna, svo og stafrænna grunnvirkja, sbr. 3. og 6. gr. laganna, sbr. og nánar reglugerð nr. 866/2020 og auglýsingu nr. 1331/2023.[18]
- *Veitendur stafrænnar þjónustu*, þ.e. þjónustu í skilningi b-liðar 1. mgr. 1. gr. tilskipunar ESB 2015/1535, sbr. skilgreiningu í 6. gr. laga nr. 78/2019 á hugtökunum netmarkaður, leitarvél á netinu eða skýjavinnsluþjónusta, sbr. og nánar reglugerð nr. 1255/2020.[19]

Þar sem gildissvið laga nr. 78/2019 nær yfir mörg svið innviða og atvinnustarfsemi gegna ýmis stjórnvöld eftirlitshlutverki samkvæmt lögunum. Fjarskiptastofa gegnir þar hlutverki samhæfingarstjórnvalds, sem og tengiliðar íslenskra stjórnvalda vegna framkvæmdar tilskipunar 2016/1148, sbr. 13. gr. laganna. Í 30. gr. reglugerðar nr. 866/2020 er kveðið nánar á um hlutverk Fjarskiptastofu sem samhæfingarstjórnvalds. Þar segir að samhæfingarstjórnvald sinni almennri stefnumörkun um eftirlit með lágmarkskröfum um öryggi net- og upplýsingakerfa mikilvægra innviða samkvæmt

[15] Samkvæmt 15. tölul. 6. gr. laga nr. 78/2019 merkir net- og upplýsingakerfi: „Fjarskiptanet í skilningi laga um fjarskipti; tæki eða samsafn innbyrðis tengdra eða skyldra tækja þar sem í einu þeirra eða fleiri fer fram sjálfvirk stafræn gagnavinnsla eftir forriti; eða stafræn gögn sem eru geymd, unnin, sótt eða send fyrir tilstilli þátta sem falla undir framangreint að því er varðar starfrækslu þeirra, notkun, verndun og viðhald.“ Sjá einnig efnislega sömu skilgreiningar í 4. gr. tilskipunar ESB 2016/1148. Sjá einnig, Jónatan Þórmundsson, *Afbrot og refsiábyrgð I* (2023), bls. 167-168.

[16] Sjá nánar, Greiningardeild ríkislögreglustjóra, *Tölvu- og netglæpir – áhættu- og ógnarmat* (2016), bls. 30.

[17] Sjá 2. gr. laga nr. 78/2019 og skilgreiningu á mikilvægum innviðum í 13. tölul. 6. gr. laganna.

[18] Sjá einnig m.a. 1. og 3. mgr. 3. gr. laga nr. 78/2019 þar sem finna má sjónarmið sem lúta að því hvenær aðili telst falla undir rekstraraðila nauðsynlegrar þjónustu, en í því sambandi skiptir einkum máli hvort þjónustan sé háð net- og upplýsingakerfum og hvort öryggisbrestur varðandi slík kerfi hefði verulega skerðandi áhrif á veitingu þjónustunnar, að teknu tilliti til fjölda og eðlis þjónustunotenda, o.fl.

[19] Tilskipun ESB 2015/1535 um tilhögun miðlunar upplýsinga um tæknireglugerðir og reglur um þjónustu í upplýsingasamfélaginu (kerfisbinding).

lögum nr. 78/2019 með það að markmiði að stuðla að sem bestri samræmingu og jafnræði við framkvæmd laganna, en í því skyni er samhæfingarstjórnvaldi meðal annars heimilt að gefa út almenn leiðbeinandi tilmæli um framkvæmd eftirlits, svo sem aðferðarfræði úttekta. Þá skuli samhæfingarstjórnvald vera tengiliður milli eftirlitsstjórnvalda og hvetja til reglulegra upplýsingafunda og samskipta meðal eftirlitsstjórnvalda og að það skuli koma á og leiða samráðsvettvang eftirlitsstjórnvalda til að miðla þekkingu og reynslu sem og að samhæfa framkvæmd eftirlits. Þessu til viðbótar skal samhæfingarstjórnvald leitast við að verða við beiðni eftirlitsstjórnvalds um aðstoð við undirbúning, framkvæmd og eftirfylgni úttekta á grundvelli laga nr. 78/2019.

Verkaskipting milli einstakra eftirlitsstjórnvalda samkvæmt lögum nr. 78/2019 er með eftirfarandi hætti, sbr. 1. mgr. 11. gr. laganna:

Rekstraraðilar nauðsynlegrar þjónustu	**Eftirlitsstjórnvald**
Orka og hitaveitur	Orkustofnun
Flutningar	Samgöngustofa
Bankastarfsemi og innviðir fjármálamarkaða	Seðlabanki Íslands
Heilbrigðisþjónusta	Embætti landlæknis
Vatnsveitur	Umhverfisstofnun
Stafræn grunnvirki	Fjarskiptastofa
Veitendur stafrænnar þjónustu	Fjarskiptastofa

Það er í verkahring hlutaðeigandi eftirlitsstjórnvalds að tilgreina þá aðila sem falla undir rekstraraðila nauðsynlegrar þjónustu innan einstakra sviða, sbr. töfluna hér að framan. Slíkar ákvarðanir skulu teknar „eftir því sem tilefni er til og a.m.k. á tveggja ára fresti“ og tilkynntar Fjarskiptastofu, sbr. 2. mgr. 11. gr. laga nr. 78/2019. Ef aðili veitir jafnframt þjónustu í öðru ríki á EES skal viðhafa samráð við þarlend stjórnvöld áður en ákvörðun er tekin. Ákvörðun um að tilgreina aðila sem rekstraraðila nauðsynlegrar þjónustu lýtur málsmeðferðarreglum stjórnsýsluréttar, þ.m.t. um andmælarétt, sbr. einnig fyrrnefnt lagaákvæði. Slík ákvörðun verður ekki kærð til æðra stjórnvalds, sbr. 6. mgr. 23. gr.

laganna, en verður borin undir dómstóla.[20] Jafnframt skal ráðherra halda opinbera skrá yfir rekstraraðila nauðsynlegrar þjónustu hér á landi og birta með auglýsingu í B-deild Stjórnartíðinda að fenginni tillögu Fjarskiptastofu, sbr. 4. mgr. 3. gr. laganna. Skráin skal uppfærð eftir því sem tilefni er til og á a.m.k. tveggja ára fresti. Skráin nær ekki til veitenda stafrænnar þjónustu.

Í gildandi skrá ráðherra, sbr. auglýsingu nr. 1331/2023, eru 68 aðilar tilgreindir sem rekstraraðilar nauðsynlegrar þjónustu.[21] Skráningu aðila er ekki að fullu lokið en stefnt er að því að ljúka henni á næstu misserum.

Það ber að hafa í huga að gildissvið laga nr. 78/2019 er afmarkað við þá rekstraraðila sem áður voru nefndir, í samræmi við NIS 1 tilskipunina sem lögunum er ætlað að innleiða. Gildissvið laganna er þannig sértækt og undanskilur starfsemi í þjóðfélaginu sem gæti þó verið rökrétt að flokka sem mikilvæga innviði, t.d. innan menntakerfisins og löggæslu.[22] Þó er fyrirséð að gildissvið þessara lagareglna muni taka breytingum til rýmkunar á næstu misserum. Stafar það einkum af tilskipun ESB 2022/2555, þ.e. svonefndri NIS 2 tilskipun sem tekur við NIS 1, sem gerir ráð fyrir verulegri fjölgun rekstraraðila sem falla munu undir umræddar reglur. NIS 2 hefur ekki verið tekin upp í EES-samninginn enn sem komið er en þrátt fyrir það er hafinn undirbúningur að innleiðingu hennar í íslenskan rétt.

Þá ber að nefna að þótt gildissvið laga nr. 78/2019 miðist í meginatriðum við mikilvæga innviði, taka lögin að ákveðnu leyti einnig til Stjórnarráðs Íslands og opinberra stofnana, þ.e. annarra stofnana en þeirra sem teljast mikilvægir innviðir í skilningi laganna. Nánar verður vikið að þessum atriðum í umfjöllun um netöryggissveit hér síðar.

[20] Í tilviki ákvarðana Fjarskiptastofu gildir þriggja mánaða málshöfðunarfrestur, sbr. 4. mgr. 20. gr. laga nr. 75/2021.
[21] Auglýsing nr. 1331/2023 ásamt viðauka var birt í B-deild Stjórnartíðinda 5. desember 2023 og leysti af hólmi eldri auglýsingar nr. 70/2021 og 67/2022.
[22] Sjá m.a. umfjöllun um mikilvæga innviði og samfélagsverkefni í skýrslu almannavarnadeildar ríkislögreglustjóra, *Mikilvæg verkefni í samfélaginu*, 2021, sbr. einnig NOU 2006:6, *Når sikkerheten er viktigst*.

2.2.2. Kröfur til netöryggis mikilvægra innviða

Ákvæði laga nr. 78/2019 leggja ýmsar skyldur á mikilvæga innviði til fyrirbyggjandi ráðstafana til verndar öryggi net og upplýsingakerfa þeirra. Meðal annars skulu þeir skv. 7. gr. laganna hafa skjalfesta stefnu og ferla til að meta, stýra og lágmarka áhættu sem steðjað getur að öryggi net- og upplýsingakerfa þeirra, þ.m.t. vegna fátíðra atburða sem geta haft alvarlegar afleiðingar. Þá skulu þeir setja sér öryggisstefnu, framkvæma áhættumat reglubundið og ákvarða og endurmeta öryggisráðstafanir á grundvelli þess.[23] Enn fremur skulu mikilvægir innviðir hafa skjalfesta viðbragðsáætlun og áætlun um samfelldan og órofinn rekstur og þjónustu til að tryggja takmörkun á tjóni ef alvarleg röskun verður á starfsemi þeirra. Verkferlum og viðbrögðum við atvikum í eða tengdum rekstri net- og upplýsingakerfa mikilvægra innviða skulu gerð skil í áætlunum, þar á meðal skráningu atvika. Meðhöndlun atvika skal m.a. fela í sér að finna orsakir þeirra, koma aftur á eðlilegu rekstrarástandi og koma í veg fyrir að atvik endurtaki sig. Þá skal í starfsemi mikilvægra innviða vera til staðar virkt kerfi innra eftirlits sem samræmist lögum þessum og sérlögum sem um starfsemi þeirra kunna að gilda.[24] Í reglugerð nr. 866/2020 um öryggi net- og upplýsingakerfa rekstraraðila mikilvægrar þjónustu, og reglugerð nr. 1255/2020 um öryggi net- og upplýsingakerfa veitenda stafrænnar þjónustu, er kveðið nánar á um þær netöryggiskröfur sem gerðar eru til mikilvægra innviða svo sem um lágmarkskröfur um áhættustýringu og kröfur um skipulagslegar ráðstafanir, tæknilegar ráðstafanir, viðhald, viðbragðsáætlun, innra eftirlit og atvika-tilkynningar.

Samkvæmt 12. gr. laga nr. 78/2019 er viðkomandi eftirlitsstjórnvaldi m.a. heimilt að gangast fyrir úttektum og prófunum varðandi netöryggi mikilvægra innviða og krefja þá um upplýsingar vegna eftirlits með öryggi net- og upplýsingakerfa þeirra. Jafnframt getur eftirlitsstjórnvald óskað eftir reglubundinni skýrslugjöf mikilvægra innviða um meðhöndlun einstakra atvika, auk þess að kalla einstaklinga til skýrslugjafar vegna

[23] Með öryggisráðstöfunum er átt við bæði tæknilegar og skipulagslegar ráðstafanir, eftir því sem við kann að eiga. Aðgangsstýring skal viðhöfð í rekstri net- og upplýsingakerfa mikilvægra innviða eftir því sem við á og viðeigandi prófanir framkvæmdar reglubundið og í samræmi við alþjóðleg viðmið um bestu framkvæmd á hverjum tíma.

[24] Sjá enn fremur ítarleg fyrirmæli um öryggisráðstafanir o.fl. í reglugerðum nr. 866/2020 (rekstraraðilar nauðsynlegrar þjónustu) og 1255/2020 (veitendur stafrænnar þjónustu).

tiltekinna mála. Samkvæmt 5. mgr. 12. gr. laganna getur eftirlitsstjórnvald einnig veitt mikilvægum innviðum fyrirmæli um úrbætur ef í ljós kemur við eftirlit að þeir fylgi ekki lögunum eða öðrum reglum sem gilda um net- og upplýsingakerfi. Um eftirlit fer einnig eftir þeim sérlögum sem gilda um einstaka mikilvæga innviði, sbr. 5. gr. laganna.

Á mikilvægum innviðum hvílir skylda til að tilkynna netöryggissveit Fjarskiptastofu um alvarleg atvik eða áhættu sem ógnar öryggi net- og upplýsingakerfa þeirra, sbr. 8. gr. laga nr. 78/2019. Að slíkum tilkynningum verður jafnframt vikið í umfjöllun um netöryggissveit hér síðar.

Brot gegn tilgreindum ákvæðum laga nr. 78/2019 geta varðað stjórnvaldssektum, sem lagðar eru á af viðkomandi eftirlitsstjórnvaldi, sbr. 23. gr. laganna. Enn fremur geta slík brot varðað hefðbundinni refsiábyrgð í sakamáli, sbr. 26. gr. laganna. Þetta á m.a. við um brot gegn 7. gr. laganna um lágmarkskröfur um áhættustýringu og viðbúnað og 8. gr. um tilkynningarskyldu til netöryggissveitar. Einnig varðar það refsingu samkvæmt 120. gr. og 120. gr. a almennra hegningarlaga að gefa af ásetningi eða stórkostlegu gáleysi ranga tilkynningu til netöryggissveitar skv. 8. eða 15. gr. laga nr. 78/2019, sbr. 4. mgr. 26. gr. Hvort tveggja einstaklingum og lögaðilum verður gerð stjórnvaldssekt eða hefðbundin refsing í sakamáli samkvæmt nefndum ákvæðum laga nr. 78/2019. Eftirlitsstjórnvaldi er heimilt að kæra til lögreglu brot gegn lögum nr. 78/2019, sbr. 1. mgr. 25. gr., og er skylt að gera það ef brot er meiri háttar, sbr. 2. mgr. sama ákvæðis. Þess skal getið að ákvæðið gerir það ekki að almennu skilyrði þess að brot gegn lögum nr. 78/2019 sæti rannsókn lögreglu að eftirlitsstjórnvald hafi lagt fram kæru.[25]

2.3. Fjarskiptalög

Áður var vikið að lögum nr. 70/2022 um fjarskipti sem kveða á um skyldur fjarskiptafyrirtækja á sviði netöryggis. Spyrja má hvers vegna mæla þurfi fyrir um slíkar skyldur í fjarskiptalögum til viðbótar lögum nr. 78/2019. Því er til að svara að þær netöryggiskröfur sem kveðið er á um í XII. kafla laga nr. 70/2022 um fjarskipti eru settar til innleiðingar á 40. gr. tilskipunar ESB 2018/1972 um setningu evrópskra reglna um rafræn fjarskipti. Regluverk ESB á sviði netöryggis er því tvískipt þar sem annars vegar

[25] Sjá, til samanburðar, gagnstæða reglu í 1. mgr. 42. gr. samkeppnislaga nr. 44/2005, þar sem segir að brot gegn lögunum sæti aðeins rannsókn lögreglu að undangenginni kæru Samkeppniseftirlitsins.

er kveðið á um netöryggiskröfur mikilvægra innviða í tilskipun 2016/1148 (NIS) og hins vegar er kveðið sérstaklega á um netöryggi fjarskiptafyrirtækja í tilskipun 2018/1972.

Í XII. kafla laga nr. 70/2022 er að finna ítarleg fyrirmæli m.a. um öryggi upplýsinga, fjarskiptaneta og fjarskiptaþjónustu. Í 78. gr. laganna er m.a. ráðgert að fjarskiptafyrirtæki setji sér skjalfesta öryggisstefnu og viðbragðsáætlun, svo og áætlun um samfelldan og órofinn rekstur og fjarskiptaþjónustu til að tryggja takmörkun á tjóni ef alvarleg röskun verður á starfsemi þess. Jafnframt er ráðgert að fjarskiptafyrirtæki framkvæmi reglubundið áhættumat og endurmeti öryggisráðstafanir á þeim grunni, auk þess að hafa virkt innra eftirlit. Einnig er gert ráð fyrir í ákvæðinu að fjarskiptafyrirtæki hafi samráð sín á milli um netöryggi o.fl. ef þau nota fjarskiptanet hvers annars. Þá geymir ákvæðið fyrirmæli um netöryggi vegna útvistunar fjarskiptastarfsemi m.a. út fyrir íslenska lögsögu.[26] Í reglum nr. 1221/2007 um vernd upplýsinga í almennum fjarskiptanetum og reglum nr. 1222/2007 um virkni almennra fjarskiptaneta er svo kveðið nánar á um þær netöryggiskröfur sem gerðar eru til fjarskiptafyrirtækja svo sem almennar kröfur til leyndar í fjarskiptum, réttleika upplýsinga, öryggiskipulag, innra eftirlit og ýmsar öryggisráðstafanir, á borð við aðgangstýringu og skipulags- og tæknilegar ráðstafanir, kröfur um neyðaráætlun, raunlæga vernd og kröfur um virkni og stjórn fjarskiptaneta og meðhöndlun öryggisatvika.

Fjarskiptastofu er heimilt samkvæmt 79. gr. laga nr. 70/2022 að gangast fyrir úttektum og prófunum varðandi netöryggi fjarskiptafyrirtækja, auk þess að framkvæma mat á heildstæði, öryggi og virkni almennra fjarskiptaneta með tilliti til áhættu. Þá getur Fjarskiptastofa, svo að dæmi sé nefnt, lagt fyrir fjarskiptafyrirtæki að það framkvæmi sértækt áhættumat á einstökum rekstrar- og kerfisþáttum fjarskiptaneta, sérstökum ógnum o.fl., sbr. 8. mgr. 78. gr. laganna.

Þá ber fjarskiptafyrirtækjum að tilkynna til netöryggissveitar Fjarskiptastofu öll alvarleg öryggisatvik sem ógna öryggi eða virkni almennra fjarskiptaneta eða -þjónustu, sbr. 1.

[26] Samkvæmt 11. mgr. 78. gr. laga nr. 70/2022 getur ráðherra ákveðið í reglugerð, að fengnum umsögnum Fjarskiptastofu og ríkislögreglustjóra að kerfi og búnaður í fjarskiptanetum sem teljast mikilvæg með tilliti til almannahagsmuna eða þjóðaröryggis skuli vera staðsett eða rekin í íslenskri lögsögu, eins og nánar greinir í ákvæðinu. Slík reglugerðarfyrirmæli hafa ekki verið sett svo séð verði.

og 2. mgr. 80. gr. laganna. Gerð verður nánari grein fyrir tilkynningarskyldu til net- öryggissveitar í umfjöllun um sveitina hér síðar.

Sérstök skylda hvílir að auki á fjarskiptafyrirtækjum um að tilkynna Fjarskiptastofu (ekki netöryggissveit) um það ef hætta er á að öryggi eða leynd upplýsinga á fjarskiptanetum verði rofin eða ef til rofs hefur komið, sbr. 3. mgr. 80. gr. laga nr. 70/2022. Sú tilkynningarskylda, sem á rætur að rekja til tilskipunar ESB 2002/58/EB um persónuvernd á sviði fjarskipta, hvílir á öðrum grunni en almenn tilkynningarskylda til netöryggissveitar skv. 1. og 2. mgr. Í skýringum við 3. mgr. er rakið að ákvæðið varði „fjarskiptaleyndina sérstaklega". Rétt þyki „að hafa það í sérstöku ákvæði þar sem þeir matskenndu þættir sem tilgreindir eru í 2. mgr. og varða virkni neta og þjónustu eiga ekki við þegar kemur að öryggi upplýsinganna sjálfra".[27] Tilkynningarskylda skv. 3. mgr. stendur því sjálfstætt en getur þó eftir atvikum átt við samhliða tilkynningarskyldu skv. 1. og 2. mgr.

Samkvæmt 1. mgr. 81. gr. laga nr. 70/2022 ber fjarskiptafyrirtæki skylda til að upplýsa hlutaðeigandi notendur án endurgjalds um það ef sérstök eða umfangsmikil ógn steðjar að fjarskiptaneti eða -þjónustu, m.a. hættu á að leynd eða öryggi fjarskipta verði rofin. Jafnframt skal upplýsa um mögulegar öryggisráðstafanir og úrræði sem hægt er að grípa til. Þá er Fjarskiptastofu heimilt skv. 2. mgr. 81. gr. laganna að upplýsa almenning um einstök öryggisatvik eða kveða á um að fjarskiptafyrirtæki geri slíkt ef almennings- vitundar er þörf til að koma í veg fyrir eða takast á við öryggisatvik og þegar upplýsingagjöf um öryggisatvik er af öðrum ástæðum nauðsynleg í þágu almanna- hagsmuna. Fjarskiptastofu er einnig heimilt samkvæmt sama ákvæði að tilkynna almenningi um veikleika og almennar hættur ef það er nauðsynlegt í þágu almanna- hagsmuna, eftir atvikum í samráði við lögreglu.[28] Framangreindu til viðbótar er mælt svo fyrir í 3. mgr. 81. gr. laga nr. 70/2022 að Fjarskiptastofa skuli, ef þörf krefur, upplýsa eftirlitsstjórnvöld í öðrum aðildarríkjum EES og Netöryggisstofnun Evrópu (ENISA) um öryggisatvik. Þá skal Fjarskiptastofa senda síðarnefndu stofnuninni og Eftirlits-

[27] Athugasemdir við 80. gr. í greinargerð með frumvarpi til laga nr. 70/2022 (149. lögþ. 2021-2022, þskj. 666 – 461. mál). Sjá tilskipun 2002/58/EB vinnslu persónuupplýsinga og um verndun einkalífs á sviði rafrænna fjarskipta (tilskipun um friðhelgi einkalífsins og rafræn fjarskipti).
[28] Sjá einnig 10. gr. laga nr. 78/2019.

stofnun EFTA árlega yfirlitsskýrslu um tilkynnt öryggisatvik skv. 80. gr. laganna og meðhöndlun þeirra. Sjá einnig umfjöllun um netöryggissveit hér síðar.

Þá má nefna ákvæði XIV. kafla laga nr. 70/2022 um neyðar- og öryggisfjarskipti og fjarskipti á hættutímum. Hér má nefna 100. gr. sem veitir stjórnvöldum heimildir til að hlutast til um fjarskipti í þágu öryggis almennings o.fl. þegar hætta steðjar að, auk 2. mgr. 95. gr. þar sem ráðherra er veitt heimild til kveða í reglugerð á um auknar kröfur til skipulags net- og upplýsingaöryggis og fyrirkomulag áhættustýringar neyðar- og öryggisfjarskipta og tengdra fjarskiptaneta.[29]

Að lokum er kveðið á um það í 3. mgr. 79. gr. laga nr. 70/2022 að ef í ljós kemur að fjarskiptafyrirtæki uppfylla ekki kröfur 78. gr. laganna þá getur Fjarskiptastofa veitt fjarskiptafyrirtæki fyrirmæli um úrbætur. Hefur Fjarskiptastofa einnig heimild til að leggja á fjarskiptafyrirtæki stjórnvaldssekt sem numið getur allt að 4% af heildarveltu síðasta rekstrarárs ef brotið hefur verið gegn 78. gr., 80. gr., og 1. mgr. 81. gr. laganna, sbr. 103. gr. sömu laga. Brot gegn lögum nr. 70/2022 og reglum settum á grundvelli þeirra sæta aðeins rannsókn lögreglu að undangenginni kæru Fjarskiptastofu, en ef brot er meiri háttar er Fjarskiptastofu skylt að vísa þeim til lögreglu, sbr. 105. gr. laganna.

3. Verkefni stjórnvalda á sviði netöryggis

3.1. Almennt

Helstu verkefni á sviði netöryggis heyra undir nokkra opinbera aðila. Netöryggi heyrir stjórnarfarslega undir *háskóla-, iðnaðar- og nýsköpunarráðuneytið*.[30] Jafnframt gegna önnur ráðuneyti mikilvægu hlutverki í málaflokknum hvert vegna sinna málefnasviða, til dæmis:

[29] Hugtakið „neyðar- og öryggisfjarskipti“ er ekki skilgreint sérstaklega í lögum nr. 70/2022. Á hinn bóginn er hugtakið *neyðarþjónusta* skilgreint svo í 33. tölul. 5. gr. laganna: „Þjónusta sem er viðurkennd sem slík af stjórnvöldum, sem veitir aðstoð tafarlaust og hratt við aðstæður þar sem bein hætta steðjar að lífi eða limum einstaklinga, lýðheilsu eða almannaöryggi, eignum í einkaeigu eða eigu hins opinbera eða umhverfinu, í samræmi við landslög.“

[30] Miðað við árið 2024 þegar skýrsla þessi er rituð.

- *Dómsmálaráðuneytið*, vegna almannavarna og löggæslu, og CER-tilskipunar ESB sem til stendur að innleiða í íslenskan rétt.[31]
- *Fjármála- og efnahagsráðuneytið*, vegna Stafræns Íslands og Umbru, þjónustumiðstöðvar Stjórnarráðsins, og DORA-gerða ESB um netöryggi fjármálakerfisins sem verða innleiddar í íslenskan rétt.[32]
- *Forsætisráðuneytið*, vegna þjóðaröryggisráðs og almenns samhæfingarhlutverks.
- *Utanríkisráðuneytið*, vegna öryggis- og varnarmála.

Þá ber að nefna netöryggisráð sem hefur einkum það hlutverk að fylgja eftir framkvæmd stefnu stjórnvalda á sviði net- og upplýsingaöryggis, sem mörkuð er af ráðherra, sbr. 4. gr. laga nr. 78/2019 og nánari umfjöllun hér á eftir.

Ýmsar stofnanir ríkisins gegna jafnframt mikilvægu hlutverki á sviði netöryggismála. Má þar einkum nefna Fjarskiptastofu og netöryggissveit hennar, sem nánar verður fjallað um hér á eftir. Einnig má nefna önnur eftirlitsstjórnvöld samkvæmt lögum nr. 78/2019,[33] og löggæsluaðila, m.a. embætti ríkislögreglustjóra. Þá má nefna hlutverk Seðlabanka Íslands viðvíkjandi netöryggi fjármálakerfisins, sbr. fyrrnefndar DORA-gerðir ESB sem til stendur að innleiða í íslenskan rétt.

Sum áðurnefndra ráðuneyta og stofnana eru jafnframt tengiliðir við fjölþjóðlegar stofnanir sem sinna verkefnum á sviði netöryggis. Má þar nefna Netöryggisstofnun Evrópu, ENISA (háskóla-, iðnaðar- og nýsköpunarráðuneyti og Fjarskiptastofa),[34] Europol (dómsmálaráðuneyti og ríkislögreglustjóri) og NATO (utanríkisráðuneyti).

---

[31] Tilskipun ESB 2022/2557 frá 14. desember 2022 „on the resilience of critical entities and repealing Council Directive 2008/114/EC“. Í 1. gr. CER-tilskipunarinnar er m.a. gert ráð fyrir að hún og NIS2-tilskipunin skuli framkvæmdar með samræmdum hætti vegna tengsla milli þeirra, „[i]n light of the relationship between the physical security and cybersecurity of critical entities“.

[32] Reglugerð ESB 2022/2554 frá 14. desember 2022 „on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011“. Sjá einnig tengda breytingatilskipun ESB 2022/2556 frá 14. desember 2022. Í 1. gr. DORA-reglugerðarinnar er tekið af skarið um að efnisákvæði hennar teljist sérlög (e. sector-specific Union legal act) og gangi þar með framar efnisreglum NIS2-tilskipunarinnar að því er varðar aðila á fjármálamarkaði sem skilgreindir verða að landslögum á grundvelli NIS2 sem ómissandi eða mikilvægir (e. essential or important entities).

[33] Þ.e. Orkustofnun, Samgöngustofa, Seðlabanki Íslands, embætti landlæknis og Umhverfisstofnun, sbr. 1. mgr. 11. gr. laga nr. 78/2019.

[34] European Union Agency for Cybersecurity.

Þótt tiltekin stjórnvöld beri meginábyrgð á netöryggismálum, er netöryggi á endanum viðvarandi samvinnuverkefni stjórnkerfisins í heild sinni. Sérhver opinber aðili þarf að gæta að netöryggi í starfsemi sinni og gera viðeigandi ráðstafanir í því skyni, en þeir geta þar m.a. notið þjónustu Fjarskiptastofu og netöryggissveitar, sbr. nánari umfjöllun hér á eftir. Þá er framfylgd þjóðaröryggisstefnunnar, sem leggur m.a. áherslu á netöryggi og vernd mikilvægra innviða, í höndum Stjórnarráðs Íslands í heild sinni, þ.e. einstakra ráðuneyta innan viðkomandi málefnasviða, með eftirfylgni þjóðaröryggisráðs, sbr. samnefnd lög nr. 98/2016. Þessu til viðbótar ber að minnast á ábyrgð einstakra ráðuneyta, sveitarfélaga og undirstofnana á könnun áfallaþols og gerð hættumats og viðbragðsáætlana innan sviðsábyrgðar viðkomandi, í samstarfi við ríkislögreglustjóra, sbr. 15. og 16. gr. laga nr. 82/2008 um almannavarnir.[35]

Þótt netöryggi sé þverlægt verkefni stjórnsýslunnar í heild, eins og hér hefur verið rakið, verður sjónum hér í framhaldinu aðallega beint að þeim aðilum stjórnkerfisins sem bera meginábyrgð á netöryggismálum, þ.m.t. stefnumótun og samhæfingu í því sambandi. Þar er m.a. um að ræða háskóla-, iðnaðar- og nýsköpunarráðuneytið, netöryggisráð, Fjarskiptastofu og netöryggissveit hennar. Samhliða verður vikið að hlutverkum annarra stjórnvalda viðvíkjandi netöryggi þar sem við á.

3.2. Háskóla-, iðnaðar- og nýsköpunarráðuneytið

Eins og áður kom fram heyra netöryggi og fjarskipti stjórnarfarslega undir háskóla-, iðnaðar- og nýsköpunarráðuneytið.[36] Í 1. mgr. 4. gr. laga nr. 78/2019 er ráðherra falið að marka stefnu um net- og upplýsingaöryggi þar sem m.a. skal greina frá markmiðum og ráðstöfunum stjórnvalda í því skyni að stuðla að öryggi og viðnámsþrótti net- og upplýsingakerfa mikilvægra innviða. Ákvæðinu er ætlað að innleiða 7. gr. tilskipunar 2016/1148 (NIS) sem fjallar með ítarlegum hætti um landsbundnar stefnuáætlanir í þessum efnum (e. national strategy on the security of network and information systems). Eins og rakið er í skýringum við 4. gr. laga nr. 78/2019 gerir tilskipunin m.a. ráð fyrir

[35] Með sviðsábyrgðarreglu er átt við að sá aðili sem fer venjulega með stjórn tiltekins sviðs samfélagsins eða tiltekins svæðis eða umdæmis skuli skipuleggja viðbrögð og koma að stjórn aðgerða þegar hættu ber að garði. Sjá umfjöllun í greinargerð með frumvarpi til laga nr. 82/2008 um almannavarnir (lögþ. 2007-2008, þskj. 204 - 190. mál).
[36] Miðað við árið 2024 þegar skýrsla þessi er rituð.

að við stefnumörkun um net- og upplýsingaöryggi skuli markmið skilgreind og þeim forgangsraðað á hverjum tíma; að hlutverk og ábyrgð ólíkra stjórnsýslustofnana með snertifleti við málaflokkinn séu útlistuð skilmerkilega og að aðferðafræði við áhættumat í því skyni að draga fram stöðumynd liggi fyrir á hverjum tíma. Þá skal t.d. sérstaklega vikið að atriðum á borð við menntun, þjálfun og hvernig standa beri að vitundarvakningu í samfélaginu gagnvart netógnum.[37]

Í 1. mgr. 4. gr. laga nr. 78/2019 er ráðgert að netöryggisstefnan skuli endurskoðuð reglubundið og hefur verið miðað við að það skuli gert á þriggja ára fresti þótt sá árafjöldi sé ekki beinlínis nefndur í fyrrnefndu lagaákvæði. Gildandi netöryggisstefna Íslands tekur til tímabilsins 2022-2037, en hún var upphaflega samþykkt af samgöngu- og sveitarstjórnarráðherra í nóvember 2021. Við tilfærslu málaflokks netöryggis til ráðuneytis háskóla, iðnaðar og nýsköpunar í febrúar 2022, var stefnan gefin út að nýju.[38] Netöryggisstefnan er jafnframt hluti af fjarskiptaáætlun stjórnvalda. Netöryggi kemur einnig við sögu í fleiri opinberum stefnum, t.d. þjóðaröryggisstefnunni sem vikið var að í inngangi.

Lykilviðfangsefni netöryggisstefnunnar snúa að hæfni og getu á sviði netöryggis með því að efla vitund, menntun, rannsóknir og þróun. Meðal annars þurfi að efla getu stjórnvalda og atvinnulífs til að sporna við netárásum og lágmarka skaða þeirra, með stuðningi í innlendri og alþjóðlegri þekkingu. Jafnframt þurfi að efla lagaumhverfi og löggæslu innanlands og yfir landamæri til samræmis við alþjóðlegar kröfur og viðmið. Einkum þurfi að huga að vernd barna á Netinu, auk þess að skýra hvernig brugðist skuli við net- og upplýsingaáskorunum tengdum öryggis- og varnamálum. Þá þurfi að styrkja og formgera samstarf innan stjórnkerfisins og við atvinnulífið, þar sem hlutverka-skipting og ábyrgð sé skýr. Enn fremur þurfi að tryggja samhæfingu opinberra aðgerðaraðila vegna netöryggis.[39] Í stefnunni eru sett fram markmið og framtíðarsýn sem lúta m.a. að framangreindum atriðum.[40] Þá leggur stefnan grunnur að frekari aðgerðum á sviði netöryggismála en slík aðgerðaáætlun var kynnt í nóvember 2022.

[37] Athugasemdir við 4. gr. í greinargerð með lögum nr. 78/2019.
[38] *Netöryggisstefna Íslands 2022-2037*, bls. 4.
[39] *Netöryggisstefna Íslands 2022-2037*, bls. 6.
[40] *Netöryggisstefna Íslands 2022-2037*, bls. 9-16.

3.3. Netöryggisráð

Ráðherra skipar netöryggisráð sem starfar samkvæmt ákvæðum laga nr. 78/2019. Um netöryggisráð er fjallað í 2. mgr. 4. gr. laganna. Í ákvæðinu kemur fram að hlutverk netöryggisráðs sé einkum að fylgja eftir framkvæmd stefnu stjórnvalda á sviði net- og upplýsingaöryggis. Þá leggur netöryggisráð mat á stöðu netöryggis á Íslandi á hverjum tíma og er vettvangur upplýsingamiðlunar og samhæfingar, sbr. einnig umfjöllun um netöryggissveit o.fl. hér á eftir. Fulltrúar sem skipaðir eru í netöryggisráð skulu hafa viðeigandi menntun og/eða reynslu á þeim sviðum sem máli skipta. Með því er áréttað mikilvægi þess að tryggja hlutlausa og greinargóða umfjöllun um málefni ráðsins enda er því ætlað veigamikið hlutverk í netöryggismálum.[41] Netöryggisráði er jafnframt heimilt að skipa vinnuhópa til mats eða rannsóknar á afmörkuðum þáttum tengdum net- og upplýsingaöryggi, m.a. með aðstoð utanaðkomandi sérfræðinga.[42]

Fundir netöryggisráðs skulu haldnir fyrir luktum dyrum og getur ráðið ákveðið að trúnaður ríki um fundi þess eða einstök mál á dagskrá fundar, svo og gögn og afrakstur vinnu í smærri hópum fyrir ráðið. Þessi tilhögun er rökstudd með vísan til sjónarmiða um þjóðaröryggi og þess að um viðkvæmar upplýsingar kann að vera að ræða.[43] Ofangreindar trúnaðarreglur takmarka rétt til aðgangs að gögnum samkvæmt upplýsingalögum nr. 140/2012.

Netöryggisráð var upphaflega skipað 2015 til að fylgja eftir stefnu stjórnvalda um net- og upplýsingaöryggi, sem sett var sama ár og hafði að geyma framtíðarsýn til ársins 2026. Netöryggisráð hefur á undanförnum árum verið skipað fulltrúum háskóla-, iðnaðar- og nýsköpunarráðuneytis, dómsmálaráðuneytis, fjármála- og efnahagsráðuneytis, utanríkisráðuneytis, menningar- og viðskiptaráðuneytis, landlæknis, Seðlabanka

[41] Við þinglega meðferð frumvarps til laga nr. 78/2019 kom fram gagnrýni á að ekki kæmi fram í ákvæðinu hvaða aðilar skyldu tilnefna í ráðið. Þá kom jafnframt fram að hvergi væri fjallað um hvaða kröfur væru gerðar til hæfni þeirra aðila sem skipaðir væru í ráðið. Þó var talið rétt að tilgreina ekki tilnefningaraðila í ákvæðinu enda væri net- og upplýsingaöryggi síbreytilegur málaflokkur sem snerti mörg ráðuneyti og stofnanir sem og atvinnulífið almennt. Þannig gæti orðið ástæða til þess síðar að hafa aðra eða fleiri aðila í netöryggisráði en þá sem sitja nú í því. Álit umhverfis- og samgöngunefndar um frumvarp til laga nr. 78/2019 (149. lögþ. 2018–2019 - þskj. 1699 - 416. mál).

[42] Athugasemdir við 4. gr í greinargerð með frumvarpi til laga nr. 78/2019 (149. lögþ. 2018-2019, þskj. 557 – 416. mál).

[43] Athugasemdir við 4. gr. í greinargerð með frumvarpi til laga nr. 78/2019 (149. lögþ. 2018-2019, þskj. 557 – 416. mál).

Íslands, Fjarskiptastofu, ríkislögreglustjóra og Persónuverndar. Í 2. mgr. 4. gr. laga nr. 78/2019 er ráðherra veitt heimild til að setja nánari ákvæði um netöryggisráð í reglugerð, en unnið er að samningu slíkrar reglugerðar. Þá er ráðgert í fyrrnefndu ákvæði að netöryggisráð setji sér starfsreglur.

Í ákvæðum laga nr. 78/2019 og reglugerðar nr. 480/2021 er að finna ýmis ákvæði um upplýsingagjöf netöryggissveitar Fjarskiptastofu til netöryggisráðs, sem fjallað verður um hér í framhaldinu.

3.4. Fjarskiptastofa

Áður hefur verið vikið að eftirlits- og samhæfingarhlutverki Fjarskiptastofu samkvæmt lögum nr. 78/2019 og lögum nr. 70/2022. Fjarskiptastofa er sjálfstæð stofnun sem heyrir stjórnarfarslega undir háskóla-, iðnaðar- og nýsköpunarráðherra, sbr. 1. gr. laga nr. 75/2021. Hlutverk hennar lýtur m.a. að stjórnsýslu og eftirliti með framkvæmd fjarskipta- og netöryggismála, auk þess að stuðla að öryggi almennings, fyrirtækja og samfélagsins alls á sviði fjarskipta og netöryggis, sbr. nánar 2. og 3. gr. laganna. Skal þar sérstök áhersla lögð á þjónustu við samfélagið, almenning og fyrirtæki, og við-bragðsgetu netöryggissveitar sem starfar á vegum Fjarskiptastofu, en nánar verður fjallað um netöryggissveitina hér á eftir.

Skipulag Fjarskiptastofu byggir á fjórum fagsviðum, þar af eru tvö sem sinna eingöngu netöryggismálum, þ.e. svið stafræns öryggis og netöryggissveitin. Um netöryggisveitina verður fjallað nánar hér á eftir. Fjarskiptainnviðasvið stofnunarinnar fer einnig með mál er snúa að netöryggi svo sem áfallaþol fjarskiptaneta og almannavarnir. Svið stafræns öryggis hefur hins vegar með höndum hlutverk Fjarskiptastofu sem samhæfingar-stjórnvalds og eftirlitsstjórnvalds samkvæmt lögum nr. 78/2019 og eftirlitshlutverk Fjarskiptastofu gagnvart netöryggiskröfum laga nr. 70/2022 um fjarskipti. Starfsmenn stafræns öryggis, og hluti af starfsmönnum fjarskiptainnviðasviðs, eru með öryggis-vottun skv. 24. gr. varnarmálalaga nr. 34/2008, sbr. 3. mgr. 9. gr. laga nr. 75/2021 og eru starfsstöðvar stafræns öryggis aðgreindar frá öðrum starfsstöðvum Fjarskiptastofu. Svið stafræns öryggis sinnir fyrirbyggjandi eftirliti (ex ante) með netöryggiskröfum laga nr. 78/2019 og laga nr. 70/2022 og eftirfarandi eftirliti (ex post) t.d. í kjölfar tilkynningar til

netöryggisveitar um atvik. Þess skal geta að sérstök þagnarskylda hvílir á starfsfólki stafræns öryggis vegna upplýsinga sem aflað er frá eftirlitsskyldum aðilum, sbr. 19. gr. laga nr. 78/2019 og 5. mgr. 25. gr. laga nr. 75/2021. Einnig hefur sviðið með höndum stjórnsýslu með framkvæmd netöryggismála, svo sem hvað varðar leiðbeiningar til hagaðila og eftirlit á grundvelli laga nr. 55/2019 um rafræna auðkenningu og traust-þjónustur fyrir rafræn viðskipti og laga nr. 54/2021 um íslensk landshöfuðlén.

Fjarskiptastofa skal skv. 1. mgr. 8. gr. laga nr. 75/2021 stuðla að því að fjarskiptanet hér á landi byggist á „bestu framkvæmd og nýjustu stöðlum“ og „ávallt sé litið til áreiðanleika- og öryggissjónarmiða“, þ.m.t. við uppbyggingu nýrra fjarskiptainnviða. Í því sambandi skal Fjarskiptastofa stuðla að áreiðanlegum fjarskiptum með tilliti til almannavarna, neyðarfjarskipta og netöryggis, sbr. 2. mgr. 8. gr. laganna, en vikið verður nánar að þessu hlutverki Fjarskiptastofu hér síðar.

Vegna hlutverks Fjarskiptastofu m.a. á sviði netöryggis er henni heimilt að krefjast upplýsinga m.a. um eignarhald fjarskiptafyrirtækja, stjórnarmenn, framkvæmdastjóra og eftirlits- og stjórnkerfi innan fjarskiptafyrirtækis, sbr. 6. mgr. 15. gr. laga nr. 75/2021. Síðastnefnt ákvæði var lögfest með lögum nr. 17/2022. Þau breytingalög voru sett m.a. í tilefni af sölu fjarskiptainnviðafyrirtækisins Mílu ehf. til erlends aðila sem þá var fyrirhuguð og gekk síðan eftir.[44] Fjarskiptastofa mun hafa beitt ofangreindri lagaheimild til upplýsingaöflunar frá innlendum fjarskiptafyrirtækjum í erlendu eignarhaldi.

Til að bæta þekkingu á sviði netöryggismála er Fjarskiptastofu heimilt að taka þátt í rannsóknum og þróunarstarfi, þ.m.t. nýsköpunarverkefnum, auk þess að stuðla að fræðslu á þessu sviði, sbr. 1. og 2. mgr. 13. gr. laga nr. 75/2021. Liður í því er að stuðla að þróun upplýsingasamfélagsins og netöryggis með markvissri kynningu þróunar og viðmiða og innleiðingu nýrrar tækni og vinnubragða, sbr. d-lið 3. mgr. 13. gr. laganna. Á þessum grundvelli starfrækir Fjarskiptastofa vefsvæðið netoryggi.is sem hefur að geyma ýmsa fræðslu á sviði netöryggis. Í skýringum við 13. gr. er hvatt til þess að Fjarskiptastofa stuðli að fræðslu á sínu sviði og veiti t.d. starfsmönnum sínum svigrúm til að stunda m.a. kennslu í háskólum landsins, gerast leiðbeinendur við lokaritgerðir

[44] 152. lögþ. 2021–2022, 169. mál.

o.fl.[45] Samkvæmt 23. gr. laganna er Fjarskiptastofu enn fremur heimilt að hafa tekjur af sérhæfðri þjónustu og verksamningum, svo og af rannsóknastarfsemi og þróunarverkefnum, á starfssviðum sínum á borð við netöryggismál. Ákvæðinu er ætlað að auka getu stofnunarinnar til sinna verkefnum skv. 13. gr. laganna, sem áður var getið.[46]

Fjarskiptastofa skal hafa samvinnu og samráð við aðila, félög, samtök og stofnanir sem tengjast starfsemi hennar, sbr. 1. mgr. 26. gr. laga nr. 75/2021. Jafnframt tekur Fjarskiptastofa þátt í alþjóðlegu samstarfi og mótun alþjóðareglna á starfssviði sínu, þ.m.t. samstarfi við aðrar eftirlitsstofnanir á EES og Eftirlitsstofnun EFTA í samræmingu eftirlitshátta og túlkun löggjafar, sbr. nánar 27. gr. laganna.[47] Sjá einnig umfjöllun um netöryggissveit hér á eftir, varðandi samvinnu hennar við erlenda samstarfsaðila.

Þá er Fjarskiptastofu falið í 14. gr. laganna að vera ráðgefandi fyrir stjórnvöld um málefni sem varða fjarskipti, netöryggismál, tækniþróun á sviði fjarskipta og öryggi net- og upplýsingakerfa og hafa eftirlit með því að Ísland uppfylli þær skuldbindingar sem mælt er fyrir um í alþjóðlegum samningum á umræddum sviðum. Skal Fjarskiptastofa enn fremur gera tillögur til ráðherra um nauðsynlegar breytingar á lögum og reglugerðum ef þess gerist þörf.

Í 2. mgr. 8. gr. laga nr. 75/2021 er vísað til þess að Fjarskiptastofa skuli stuðla að áreiðanlegum fjarskiptum út frá hagsmunum almannavarna, neyðarfjarskipta og netöryggis og skal vera ráðgefandi aðili fyrir yfirvöld þegar almannavarnaástand er yfirvofandi, það stendur yfir og er afstaðið.[48] Jafnframt skal Fjarskiptastofa stuðla að öryggi og viðnámsþrótti fjarskiptainnviða, almanna- og þjóðaröryggi og samhæfðum viðbrögðum við sérstakar aðstæður, eftir atvikum með fyrirmælum um ráðstafanir samkvæmt XII. kafla laga nr. 70/2022.[49] Þegar almannavarnaástandi hefur verið lýst yfir

[45] 151. lögþ. 2020–2021, þskj. 852 — 506. mál.
[46] 151. lögþ. 2020–2021, þskj. 852 — 506. mál.
[47] Um heimildir Fjarskiptastofu til upplýsingamiðlunar til ákveðinna erlendra samstarfsaðila, og vinnslu upplýsinga í því sambandi, má benda á 4.-7. mgr. 25. gr. laga nr. 75/2021, sbr. einnig 20. og 21. gr. laga nr. 78/2019 og 29.-31. gr. reglugerðar nr. 480/2021.
[48] Í kjölfar breytinga á lögum nr. 82/2008 um almannavarnir með lögum nr. 39/2022, vísar hugtakið almannavarnaástand nú til almannavarnastigs, sbr. 2. gr. a laganna, sbr. einnig 2. mgr. 5. gr.
[49] Í 2. mgr. 8. gr. laga nr. 75/2021 er vísað til fyrirmæla um ráðstafanir skv. 4. eða 5. mgr. 47. gr. laga nr. 81/2003 um fjarskipti, en nú gilda lög nr. 70/2022 um það efni.

getur Fjarskiptastofa enn fremur gefið fjarskiptafyrirtækjum fyrirmæli um aðgerðir til að tryggja fjarskiptasamband á tilteknu svæði, svo sem að opnað skuli fyrir reiki-þjónustu, sbr. 3. mgr. 8. gr. laga nr. 75/2021. Sjá einnig síðari umfjöllun um samstarf Fjarskiptastofu, þ.m.t. netöryggissveitar, við ríkislögreglustjóra vegna almannavarna.

Að öðru leyti má vísa til umfjöllunar um verkefni Fjarskiptastofu í 2. kafla, svo og til umfjöllunar um netöryggissveit hér á eftir.

3.5. Netöryggissveit Fjarskiptastofu

3.5.1. Almenn atriði

Netöryggissveit Fjarskiptastofu er landsbundið öryggis- og viðbragðsteymi vegna atvika og áhættu sem varða net- og upplýsingaöryggi, ógnir, hættur og atvik á netinu hér á landi og gegnir hlutverki CSIRT-teymis[50] fyrir Ísland, sbr. 1. mgr. 9. gr. laga nr. 75/2021, sbr. einnig 9. gr. tilskipunar 2016/1148 (NIS).[51] Ákvæði um netöryggissveit (CERT-IS) er að finna m.a. í lögum nr. 78/2019, 75/2021 og 70/2022, auk reglugerðar nr. 480/2021.[52]

Gildandi lagafyrirmæli um netöryggissveit fela að stofni til í sér innleiðingu á tilskipun 2016/1148 (NIS) en eiga sér þó lengri sögu. Í áhættumatsskýrslu 2009 var t.a.m. bent á mikilvægi þess „að setja á stofn viðbragðsteymi hér á landi til að auka netöryggi eins og gert hefur verið víða erlendis. Það mundi ekki aðeins gegna mikilvægu samræmingar-hlutverki, heldur einnig skilgreina og upplýsa um hættur.“[53] Fyrstu lagaákvæðin um netöryggissveit voru lögfest með lögum nr. 62/2012, og voru staðsett í þágildandi lögum nr. 81/2003 um fjarskipti. Þar var vísað til öryggis- og viðbragðshóps til verndar ómissandi upplýsingainnviðum gegn netárásum, sem nefndist CERT-ÍS (Computer

[50] Netöryggissveitir erlendis eru ýmist nefndar *CSIRT* (computer security incident response team), *CERT* (computer emergency response/readiness team) eða *CIRT* (computer/cybersecurity incident response team).
[51] Sjá einnig 1. mgr. 14. gr. laga nr. 78/2019 og 6. gr. reglugerðar nr. 480/2021, sbr. jafnframt m.a. 82. gr. laga nr. 70/2022. Í 4. tölul. 3. gr. reglugerðar nr. 480/2021 er *CERT- eða CSIRT-teymi* skilgreint svo: „Alþjóðleg heiti yfir öryggis- og viðbragðsteymi á sviði net- og upplýsingaöryggis, eða netöryggissveit (e. computer emergency response team eða computer security and incident response team).“
[52] Reglugerð nr. 480/2021 um netöryggissveit Póst- og fjarskiptastofnunar (CERT-ÍS). Efni reglugerðar nr. 480/2021 hefur ekki verið breytt eftir gildistöku laga nr. 75/2021 um Fjarskiptastofu og laga nr. 70/2022 um fjarskipti, og geymir reglugerðin því enn tilvísanir til eldri fjarskiptalaga og eldra heitis Fjarskiptastofu, Póst- og fjarskiptastofnunar. Forveri reglugerðarinnar er reglugerð nr. 475/2013 um málefni CERT-ÍS netöryggissveitar.
[53] *Áhættumatsskýrsla fyrir Ísland – hnattrænir, samfélagslegir og hernaðarlegir þættir*, bls. 20.

Emergency Response Team). Í skýringum með breytingalögunum var rakið að hópurinn væri „nokkurs konar alþjóðlegt tengslanet og samráðs- og samvinnuvettvangur fyrir vernd gegn öryggisatvikum í upplýsingainnviðum“.[54] Gildandi ákvæði um netöryggissveit er nú að finna í þeim lagabálkum og reglugerð sem nefnd voru hér að framan.

Samkvæmt 2. mgr. 9. gr. laga nr. 75/2021 er hlutverk netöryggissveitar að fyrirbyggja og draga úr hættu á netárásum og öðrum öryggisatvikum í netumdæmi Íslands, auk þess að koma í veg fyrir og lágmarka tjón á fjarskiptamarkaði og mikilvægum innviðum í skilningi laga nr. 78/2019.[55] Í því sambandi leitast netöryggissveit við að greina ógnir og atvik á frumstigi í netumdæmi Íslands, fyrirbyggja og takmarka útbreiðslu þeirra og tjón sem af þeim kann að hljótast. Netöryggissveit skal m.a., með fyrirbyggjandi hætti, stuðla að bættu netöryggi m.a. með ráðgjöf, upplýsingamiðlun, útgáfu leiðbeininga og tilkynninga og, ef við á, tilmælum um ákveðnar aðgerðir vegna atvika og áhættu, sbr. 3. mgr. 6. gr. reglugerðar nr. 480/2021. Þá skal netöryggissveit samhæfa viðbrögð aðila við ógnum og atvikum, m.a. í samstarfi við ríkislögreglustjóra þegar við á, sbr. 2. mgr. 9. gr. laga nr. 75/2021, sem og styðja við skjót, markviss og samhæfð viðbrögð gegn aðsteðjandi ógnum, áhættu og atvikum, sbr. 2. gr. reglugerðar nr. 480/2021 og nánari umfjöllun hér á eftir. Verkefni netöryggissveitar skulu ávallt unnin með það að markmiði að samræma og hámarka árangur aðgerða til verndar netumdæmis Íslands, sbr. 4. mgr. 6. gr. reglugerðarinnar.

Af framansögðu leiðir að hlutverk netöryggissveitar er bæði fólgið í fyrirbyggjandi aðgerðum gegn mögulegum netógnum, sem og viðbrögðum við ógnum sem hafa raungerst. Hlutverk netöryggissveitar er skilgreint með víðtækum hætti í áðurnefndum lögum og reglugerð nr. 480/2021. Hlutverk sveitarinnar er t.a.m. ekki einskorðað við varnir gegn netógnum sem steðja að net- og upplýsingakerfum er falla undir gildissvið laga nr. 78/2019, heldur nær hlutverk sveitarinnar yfir „ógnir, hættur og atvik á netinu“,

[54] Athugasemdir við 8. gr. í greinargerð með frumvarpi til laga nr. 62/2012 (140. lögþ. 2011-2012, þskj. 438 – 362. mál).
[55] Í 8. tölul. 3. gr. reglugerðar nr. 480/2021 er *netumdæmi Íslands* skilgreint svo: „Sjálfstæð eða eftir atvikum samtengd net- og upplýsingakerfi sem falla innan þeirra raða IP-vistfanga sem úthlutað hefur verið hér á landi og ásamt lénum sem skráð eru undir íslensku landshöfuðléni.“

þ.e.a.s. í netumdæmi Íslands, sbr. 1. mgr. 9. gr. laga nr. 75/2021, sbr. einnig 1. mgr. 6. gr. reglugerðar nr. 480/2021.

Netöryggissveit er tengiliður íslenskra stjórnvalda í alþjóðlegu samstarfi CSIRT-teyma, sbr. 1. mgr. 9. gr. laga nr. 75/2021. Í 1. mgr. 6. gr. reglugerðar nr. 480/2021 segir að slíkt samstarf taki einkum til miðlunar og móttöku upplýsinga er varða áhættu, atvik, varnir og viðbúnað vegna mögulegra ógna. Netöryggissveit taki jafnframt þátt í öðru samstarfi á sviði netöryggismála, innan og utan þjónustuhópa sinna, við CSIRT-sveitir, CERT-teymi eða aðra aðila sem vinna að netöryggismálum.

Í 1. mgr. 19. gr. reglugerðar nr. 480/2021 er ráðgert að netöryggissveit birti árlega á vef sínum skýrslu um starfsemi sína sem hefur að geyma tölfræðilega samantekt og almenna umfjöllun um starfsemi hvers árs. Efnistök skýrslunnar skulu miðast við birtingu á opinberum vettvangi. Skýrslan skal jafnframt kynnt fyrir þjónustuhópum sveitarinnar og netöryggisráði.

3.5.2. Skipulag og starfslið netöryggissveitar

Netöryggissveit er starfrækt sem sérstök eining (deild) innan Fjarskiptastofu og ber forstjóri stofnunarinnar ábyrgð á starfsemi og innra skipulagi sveitarinnar. Engu að síður er netöryggissveit skipulagslega aðgreind frá eftirlitshlutverki Fjarskiptastofu á sviði net- og upplýsingaöryggis, sbr. nánar 4. gr. reglugerðar nr. 480/2021. Netöryggissveit telst því sem slík ekki til eftirlitsstjórnvalds í skilningi laga nr. 78/2019, þótt Fjarskiptastofa gegni því hlutverki sem fyrr segir.

Fjallað er um starfslið netöryggissveitar í 5. gr. reglugerðar nr. 480/2021. Fimmtán starfsmenn starfa hjá netöryggissveit. Forstjóri Fjarskiptastofu veitir aðgangsheimildir að starfssvæði netöryggissveitar og er þeim einum heimill aðgangur á því sem þangað á lögmætt erindi og hefur gilda aðgangsheimild, sbr. 4. og 5. mgr. 9. gr. laga nr. 75/2021. Í 3. mgr. sama lagaákvæðis er jafnframt ráðgert að starfslið netöryggissveitar skuli uppfylla skilyrði öryggisvottunar skv. 24. gr. varnarmálalaga nr. 34/2008. Hið sama gildir um annað starfslið sem kemur að netöryggismálum hjá Fjarskiptastofu og ráðuneytinu. Sé utanaðkomandi aðila falið afmarkað verkefni hjá netöryggissveit er gerð krafa um sakavottorð og trúnaðaryfirlýsingu, sbr. 3. mgr. 5. gr. reglugerðar nr. 480/2021,

og skal meta hverju sinni hvort einnig skuli gera kröfu um öryggisvottun. Í 3. mgr. 4. gr. reglugerðarinnar er netöryggissveit jafnframt falið það verkefni móta og innleiða stefnu um öryggi starfssvæðis sveitarinnar, m.a. öryggi búnaðar og kerfa, að öðru leyti en mælt er fyrir um í lögum og reglugerðinni.

3.5.3. Stöðumyndir vegna netógna, almenn ástandsvitund, o.fl.

Það er sem fyrr segir meðal hlutverka netöryggissveitar að greina ógnir og atvik á frumstigi í netumdæmi Íslands, fyrirbyggja og takmarka útbreiðslu þeirra og tjón sem af þeim kann að hljótast, sbr. 2. mgr. 9. gr. laga nr. 75/2021. Í því sambandi skal netöryggissveit m.a. móta stöðumynd vegna netógna, sbr. 6. mgr. 14. gr. laga nr. 78/2019 og 2. mgr. 7. gr. reglugerðar nr. 480/2021. Slík stöðumynd felur í sér heildstætt mat á stöðu og þróun netöryggismála á ákveðnu tímabili í netumdæmi Íslands eða afmarkaðra samhengi, t.d. ólíkra þjónustuhópa netöryggissveitar, og byggir á öflun og úrvinnslu tiltækra upplýsinga og gagna, sbr. 10. tölul. 3. gr. reglugerðarinnar. Samkvæmt 2. mgr. 7. gr. reglugerðarinnar skal netöryggissveit skjalfesta og miðla stöðumyndinni til netöryggisráðs a.m.k. árlega, en í 6. mgr. 14. gr. laga nr. 78/2019 segir að stöðumati skuli reglubundið miðlað til netöryggisráðs í samræmi við óskir þess. Enn fremur skal netöryggissveit leitast við að upplýsa eftirlitsstjórnvöld reglulega um stöðumyndina, eftir atvikum að því er tiltekna þjónustuhópa varðar, sbr. 2. mgr. 7. gr. reglugerðarinnar. Með þjónustuhópum netöryggissveitar er átt við aðila sem lögum samkvæmt njóta þjónustu netöryggissveitar, þ.e. mikilvægir innviðir, fjarskiptafyrirtæki, Stjórnarráð Íslands og eftir atvikum aðrir aðilar.[56] Með samstarfsaðilum netöryggissveitar er átt við aðila utan þjónustuhópa sveitarinnar sem eru í samskiptum við sveitina vegna öryggis net- og upplýsingakerfa.[57]

Netöryggissveit leitast við að skapa „viðeigandi almenna ástandsvitund“ um ógnir, áhættu og atvik innan netumdæmis Íslands, sbr. 1. mgr. 7. gr. og 2. gr. reglugerðar nr. 480/2021. Jafnframt skal netöryggisráð árlega birta skýrslu með tölfræðilegri samantekt og almennri umfjöllun um starfsemi hvers árs á vef sveitarinnar og skal hún kynna

[56] Sjá 9. tölul. 3. gr. reglugerðar nr. 480/2021. Sjá einnig 24.-26. gr. reglugerðarinnar (tilhögun þjónustu netöryggissveitar við opinberar stofnanir, Stjórnarráð Íslands og þriðju aðila).
[57] Sjá 11. tölul. 3. gr. reglugerðar nr. 480/2021.

skýrsluna fyrir þjónustuhópum sínum og netöryggisráði, sbr. 19. gr. reglugerðarinnar.[58] Að öðru leyti forgangsraðar netöryggissveit og skipuleggur fyrirbyggjandi aðgerðir og samstarf við og innan þjónustuhópa sveitarinnar o.fl. í því skyni að sporna við áhættu og atvikum sem ógna öryggi net- og upplýsingakerfa, sbr. 3. mgr. 7. gr. reglugerðar nr. 480/2021. Slíkar fyrirbyggjandi aðgerðir skulu m.a. taka mið af stöðumynd vegna netógna og almennri ástandsvitund, sem áður var vikið að.

3.5.4. Viðbrögð netöryggissveitar við netógnum

a) Tilkynningar til netöryggissveitar

Netöryggissveit gegnir mikilvægu hlutverki við að bregðast við ógnum við netöryggi og samhæfa aðgerðir ólíkra hagaðila og stjórnvalda í því sambandi. Þar hafa reglur um tilkynningarskyldu til netöryggissveitar lykilþýðingu. Mikilvægum innviðum er skylt að tilkynna netöryggissveit um alvarleg atvik eða áhættu sem ógnar öryggi net- og upplýsingakerfa þeirra svo fljótt sem verða má, sbr. 1. mgr. 8. gr. laga nr. 78/2019.[59] Hliðstæð tilkynningarskylda hvílir á fjarskiptafyrirtækjum vegna alvarlegra öryggisatvika sem ógna öryggi eða virkni almennra fjarskiptaneta eða almennrar fjarskiptaþjónustu, sbr. 1. mgr. 80. gr. laga nr. 70/2022. Í 2. mgr. beggja ofangreindra lagaákvæða eru tilgreind atriði sem litið skal til við mat á alvarleika atviks, þ.m.t. fjölda notenda þjónustunnar sem atvik hefur áhrif á; hversu lengi atvik stendur yfir; landfræðilegrar útbreiðslu og umfangs áhrifa atviks; og mögulegra áhrifa atviks á aðra mikilvæga innviði eða efnahagslega og samfélagslega starfsemi eða stafræna þjónustu.[60] Þá skal ef við á upplýst um mögulegt útvistunarfyrirkomulag og hugsanleg smitáhrif, jafnvel yfir landamæri, en umfang tilkynningar ræðst að öðru leyti af efni og aðstæðum, sbr. 3. mgr. 8. gr. laga nr. 78/2019 og 4. mgr. 80. gr. laga nr. 70/2022.

Hver sem er getur sent inn tilkynningu til netöryggissveitar vegna atviks eða ógnar viðvíkjandi netöryggi, sbr. 1. mgr. 8. gr. reglugerðar nr. 480/2021 og 1. og 2. mgr. 15.

[58] Sjá t.d. ársyfirlit CERT-IS 2022.
[59] Sjá nánar vefsvæði netöryggissveita - https://www.cert.is/ - þar sem finna má leiðbeiningar og eyðublöð vegna tilkynninga til sveitarinnar, sbr. einnig 3. mgr. 8. gr. reglugerðar nr. 480/2021.
[60] Að því er varðar tilkynningar samkvæmt lögum nr. 78/2019 má einnig vísa til nánari sjónarmiða í reglugerð nr. 866/2020 (rekstraraðilar nauðsynlegrar þjónustu, sjá nánar 25. gr.) og reglugerð nr. 1255/2020 (veitendur stafrænnar þjónustu, sjá nánar 18. gr.).

gr. laga nr. 78/2019. Bein lagaskylda til þess hvílir hins vegar aðeins á mikilvægum innviðum og fjarskiptafyrirtækjum samkvæmt ofangreindum ákvæðum, sem fyrr segir, og nefnast tilkynningar frá þessum aðilum *skyldutilkynningar*.[61] Netöryggissveit hefur heimild til að forgangsraða þannig að brugðist sé við skyldutilkynningum og tilkynningum frá öðrum aðilum í þjónustuhópum sveitarinnar áður en brugðist er við tilkynningum eða upplýsingum frá öðrum, sbr. 1. mgr. 8. gr. reglugerðar nr. 480/2021, sbr. einnig 3. mgr. 15. gr. laga nr. 78/2019. Undir þjónustuhópa netöryggissveitar falla, auk mikilvægra innviða og fjarskiptafyrirtækja, Stjórnarráð Íslands og aðrar opinberar stofnanir, eins og áður var rakið. Í 3. mgr. 16. gr. laga nr. 78/2019 segir jafnframt að Fjarskiptastofa skuli vekja athygli opinberra stofnana á ákvæðum um tilkynningar um atvik og viðbrögð við þeim. Það athugast þó að tilkynningarskylda til netöryggissveitar hvílir, sem fyrr segir, eingöngu á mikilvægum innviðum og fjarskiptafyrirtækjum.[62]

Í tengslum við umfjöllun þessa kafla, um tilkynningar til netöryggissveitar, má vekja aftur athygli á sérstakri tilkynningarskyldu *fjarskiptafyrirtækja* til *Fjarskiptastofu* um það ef hætta er á að öryggi eða leynd upplýsinga á fjarskiptanetum verði rofin eða ef til rofs hefur komið, sbr. 3. mgr. 80. gr. laga nr. 70/2022, sbr. einnig fyrri umfjöllun.

b) Viðbrögð – samhæfing, ráðgjöf og upplýsingamiðlun vegna netógnar

Netöryggissveit gegnir mikilvægu samhæfingarhlutverki vegna netógna sem upp koma hjá þjónustuhópum sveitarinnar og innan netumdæmis Íslands, sbr. 9. gr. reglugerðar nr. 480/2021. Viðbragð netöryggissveitar við netógn getur ýmist verið virkjað í kjölfar tilkynningar til sveitarinnar, sem áður var lýst, eða þegar sveitinni berst vitneskja um atvik eða ógn með öðrum hætti. Skal ávallt leitast við að ná sem bestum tökum á aðstæðum svo takmarka megi mögulegt tjón, sbr. 9. gr. reglugerðarinnar, sbr. einnig 1. mgr. 6. gr. hennar.[63]

[61] https://www.cert.is – Leiðbeiningar í atvikum – Skyldutilkynningar.
[62] Í 27. gr. laga nr. 78/2019 er að finna reglu þess efnis að tilkynning um atvik til netöryggissveitar skuli ekki hafa áhrif á eða auka mögulega bótaskyldu vegna atviksins.

[63] Sjá einnig 2. mgr. 9. gr. laga nr. 75/2021, 4. mgr. 14. gr. laga nr. 78/2019 og 2. mgr. 82. gr. laga nr. 70/2022.

Í 1. mgr. 8. gr. reglugerðar nr. 480/2021 er fjallað um meðhöndlun áhættu og atvika.[64] Þar segir að netöryggissveit skuli bregðast við tilkynningum um atvik samkvæmt lögum nr. 78/2019 og lögum nr. 70/2022 með því að veita viðeigandi upplýsingar eða ráðgjöf um viðbrögð og aðgerðir, eftir því sem tilefni og nauðsyn ber til, í því skyni að styðja við skilvirka meðhöndlun atviks, sbr. einnig 2. mgr. 14. gr. laga nr. 78/2019. Skal netöryggissveit leitast við að fyrirbyggja að atvik breiðist út og valdi tjóni, eftir atvikum í samstarfi við ríkislögreglustjóra, sbr. 4. mgr. 14. gr. laga nr. 78/2019. Við útbreitt öryggisatvik samhæfir netöryggissveitin aðgerðir viðeigandi aðila gegn aðsteðjandi hættu til að lágmarka tjón og reisa við eða lagfæra óvirk kerfi, sbr. 1. mgr. 82. gr. laga nr. 70/2022. Í þessu skyni getur netöryggissveit einnig beint tilmælum um aðgerðir til mikilvægra innviða og fjarskiptafyrirtækja, sbr. umfjöllun hér á eftir.

Í 9. gr. reglugerðar nr. 480/2021 kemur fram að netöryggissveit sé heimilt við samhæfingu aðgerða að miðla viðeigandi gögnum og upplýsingum til þriðju aðila ef slík miðlun er nauðsynleg til að lágmarka tjón og/eða tryggja öryggi net- og upplýsinga-kerfa.[65] Um meðferð gagna og upplýsinga í starfsemi sveitarinnar fer samkvæmt 29. gr. reglugerðarinnar, og um miðlun og aðra vinnslu persónuupplýsinga fer samkvæmt ákvæðum VII. kafla reglugerðarinnar. Einnig fer um upplýsingamiðlun eftir ákvæðum V. kafla laga nr. 78/2019 þar sem við á. Þegar miðlað er upplýsingum sem háðar eru þagnarskyldu, skal þagnarskyldan ríkja áfram um viðkomandi upplýsingar og skal m.a. gætt trúnaðar um öryggis- og viðskiptahagsmuni mikilvægra innviða þar sem við á, sbr. 3. mgr. 20. gr. laga nr. 78/2019. Þá skal netöryggissveit eftir fremsta megni reyna að tryggja framfylgni við skilgreint trúnaðarstig og öryggi gagna sem miðlað er til samstarfsaðila, sbr. 40. mgr. 20. gr. reglugerðarinnar.

Í 1. mgr. 9. gr. laga nr. 78/2019 er ráðgert að netöryggissveit skuli tryggja að upplýsingar um atvik skv. 8. gr. laganna séu aðgengilegar viðkomandi *eftirlitsstjórnvöldum* án tafar,

[64] Í 12. tölul. 6. gr. laga nr. 78/2019 er meðhöndlun atvika skilgreind sem allt það verklag sem styður við að koma upp um, greina og afmarka atvik og viðbrögð við þeim.
[65] Í 4. mgr. 82. gr. laga nr. 70/2022 er ráðgert að netöryggissveit skuli tilkynna og miðla upplýsingum til „viðeigandi hagsmunaaðila“ um ógnir og öryggisatvik. Í lögskýringargögnum er ekki að finna sérstakar skýringar á tilvitnuðu orðalagi, en líklega vísar það aðallega til þjónustuhópa netöryggissveitar og þeirra sem netógn beinist að.

sbr. einnig 5. mgr. 80. gr. laga nr. 70/2022.[66] Það þýðir að slík tilkynning getur leitt til rannsóknar á atvikum og hvort lög hafi verið brotin í tengslum við þau, sem svo getur leitt til fyrirmæla og/eða viðurlaga til að stuðla að því að brot endurtaki sig ekki. Um eftirlitsstjórnvöld samkvæmt lögum nr. 78/2019 vísast til 11. gr. þeirra laga og fyrri umfjöllunar um ákvæði þeirra laga, og um eftirlit Fjarskiptastofu með netöryggiskröfum laga nr. 70/2022 um fjarskipti vísast jafnframt til fyrri umfjöllunar.

Netöryggissveit skal einnig tilkynna *þjónustuhópum* sínum um þekkta ógn, áhættu eða atvik og styðja við hópana með leiðbeiningum um fyrirbyggjandi aðgerðir og upplýsingamiðlun, er miðar að því að draga úr ógn, áhættu og afleiðingum atvika, sbr. 1. og 2. mgr. 11. gr. reglugerðar nr. 480/2021. Fjarskiptafyrirtæki og mikilvægir innviðir skulu gera viðeigandi ráðstafanir til að vakta og móttaka upplýsingar sem berast frá netöryggissveit samkvæmt framansögðu, sbr. 3. mgr. síðastnefnds ákvæðis.[67]

Þá skal netöryggissveit leitast við að upplýsa *netöryggisráð* um alvarleg og/eða útbreidd atvik eða áhættu sem ógna öryggi net- og upplýsingakerfa og tengjast þjónustuhópum sveitarinnar eða, ef við á, netumdæmi Íslands almennt, eins og við á hverju sinni, sbr. 1. mgr. 15. gr. reglugerðar nr. 480/2021. Enn fremur er netöryggissveit skylt skv. 2. mgr. sama ákvæðis að upplýsa netöryggisráð um yfirvofandi atvik og áhættu sem sveitin telur geta haft víðtæk eða alvarleg áhrif á þjónustuhópa sína, almannahagsmuni eða þjóðaröryggi, svo og þegar slík netógn hefur raungerst og aðstæður kalla á fullan viðbúnað sveitarinnar. Þegar stjórn hefur náðst á áhættu eða atviki samkvæmt síðastnefndu ákvæði skal netöryggissveit skila viðeigandi samantekt þar um til netöryggisráðs.

Netöryggissveit er „heimilt“ að tilkynna *ríkislögreglustjóra* um alvarleg eða útbreidd atvik og áhættu sem ógnar net- og upplýsingaöryggi, og „skal, eftir því sem við kann að eiga“ viðhafa samstarf við ríkislögreglustjóra um varnir og viðbrögð, sbr. 3. mgr. 14. gr. laga nr. 78/2019 og 6. mgr. 82. gr. laga nr. 70/2022. Í 1. mgr. 14. gr. reglugerðar nr.

[66] Samkvæmt 17. gr. reglugerðar nr. 480/2021 skal netöryggissveit setja sér verklagsreglur um miðlun nauðsynlegra upplýsinga til eftirlitsstjórnvalda í kjölfar tilkynninga um alvarleg atvik eða áhættu sem ógna öryggi net- og upplýsingakerfa og henni berast frá mikilvægum innviðum og fjarskiptafyrirtækjum.
[67] Netöryggissveit getur sett sér verklagsreglur um form og flokka tilkynninga skv. 1. mgr. 11. gr. reglugerðar nr. 480/2021, sbr. 4. mgr. sama ákvæðis.

480/2019 kemur fram að netöryggissveit „[skuli] leitast við“ að upplýsa ríkislögreglustjóra um alvarleg og/eða útbreidd atvik eða áhættu sem ógna öryggi net- og upplýsingakerfa er varða þjónustuhópa netöryggissveitar og netumdæmi Íslands, eins og við eigi hverju sinni. Þá sé netöryggissveit *skylt* að tilkynna ríkislögreglustjóra um „yfirvofandi atvik og áhættu sem sveitin telur geta haft víðtæk eða alvarleg áhrif á þjónustuhópa sína, almannahagsmuni eða þjóðaröryggi, svo og þegar slík ógn hefur raungerst og aðstæður kalla á fullan viðbúnað sveitarinnar“, sbr. 2. mgr. 14. gr. reglugerðarinnar. Séu aðstæður með þeim hætti að teljist neyðarástand sem kann að ógna lífi og heilsu almennings, umhverfi og/eða eignum í skilningi laga nr. 82/2008 um almannavarnir, fer um viðbrögð stjórnvalda eftir ákvæðum þeirra laga, sbr. 3. mgr. sama ákvæðis reglugerðarinnar, sbr. einnig 2. mgr. 5. gr. laga nr. 78/2019.[68] Sjá einnig síðari umfjöllun um verkefni ríkislögreglustjóra.

Í 1. mgr. 16. gr. reglugerðar nr. 480/2021 er fjallað um upplýsingagjöf netöryggissveitar til *erlendra tengiliða*. Búi netöryggissveit yfir upplýsingum um atvik eða áhættu sem ógnar öryggi net- og upplýsingakerfa og áhrifa kann að gæta yfir landamæri, skal sveitin eftir því sem við á tilkynna um það til tengiliðar í því ríki eða ríkjum sem um ræðir. Í 5. mgr. 14. gr. laga nr. 78/2019 er jafnframt mælt fyrir um að berist netöryggissveit tilkynning um atvik sem hefur áhrif yfir landamæri skuli sveitin miðla tilkynningu þar um til útnefndra tengiliða í viðkomandi ríki.[69]

Framangreindu til fyllingar má einnig vísa til fyrri umfjöllunar um verkefni Fjarskiptastofu m.a. að því er varðar upplýsingagjöf til hagaðila og almennings, sbr. 81. gr. laga nr. 70/2022 og 10. gr. laga nr. 78/2019, sbr. kafla 2.3 og 3.4 hér að framan.

c) Tilmæli um aðgerðir og ráðstafanir

Netöryggissveit er heimilt að gefa út tilmæli um aðgerðir og ráðstafanir í því skyni að bregðast við og samhæfa viðbrögð við ógn, atviki eða áhættu innan netumdæmis Íslands,

[68] Í 4. mgr. 14. gr. reglugerðar nr. 480/2021 er ráðgert að netöryggissveit skuli setja sér verklagsreglur um upplýsingagjöf og samskipti við ríkislögreglustjóra samkvæmt ákvæðinu, í samráði við embættið. Um mat á stöðu, viðbrögð, samstarf og samhæfingu í kjölfar tilkynningar skv. 2. mgr. 14. gr. reglugerðarinnar fer samkvæmt viðbragðsáætlun ríkislögreglustjóra sem gerð er í samráði við netöryggissveit og sett á grundvelli laga um almannavarnir, sbr. 5. mgr. sama ákvæðis reglugerðarinnar.
[69] Í 2. mgr. 16. gr. reglugerðar nr. 480/2021 er gert ráð fyrir að netöryggissveit skuli setja sér verklagsreglur um tilkynningar og miðlun upplýsinga til erlendra aðila samkvæmt ákvæðinu.

sbr. 1. mgr. 10. gr. reglugerðar nr. 480/2021. Um tilmæli netöryggissveitar til mikilvægra innviða er fjallað í 4. mgr. 14. gr. laga nr. 78/2019, en sérstakt ákvæði um viðbrögð fjarskiptafyrirtækja við tilmælum sveitarinnar kemur fram í 3. mgr. 82. gr. laga nr. 70/2022. Ákvæði 10. gr. reglugerðarinnar gildir hvoru tveggja um tilmæli netöryggissveitar til mikilvægra innviða og fjarskiptafyrirtækja.

Í 2. mgr. 10. gr. reglugerðar nr. 480/2021 er ráðgert að mikilvægir innviðir skuli „ávallt leitast við“ að verða við tilmælum netöryggissveitar vegna atviks, áhættu eða bráðrar netógnar sem steðjar að einum eða fleiri mikilvægum innviðum eða fjarskiptafyrirtækjum. Skylt er að staðfesta móttöku tilmælanna og bregðast við þeim eins fljótt og kostur er og aðstæður krefjast. Í viðbrögðum samkvæmt ákvæðinu felst m.a. að veita netöryggissveit upplýsingar um hvernig tilmælum verður fylgt og innan hvaða tímaramma. Ef ekki er orðið við tilmælum netöryggissveitar ber viðkomandi að upplýsa sveitina eins fljótt og kostur er um ástæður þess og hvaða aðrar ráðstafanir eru taldar eiga betur við til að tryggja vernd net- og upplýsingakerfa. Ef mikilvægir innviðir fara ekki að tilmælum skulu þeir einnig upplýsa viðkomandi eftirlitsstjórnvald um ástæður þess með rökstuddum hætti, sbr. 4. mgr. 14. gr. laga nr. 78/2019.[70]

Það athugast að 2. mgr. 10. gr. reglugerðarinnar tekur samkvæmt efni sínu einnig til fjarskiptafyrirtækja (utan mikilvægra innviða). Reglugerðarákvæðið verður þó, hvað fjarskiptafyrirtæki áhrærir, að skoða með hliðsjón af eftirfarandi ákvæðum sem fela í sér ríkari skyldur fjarskiptafyrirtækja að þessu leyti, og takmörkun á svigrúmi þeirra til mats á því hvort fylgja beri tilmælum netöryggissveitar við ákveðnar aðstæður.

Í 3. mgr. 82. gr. laga nr. 70/2022 og 3. mgr. 10. gr. reglugerðar nr. 480/2021 er mælt fyrir um sérstaka skyldu fjarskiptafyrirtækja til að bregðast án tafar við tilmælum net-

[70] Í athugasemdum við ákvæðið er rakið að upplýsingar um ástæður þeirrar afstöðu, að fylgja ekki tilmælum netöryggissveitar, geti verið afar mikilvægar við samhæfingu aðgerða gegn ógnum og atvikum, svo og liður í að draga lærdóm af meðhöndlun atvika. Ekki sé gerð krafa um ítarlegan skriflegan rökstuðning, heldur fyrst og fremst að fullnægjandi upplýsingum verði miðlað um það að hvaða marki tilmæli eða ráðgjöf hafi ekki þótt eiga við og með hvaða hætti brugðist hafi verið við atvikinu. Mikilvægt sé að hafa í huga að gjarnan hafa aðilar skamman tíma til að bregðast við ógn eða árás, og má skylda samkvæmt málsgreininni ekki verða til að tefja aðila frá því að bregðast við og meðhöndla atvik. Hins vegar sé æskilegt að tilmæli sveitarinnar og svör fulltrúa mikilvægra innviða séu skjalfest. Mikilvægir innviðir útvisti ekki ábyrgð á eigin rekstri og ganga verði út frá að þekking þeirra á virkni eigin kerfa, netvörnum og viðbúnaði sé ótvíræð, eins og segir í athugasemdunum.

öryggissveitar í tveimur tilvikum. Annars vegar ef tilmæli varða aðgerðir gegn bráðri aðsteðjandi netógn, hvort sem sú ógn steðjar að öryggi neta og þjónustu eins eða fleiri fjarskiptafyrirtækja. Hins vegar ef tilmæli lúta að aðgerðum gegn mjög alvarlegri áhættu eða atvikum sem steðja að net- og upplýsingakerfum mikilvægra innviða eða opinberra stofnana, almannahagsmunum eða þjóðaröryggi. Í b-lið 3. mgr. 10. gr. reglugerðarinnar er sá viðbótaráskilnaður gerður, varðandi síðarnefnda tilvikið, að „yfirgnæfandi líkur [séu] á að fjarskiptafyrirtæki geti átt hlutdeild í að sporna við ógn, áhættu eða atviki eða lágmarka mögulegt tjón af völdum þess“. Þessi þrenging reglugerðarinnar á skyldu fjarskiptafyrirtækja til að hlíta tilmælum netöryggissveitar skv. 3. mgr. 82. gr. laga nr. 70/2022 á sér ekki stoð í texta ákvæðisins, en virðist öðru fremur helgast af meðalhófssjónarmiðum.[71] Það vekur einnig athygli að þrengingin gildir ekki um fyrra tilvikið, sbr. framangreint, heldur aðeins hið síðarnefnda, sé tekið mið af orðalagi 3. mgr. 10. gr. reglugerðarinnar.

Í tilvikum sem falla undir 3. mgr. 82. gr. laga nr. 70/2022 hefur fjarskiptafyrirtæki ekki svigrúm til sjálfstæðs mats á því hvort fylgja beri tilmælum netöryggissveitar samkvæmt efni sínu. Telji netöryggissveit að aðstæður séu með þessum hætti skal sérstaklega vísað til þess í tilmælum, sbr. 4. mgr. 10. gr. reglugerðarinnar.

d) Kæra til lögreglu

Netöryggissveit skal hvetja mikilvæga innviði og fjarskiptafyrirtæki til að tilkynna lögreglu um öryggisatvik leiki grunur á refsiverðri háttsemi, sbr. 2. mgr. 9. gr. laga nr.

[71] Áskilnaður reglugerðarinnar um að fyrir fram séu „yfirgnæfandi líkur“ á að liðsinni fjarskiptafyrirtækis komi að gagni, á sér ekki stoð í orðalagi 3. mgr. 82. gr. laga nr. 70/2022. Aftur á móti er í skýringum við ákvæðið (athugasemdum við 27. gr. frumvarps til laga nr. 78/2019 sem vísað er til í athugasemdum við 82. gr. frumvarps til laga nr. 70/2022) vísað til aðstæðna þar sem „mjög aðkallandi er að bregðast við bráðri aðsteðjandi netógn og yfirgnæfandi líkur eru á að fjarskiptafyrirtæki geti átt hlutdeild í að leysa neyðarástandið og/eða lágmarka mögulegt tjón af völdum þess“. Þá kunni „litlar líkur … að vera á því að fjarskiptafyrirtæki líti viðbrögð við slíkri ógn öðrum augum en sérfræðingar Póst- og fjarskiptastofnunar [nú Fjarskiptastofu]“. Þar sem viðbragðstími geti skipt sköpum við slíkar aðstæður þyki „óhjákvæmilegt að leggja til lögfestingu slíkrar heimildar“ en ljóst megi vera að „slíku úrræði þyrfti að beita af fyllstu varkárni, ef til kæmi“. Þá megi ljóst vera að „kortlagning samspils ólíkra laga við ólíkar aðstæður, á grundvelli fjölbreytilegra sviðsmynda, ekki síst þar sem net- og upplýsingakerfi mikilvægra innviða koma við sögu, [sé] afar æskileg“. Netógnir eru á hinn bóginn fjölbreytilegar, mannlega þáttinn má til að mynda ekki vanmeta, og því fer fjarri að slík neyðarheimild gagnvart fjarskiptafyrirtækjum sé lykillinn að farsælli lausn og viðbrögðum við öllum alvarlegum atvikum. Athugasemdir við 14. gr. frumvarps sem varð að lögum nr. 78/2019 (149. lögþ. 2018-2019, þskj. 557 – 416. mál).

78/2019 og 6. mgr. 82. gr. laga nr. 70/2022, sbr. einnig 1. mgr. 18. gr. reglugerðar nr. 480/2021. Jafnframt er netöryggissveit heimilt að vísa til lögreglu „upplýsingum sem henni berast vegna landsbundins hlutverks síns sem tengiliðar ef efni þeirra teljast fremur varða viðfangsefni löggæslu en netöryggissveitar“, sbr. 2. mgr. sama reglugerðarákvæðis. Samkvæmt framansögðu er meginreglan sú að netöryggissveit kærir ekki sjálf refsiverðra háttsemi til lögreglu. Á hinn bóginn er ákvæði 2. mgr. 18. gr. reglugerðarinnar nokkuð almennt orðað að því er varðar miðlun netöryggissveitar á upplýsingum til lögreglu ef þær varða frekar „viðfangsefni löggæslu“.

Gera verður greinarmun á því þegar öryggisatvik eru kærð til lögreglu, svo og tilvikum þegar aðilar, þ.m.t. mikilvægir innviðir, brjóta gegn skyldum sínum samkvæmt lögum nr. 78/2019. Í síðara tilvikinu er hlutaðeigandi eftirlitsstjórnvaldi heimilt og eftir atvikum skylt að kæra mögulegt brot til lögreglu, sbr. nánar 25. gr. laganna og fyrri umfjöllun. Ef í hlut eiga mikilvægir innviðir sem lúta eftirliti Fjarskiptastofu samkvæmt lögunum þá er stofnunin bær til að kæra viðkomandi brot til lögreglu. Þá er Fjarskiptastofa bær til að kæra til lögreglu brot sem felst í rangri tilkynningu til netöryggissveitar, sbr. 4. mgr. 26. gr. laganna.[72]

3.5.5. Upplýsingaöflun netöryggissveitar

a) Almennt

Til að tryggja netöryggissveit bestu faglegar forsendur til viðbragða við ógnum, atvikum og áhættu í netumdæmi Íslands, nýtur sveitin víðtæks réttar til aðgangs að upplýsingum m.a. frá mikilvægum innviðum, fjarskiptafyrirtækjum, samstarfsaðilum og stjórnvöldum, sbr. ákvæði 17. gr. laga nr. 78/2019 og 84. gr. laga nr. 70/2022, sbr. einnig 1. mgr. 27. gr. reglugerðar nr. 480/2021.[73] Þannig er ráðgert í fyrrnefndum ákvæðum að netöryggissveit sé heimilt að afla gagna og upplýsinga sem hún telur nauðsynlegar, eftir atvikum í samráði við hlutaðeigandi eftirlitsstjórnvöld samkvæmt lögum nr. 78/2019 þar sem það á við, sbr. einnig síðari umfjöllun um dagsektarheimild 1. mgr. 22. gr. laganna.

[72] Samkvæmt ákvæðinu varðar það refsingu skv. 120. gr. og 120. gr. a almennra hegningarlaga að gefa af ásetningi eða stórkostlegu gáleysi ranga tilkynningu til netöryggissveitar skv. 8. eða 15. gr. laga nr. 78/2019.

[73] Í tilvísuðum ákvæðum laga nr. 78/2019 og reglugerðar nr. 480/2021 eru umferðarskrár netbúnaðar og -þjóna teknar sem dæmi um gögn og upplýsingar sem netöryggissveit getur aflað.

Auk þess að kalla eftir skriflegum upplýsingum eða gögnum hefur netöryggissveit heimild til að kalla einstaklinga til skýrslugjafar ef þörf krefur vegna hlutverks sveitarinnar, sbr. 3. mgr. 17. gr. laga nr. 78/2019 og 2. mgr. 27. gr. áðurnefndrar reglugerðar. Samkvæmt nefndu reglugerðarákvæði skal netöryggissveit eftir fremsta megni tryggja friðhelgi viðkomandi, m.a. með því að gæta trúnaðar um auðkenni hans. Þá skal sveitin birta nánari verklagsreglur um fyrirkomulag slíkrar skýrslugjafar, sbr. 3. mgr. sama reglugerðarákvæðis.[74]

Samkvæmt 28. gr. reglugerðar nr. 480/2021 getur netöryggissveit óskað eftir því að þjónustuhópar hennar gefi yfirlitsskýrslu í upphafi hvers árs, en eigi síðar en 1. febrúar, um öll helstu atvik og áhættu sem ógnað hafa öryggi net- og upplýsingakerfa næstliðið ár. Í slíkri skýrslu skal vera tölfræðilegt yfirlit um tíðni og gerðir áhættu og atvika.

Ákvæði um þagnarskyldu sem gilda um viðkomandi aðila víkja fyrir upplýsingarétti netöryggissveitar samkvæmt framansögðu, sbr. 4. mgr. 27. gr. reglugerðarinnar, sbr. einnig 4. mgr. 17. gr. laga nr. 78/2019. Í lagaákvæðinu er reyndar aðeins getið um þagnarskyldureglur sem taka til mikilvægra innviða, en reglugerðarákvæðið takmarkast ekki við mikilvæga innviði og er því víðtækara að þessu leyti.

Rétt er að benda á að ekki er í öllum tilvikum ljóst hvernig netöryggissveit getur knúið fram afhendingu upplýsinga á grundvelli ofangreindra ákvæða. Í 1. mgr. 22. gr. laga nr. 78/2019 er veitt heimild til að leggja dagsektir á mikilvæga innviði ef þeir verða ekki við ósk um afhendingu upplýsinga að kröfu eftirlitsstjórnvalds skv. 12. gr. laganna. Í dagsektarheimildinni er hins vegar ekki vísað til 17. gr. laganna. Því verður upplýsingakrafa netöryggissveitar ekki felld undir dagsektarheimild 1. mgr. 22. gr. laganna nema henni sé fylgt eftir með atbeina eftirlitsstjórnvalds á grundvelli heimildar í 12. gr. laganna, en síðastnefnda ákvæðið gildir í meginatriðum aðeins um gagnaöflun frá mikilvægum innviðum. Því er ekki ljóst hvernig unnt er að framfylgja kröfu netöryggissveitar um upplýsingar þegar hún beinist að öðrum aðilum en mikilvægum innviðum.

Um þagnarskyldu netöryggissveitar o.fl. og meðferð hennar á gögnum og upplýsingum, þ.m.t. persónuupplýsingum, og miðlun þeirra milli stjórnvalda, öryggisráðstafanir vegna

[74] Sjá einnig heimild eftirlitsstjórnvalda til skýrslutöku af einstaklingum í 1. mgr. 12. gr. laga nr. 78/2019.

trúnaðar um gögn o.fl., gilda ítarleg ákvæði í 19.-21. gr. laga nr. 78/2019, sbr. einnig 29.-32. gr. reglugerðar nr. 480/2021.

b) Sjálfvirk upplýsingamiðlun

Vegna upplýsingaöflunar netöryggissveitar er Fjarskiptastofu heimilt að óska eftir því við mikilvæga innviði og fjarskiptafyrirtæki að komið skuli upp sjálfvirkri upplýsingamiðlun á milli kerfa hlutaðeigandi aðila og netöryggissveitar, til að greina og meta ógnir og áhættu við net- og upplýsingakerfi viðkomandi, sbr. 2. mgr. 17. gr. laga nr. 78/2019 og 84. gr. laga nr. 70/2022, sbr. einnig 20. gr. reglugerðar nr. 480/2021. Gerður skal skriflegur samningur um sjálfvirka upplýsingamiðlun og skal hann m.a. geyma lýsingu á tæknilegri útfærslu upplýsingamiðlunarinnar svo og upplýsingar um tegund og vinnslu persónuupplýsinga sem safnað er, meðferð þeirra, vistun og eyðingu, sbr. nánar 1. mgr. 20. gr. reglugerðarinnar. Í 4. mgr. 20. gr. reglugerðarinnar er áréttað að samningur um sjálfvirka upplýsingamiðlun leysi viðkomandi aðila ekki undan tilkynningarskyldu til netöryggissveitar um alvarlega áhættu og atvik samkvæmt lögum nr. 78/2019 og lögum nr. 70/2022, sbr. einnig 3. mgr. áðurnefnds reglugerðarákvæðis.

c) Tæknileg vöktunarþjónusta og umferðarmælingar hjá fjarskiptafyrirtækjum

Í 1. mgr. 83. gr. laga nr. 70/2022 kemur fram að telji Fjarskiptastofa það nauðsynlegt skuli fjarskiptafyrirtæki og netöryggissveitin gera með sér samning um uppsetningu og rekstur tæknilegrar vöktunarþjónustu fyrir net- og upplýsingakerfi fjarskiptafyrirtækisins. Tilgangur slíks samnings er að greina hættur og ummerki um árásir, spillikóða og aðrar vísbendingar um aðstæður sem gætu skapað hættu fyrir öryggi fjarskiptaneta og fjarskiptaþjónustu fjarskiptafyrirtækisins. Í 1. mgr. 22. gr. reglugerðar nr. 480/2021 er hnykkt á því að fjarskiptafyrirtæki sé skylt að verða við beiðni netöryggissveitar um gerð samnings um tæknilega vöktunarþjónustu, sbr. einnig 2. mgr. 83. gr. laga nr. 70/2022 og 2. mgr. 21. gr. reglugerðarinnar þar sem tilgreind eru þau efnisatriði sem fjallað skal um í slíkum samningi.

Þá er kveðið svo á í 3. mgr. 83. gr. laga nr. 70/2022 og 2. mgr. 22. gr. reglugerðarinnar að fjarskiptafyrirtæki sé skylt að hýsa og samtengjast endurgjaldslaust þeim búnaði netöryggissveitar sem Fjarskiptastofa metur nauðsynlegan vegna tæknilegrar

vöktunarþjónustu, en netöryggissveit ber ábyrgð á öðrum kostnaði vegna framkvæmdar vöktunarinnar. Í 3. mgr. 83. gr. laganna segir einnig að netöryggissveit sé heimilt að taka við upplýsingum á grundvelli samnings um vöktunarþjónustu án dómsúrskurðar. Síðastnefnda reglu 3. mgr. verður væntanlega að skýra í samræmi við 4. mgr. sama ákvæðis, sbr. hér að neðan, þannig að það taki einungis til upplýsinga sem eru ópersónugreinanlegar.

Í 4. mgr. 83. gr. laga nr. 70/2022 er mælt svo fyrir að hvorki sé heimilt að persónugreina netumferð né skima einstaka netpakka eða flæði sem netöryggissveitin kann að nema í almennum netkerfum fjarskiptafyrirtækja. Netöryggissveitinni sé þó heimilt að taka við upplýsingum um almenna netumferð án dómsúrskurðar, þ.m.t. á samtengipunktum og í útlandagáttum, enda séu þær upplýsingar ópersónugreinanlegar.

Í 1. mgr. 23. gr. reglugerðar nr. 480/2021 er netöryggissveit heimilað að afla tölfræðilegra upplýsinga um heildarmagn umferðar í almennum netkerfum fjarskipta-fyrirtækja, þar með talið á samtengipunktum og í útlandagáttum, enda séu þær upplýsingar ópersónugreinanlegar. Skal netöryggissveit gera samning við fjarskipta-fyrirtæki um útfærslu umferðarmælinga samkvæmt framansögðu, sbr. 2. mgr. 23. gr. reglugerðarinnar, þ.m.t. um uppsetningu og rekstur nauðsynlegs búnaðar. Um efni slíkra samninga og endurgjald fer eftir 1. og 2. mgr. 22. gr. reglugerðarinnar.

3.5.6. Þjónusta netöryggissveitar við mikilvæga innviði, opinberar stofnanir o.fl.

a) Tæknileg vöktunarþjónusta

Samkvæmt 2. mgr. 16. gr. laga nr. 78/2019 er netöryggissveit heimilt að bjóða mikilvægum innviðum og opinberum stofnunum tæknilega vöktunarþjónustu, á nánar skilgreindum og skjalfestum forsendum, í því skyni að greina ummerki um árásir, spillikóða og aðrar hættulegar aðstæður, sbr. nánar 21. gr., 25. gr. og 1. mgr. 24. gr. reglugerðar nr. 480/2021.[75] Vöktunarþjónustan getur verið hluti af tæknilegum öryggisráðstöfunum og áhættustýringu mikilvægra innviða og opinberra stofnana.

[75] Kveðið er á um efnisatriði slíkra samninga í 2. mgr. 21. gr. reglugerðar nr. 480/2021.

Með tæknilegri vöktunarþjónustu stendur hlutaðeigandi til boða að nýta sérþekkingu og aðstoð af hálfu netöryggissveitar við að greina ógnir og áhættur gagnvart net- og upplýsingakerfum sínum, eins og nánar er rakið í lögskýringargögnum. Þjónustan gæti meðal annars falist í uppsetningu á skynjarabúnaði við kerfi hlutaðeigandi aðila sem yrði rekinn á kerfum þeirra og undir þeirra umsjá. Öflug skimun í formi tæknilegrar vöktunarþjónustu stuðlar að bættri yfirsýn netöryggissveitar á netógnir hér á landi, til viðbótar því að hún treysti á erlendar upplýsingaveitur og systursveitir og almennar tilkynningar frá aðilum. Í lögskýringargögnum er þó áréttað að ábyrgð á rekstri net- og upplýsingakerfa hlutaðeigandi verður ekki lögð á netöryggissveit með samningi um tæknilega vöktunarþjónustu.[76]

Í 4. mgr. 21. gr. reglugerðar nr. 480/2021 er áréttað að tæknileg vöktunarþjónusta netöryggissveitar leysi aðila ekki undan tilkynningarskyldu til netöryggissveitar vegna alvarlegra atvika eða áhættu samkvæmt lögum nr. 78/2019, sbr. einnig 3. mgr. áðurnefnds reglugerðarákvæðis.

Endurgjald vegna tæknilegrar vöktunarþjónustu skal taka mið af útlögðum kostnaði netöryggissveitar vegna búnaðar sem staðsettur verður við eigin net- og upplýsingakerfi hlutaðeigandi rekstraraðila, sbr. 2. mgr. 16. gr. laga nr. 78/2019. Í lögskýringargögnum er tekið dæmi um kostnað vegna uppsetningar og rekstrar skynjara af hálfu netöryggissveitar. Hins vegar nái ákvæðið ekki til kostnaðar af „miðlægu kerfi netöryggissveitar eða frekari úrvinnslu sveitarinnar á upplýsingum“.[77]

Í 3. mgr. 16. gr. laga nr. 78/2019 kemur fram að Stjórnarráð Íslands skuli njóta „þjónustu Fjarskiptastofu á sviði netöryggismála skv. 1. og 2. mgr.“, án sérstaks endurgjalds, sbr. einnig 1. mgr. 25. gr. reglugerðar nr. 480/2021. Því er gjaldtaka vegna tæknilegrar vöktunarþjónustu bundin við aðrar opinberar stofnanir, þ.e. þær sem falla ekki undir Stjórnarráð Íslands (ráðuneyti). Enn fremur greiða mikilvægir innviðir fyrir þjónustuna eins og áður var rakið.

[76] Athugasemdir við 16. gr. í greinargerð með lögum nr. 78/2019 (149. lögþ. 2018-2019, þskj. 557 – 416. mál). Þar eru einnig reifaðar ýmsar útfærslur á tæknilegri vöktunarþjónustu með skynjarabúnaði o.fl.
[77] Athugasemdir við 16. gr. í greinargerð með frumvarpi til laga nr. 78/2019 (149. lögþ. 2018-2019, þskj. 557 – 416. mál).

b) Aðstoð, ráðgjöf og leiðbeiningar um sérhæfðar forvarnir

Samkvæmt 1. mgr. 16. gr. laga nr. 78/2019 geta mikilvægir innviðir leitað til netöryggissveitar um „aðstoð og leiðbeiningar um sérhæfðar forvarnir“ í tengslum við öryggi net- og upplýsingakerfa sinna.[78] Sama á við um „Stjórnarráð Íslands og aðrar opinberar stofnanir“. Stjórnarráð Íslands skal njóta ofangreindrar þjónustu netöryggissveitar endurgjaldslaust, sbr. 3. mgr. 16. gr. laganna og 1. mgr. 25. gr. reglugerðar nr. 480/2021. Aðrar opinberar stofnanir geta jafnframt gert samninga við Fjarskiptastofu um aðstoð og ráðgjöf gegn endurgjaldi, sbr. 3. mgr. 16. gr. laganna og 2. mgr. 24. gr. reglugerðarinnar. Með þessu er svonefnd GovCERT þjónusta fest í sessi en ráðgert er að forsendur hennar séu skjalfestar á hverjum tíma og endurmetnar reglubundið. Í síðastnefndu lagaákvæði varðandi endurgjald er ekki vikið sérstaklega að mikilvægum innviðum. Af lögskýringargögnum má þó ráða að ætlunin hafi verið að mikilvægir innviðir skyldu njóta þjónustu netöryggissveitar skv. 1. mgr. 16. gr. laganna án endurgjalds. Því greiðir opinber stofnun ekki fyrir þessa þjónustu ef hún telst til mikilvægra innviða.[79]

c) Aðrir þjónustusamningar við þriðju aðila

Netöryggissveit er heimilt að bjóða öðrum en fyrrgreindum aðilum („þriðju aðilum“) þjónustu á sviði netöryggismála samkvæmt samningi milli aðila þar sem fjallað er um umfang þjónustunnar, tæknilega útfærslu og endurgjald, sbr. 26. gr. reglugerðar nr. 480/2021. Sú heimild tekur væntanlega m.a. til samninga um tæknilega vöktunarþjónustu, aðstoð og ráðgjöf varðandi sérhæfðar forvarnir, og annars konar þjónustu á sviði netöryggismála, sbr. fyrri umfjöllun.

[78] Í 1. mgr. 82. gr. laga nr. 70/2022 er einnig ráðgert að netöryggissveit skuli aðstoða fjarskiptafyrirtæki við forvarnir, leiðbeina þeim og styðja við skjót viðbrögð gegn aðsteðjandi hættu.

[79] Athugasemdir við 16. gr. í greinargerð með lögum nr. 78/2019 (149. lögþ. 2018-2019, þskj. 557 – 416. mál): „Í 1. mgr. ákvæðisins er lagt til að kveðið verði á um tiltekið aðgengi mikilvægra innviða að sérfræðiþekkingu starfsliðs netöryggissveitar Póst- og fjarskiptastofnunar. Þeir geti með öðrum orðum leitað til sveitarinnar um aðstoð og leiðbeiningar um sérhæfðar forvarnir í tengslum við öryggi net- og upplýsingakerfa sinna, en að tekið verði fram að hlutverk sveitarinnar sé einkum að styðja við skjót viðbrögð gegn aðsteðjandi hættu. Leiðbeiningar samkvæmt þessari málsgrein varða sérhæfðar forvarnir, en fela ekki í sér almenna ráðgjöf sem í boði er á samkeppnismarkaði. Netöryggissveit veitir aðstoð og ráðgjöf á bestu mögulegu faglegu forsendum á hverjum tíma, t.d. á grundvelli upplýsinga sem hún kann að búa yfir í gegnum alþjóðlegt tengslanet sitt. Ekki er lagt til að innheimt verði endurgjald vegna þessa aðgengis, þegar á þarf að halda.“

3.5.7. Samráðs- og sviðshópar og viðbúnaðaræfingar

Netöryggissveit er heimilt að setja á laggirnar ýmsa samráðs- og sviðshópa til að efla skilvirkni viðbragða við netógnum. Í 1. mgr. 18. gr. laga nr. 78/2019 er netöryggissveit veitt heimild til að setja á fót þverfaglegan samráðshóp í þeim tilgangi að efla tengsl og samstarf á milli mikilvægra innviða og sveitarinnar. Í skýringum við ákvæðið segir að samráðshópnum sé ekki markað tæmandi hlutverk í ákvæðinu og geti m.a. nýst sem vettvangur fyrir samráð og upplýsingaskipti í tengslum við greiningu ógna og samræmd viðbrögð við þeim ógnum. Samráðshópurinn muni m.a. hafa það hlutverk að upplýsa og samræma aðgerðir þegar aðkallandi ógnir eru taldar geta haft áhrif á fleiri en eitt svið mikilvægra innviða.[80]

Netöryggissveit er jafnframt heimilt skv. 2. mgr. 18. gr. laga nr. 78/2019 að setja á fót sérstaka sviðshópa fyrir hvert svið nauðsynlegrar þjónustu skv. 1. mgr. 2. gr. laganna og stafræna þjónustuveitendur (mikilvæga innviði), og fyrir opinberar stofnanir. Sviðshópar skulu vera vettvangur tæknilegs samráðs og upplýsingaskipta á sviði net- og upplýsingaöryggis, er hefur það að meginmarkmiði að greina ógnir og áhættu, stuðla að auknu net- og upplýsingaöryggi og takmarka tjón af völdum netárása. Í skýringum við ákvæðið er því lýst að hlutverk sviðshópa geti m.a. verið að skiptast á upplýsingum um stöðumat og áherslur í öryggismálum, að miðla upplýsingum og fróðleik um öryggismál, aðsteðjandi ógnir og aðferðir til að verjast þeim o.s.frv.[81]

Þá mælir 5. mgr. 82. gr. laga nr. 70/2022 fyrir um að netöryggissveit skuli setja á laggirnar samstarfshóp með fjarskiptafyrirtækjum fyrir tæknilegt samráð og upplýsingaskipti á sviði net- og upplýsingaöryggis, m.a. til að greina ógnir og öryggisatvik sem og til að samræma viðbrögð.

Í 13. gr. reglugerðar nr. 480/2021 eru ítarlegri fyrirmæli um ofangreinda samráðs- og sviðshópa á vegum netöryggissveitar, m.a. um fundi þeirra, stefnu og verklagsreglur og trúnað um upplýsingar sem fara um hendur þeirra. Samkvæmt ársyfirliti netöryggis-

[80] Athugasemdir við 18. gr. í greinargerð með frumvarpi til laga nr. 78/2019 (149. lögþ. 2018-2019, þskj. 557 – 416. mál).
[81] Athugasemdir við 18. gr. í greinargerð með frumvarpi til laga nr. 78/2019 (149. lögþ. 2018-2019, þskj. 557 – 416. mál).

sveitar 2022 eru sviðshóparnir sex talsins og með yfir 50 rekstraraðila mikilvægra innviða og nauðsynlegrar þjónustu.[82]

Netöryggissveit getur jafnframt skipulagt viðbúnaðaræfingar (netöryggisæfingar) með þátttöku fulltrúa mikilvægra innviða og opinberra stofnana, í því skyni að stuðla að efldum viðnámsþrótti net- og upplýsingakerfa og eftir atvikum í samstarfi við ríkislögreglustjóra og eftirlitsstjórnvöld, sbr. 5. mgr. 18. gr. laga nr. 78/2019, sbr. einnig 10. mgr. 25. gr. laga nr. 75/2021. Viðbúnaðaræfingar miða nánar tiltekið að því að bæta boðleiðir, stjórnun og sameiginlegt viðbragð við áhættu og atvikum sem ógna öryggi net- og upplýsingakerfa, þar á meðal lágmörkun áhættu og tjóns, sbr. 1. mgr. 12. gr. reglugerðar nr. 480/2021. Í reglugerðarákvæðinu er jafnframt ráðgert að viðbúnaðar-æfingar geti verið verkefni innan samráðs-, sviðs- og samstarfshópa sveitarinnar skv. 13. gr. reglugerðarinnar og að áhersla skuli lögð á æfingar í samstarfi við þjónustuhópa og opinbera samstarfsaðila. Í skýringum við 18. gr. laga nr. 78/2019 er rakið að dýrmætan lærdóm megi draga af framkvæmd viðbúnaðaræfinga, í því skyni að efla enn frekar öryggi og viðnámsþrótt net- og upplýsingakerfa mikilvægra innviða, og því heppilegt að tryggja þátttöku af hálfu þeirra sem netöryggissveit kann að óska eftir hverju sinni. Viðbúnaðaræfingar geti verið af ýmsu tagi, allt frá umsvifaminni æfingum þar sem reynir t.d. á þekkingu starfsliðs á viðbragðsferlum og boðleiðum, upp í tíma- og mannaflafrekari æfingar þar sem atburðarás er sviðsett og reynir á meðhöndlun atviks í rauntíma.[83]

3.6. Ríkislögreglustjóri – almannavarnir

Í ákvæðum laga og reglna um netöryggissveit, sem áður var gerð grein fyrir, er víða gert ráð fyrir samráði sveitarinnar/Fjarskiptastofu við ríkislögreglustjóra vegna málefna almannavarna, sbr. 2. mgr. 5. gr. laga nr. 82/2008 um almannavarnir, sbr. einnig ákvæði lögreglulaga nr. 90/1996. Meðal annars er í 10. mgr. 25. gr. laga nr. 75/2021 mælt fyrir um að Fjarskiptastofa og ríkislögreglustjóri skuli hafa gagnkvæmt og virkt samstarf um net- og upplýsingaöryggi, svo og um viðbúnaðaræfingar og aðrar aðgerðir sem miða að

[82] CERT-IS – Ársyfirlit 2022, bls. 12-13.
[83] Athugasemdir við 18. gr. í greinargerð með frumvarpi til laga nr. 78/2019 (149. lögþ. 2018-2019, þskj. 557 – 416. mál). Sjá einnig umfjöllun í CERT-IS – Ársyfirlit 2022, bls. 14-15.

því að stuðla að öryggi og viðnámsþrótti innviða. Samstarf Fjarskiptastofu og net-öryggissveitar við ríkislögreglustjóra er einkar mikilvægt við samhæfingu viðbragða við netógnum sem falla innan verksviðs almannavarna samkvæmt lögum nr. 82/2008 og eru því af alvarlegri gerð.[84]

Í 2. mgr. 5. gr. laga nr. 78/2019 er fjallað um skil þeirra laga gagnvart lögum nr. 82/2008. Í ákvæðinu segir að ef „hætta steðjar að net- og upplýsingaöryggi með þeim hætti að teljist neyðarástand sem kann að ógna lífi og heilsu almennings, umhverfi og/eða eignum í skilningi laga um almannavarnir [fari] um viðbrögð stjórnvalda á grundvelli þeirra laga“. Í skýringum við ákvæðið er tekið fram að því sé ekki ætlað að koma í veg fyrir viðbrögð á grundvelli ákvæða laga nr. 78/2019 heldur að minna á að ef slík staða kemur upp verði einnig að gæta að lögum nr. 82/2008.[85] Þá má minna á að eitt af hlutverkum Fjarskiptastofu, sbr. 2. mgr. 8. gr. laga nr. 75/2021, er að stuðla að áreiðanlegum fjarskiptum út frá hagsmunum almannavarna, neyðarfjarskipta og netöryggis. Skal Fjarskiptastofa vera ráðgefandi aðili fyrir yfirvöld vegna almanna-varnaástands, auk þess að stuðla að öryggi og viðnámsþrótti fjarskiptainnviða, almanna- og þjóðaröryggi og samhæfðum viðbrögðum við sérstakar aðstæður, eftir atvikum með fyrirmælum um ráðstafanir samkvæmt XII. kafla laga nr. 70/2022.[86] Þá ber að nefna að forstjóri Fjarskiptastofu á sæti í almannavarna- og öryggismálaráði skv. 1. tölul. 2. mgr. 4. gr. laga nr. 82/2008, en almannavarna- og öryggismálaráð skal eiga samráð við þjóðaröryggisráð um mál eða atburði sem kunna að snerta verksvið þeirra, sbr. 8. gr. laga nr. 98/2016 um þjóðaröryggisráð

Auk framangreinds hefur Fjarskiptastofa í almannavarnaástandi sjálfstæða heimild til að gefa fjarskiptafyrirtækjum fyrirmæli um aðgerðir til að tryggja fjarskiptasamband á tilteknu svæði, svo sem að opnað skuli fyrir reikiþjónustu, sbr. 3. mgr. 8. gr. laga nr.

[84] Í athugasemdum við 14. gr. laga nr. 78/2019 er einnig áréttað mikilvægi þess að Fjarskiptastofa og löggæsluyfirvöld eigi með sér gott og virkt samstarf á sviði netöryggis og að ferlar/verklag um boðskipti og viðbrögð við netárásum séu kortlögð og endurskoðuð reglubundið.

[85] Athugasemdir við 5. gr. í greinargerð með frumvarpi til laga nr. 78/2019 (149. lögþ. 2018-2019, þskj. 557 – 416. mál). Þar er einnig bent á að tilskipun (ESB) 2016/1148 er ekki ætlað að takmarka eða hafa áhrif á aðgerðir eða úrræði stjórnvalda til að vernda grundvallarhlutverk sitt og þjóðaröryggi, sbr. 6. mgr. 1. gr. hennar.

[86] Í kjölfar breytinga á lögum nr. 82/2008 um almannavarnir með lögum nr. 39/2022, vísar hugtakið almannavarnaástand nú til almannavarnastigs, sbr. 2. gr. a laganna, sbr. einnig 2. mgr. 5. gr.

70/2022. Sjá einnig neyðarúrræði varðandi fjarskipti á hættutímum sem ráðherra hefur heimild til að grípa til skv. 100. gr. laga nr. 70/2022.

Að almannavörnum frágengnum geta viðfangsefni á sviði netöryggis haft snertiflöt við verkefni greiningardeildar ríkislögreglustjóra, sem hefur m.a. það hlutverk að veita ráðgjöf um viðbúnað sem hefur þýðingu fyrir hagsmuni ríkisins og þjóðhagslega mikilvæga starfsemi, sbr. e-lið 2. mgr. 4. gr. reglugerðar nr. 404/2007. Einnig geta viðfangsefni netöryggis haft snertifleti við önnur verkefni greiningardeildar ríkislögreglustjóra er snúa að því að fyrirbyggja háttsemi sem kunna að varða við ákvæði X. og XI. kafla almennra hegningarlaga nr. 19/1940, svo sem starfrænar árásir og njósnir.[87]

4. Samantekt

Hér að framan hefur verið fjallað um hlutverk og verkefni lykilstjórnvalda á sviði netöryggismála eins og þeim er lýst í gildandi lögum, þ.m.t. háskóla-, iðnaðar- og nýsköpunarráðuneytisins,[88] netöryggisráðs, Fjarskiptastofu og netöryggissveit, auk eftirlitsstjórnvalda samkvæmt lögum nr. 78/2019 annarra en Fjarskiptastofu, og ríkislögreglustjóra vegna almannavarna. Enn fremur hefur verið vikið að verkefnum annarra stjórnvalda sem snúa að netöryggi, þ.m.t. dómsmálaráðuneytisins vegna almannavarna, löggæslu og CER-tilskipunarinnar, utanríkisráðuneytisins vegna öryggis- og varnarmála, fjármála- og efnahagsráðuneytisins og Seðlabanka Íslands vegna fjármálakerfisins og DORA-gerða ESB, auk þjóðaröryggisráðs vegna eftirlits með framkvæmd þjóðaröryggisstefnunnar.[89]

Þar sem verkefni vegna netöryggis í ólíkum hlutum stjórnkerfisins geta skarast með ýmsum hætti eiga hlutaðeigandi stjórnvöld í margvíslegu samstarfi m.a. á vettvangi netöryggisráðs og starfshópa, og á grundvelli samstarfssamninga um upplýsingamiðlun o.fl., með heimild í þeim lögum og reglum sem eiga við hverju sinni. Til að mynda er í lögum nr. 78/2019 og ákvæðum um netöryggissveit í reglugerð nr. 480/2021 að finna heimildir fyrir ýmissi samvinnu, samhæfingu og upplýsingaskiptum milli stjórnvalda á þessu sviði. Ekki verður annað séð en að lög nr. 78/2019 og reglugerð nr. 480/2021 veiti

[87] *Fjölþáttaógnir* - skýrsla greiningardeildar Ríkislögreglustjóra maí 2023.
[88] Miðað við árið 2024 þegar skýrsla þessi er rituð.
[89] Sjá tilvísanir í umræddar ESB-gerðir í kafla 3.1.

almennt traustan grundvöll fyrir samstarfi milli stjórnvalda á sviði netöryggis. Sem dæmi um aðrar lagaheimildir sem geta haft þýðingu í þessu samhengi má nefna 8. gr. laga nr. 98/2016 um þjóðaröryggisráð, sem veitir ráðinu heimild til að kalla eftir skýrslum eða gögnum um atriði er varða þjóðaröryggi frá ráðuneytum, opinberum stofnunum eða opinberum hlutafélögum. Þá má nefna ákvæði 23. gr. varnarmálalaga nr. 34/2008 sem gerir ráð fyrir að utanríkisráðuneytið geti miðlað til annarra stjórnvalda hér á landi upplýsingum úr upplýsingakerfum Atlantshafsbandalagsins og erlendra samstarfsaðila, sbr. einnig 4. mgr. 20. gr. laga nr. 78/2019 þar sem áréttað er að um trúnað slíkra upplýsinga fari samkvæmt 2. mgr. 24. gr. varnarmálalaga.

Ljóst er að verkefni stjórnvalda viðvíkjandi netöryggi skarast í mörgum tilvikum enda er netöryggi þverlægt viðfangsefni stjórnkerfisins í heild. Því er eðlilegt að leggja áherslu á samvinnu og samhæfingu einstakra stjórnvalda á þessu sviði, sbr. m.a. 2. mgr. 5. gr. og 18. gr. laga nr. 78/2019. Slík samvinna er t.a.m. óhjákvæmileg þegar sama netógnin steðjar að ólíkum mikilvægum innviðum eða aðilum. Þegar svo háttar til geta nákvæm hlutverka- og ábyrgðarskil þurft að víkja fyrir skilvirkri samvinnu viðkomandi stjórnvalda. Því er ákjósanlegt að við innleiðingu nýrra ESB-gerða á sviði netöryggis sé tryggt að lagagrundvöllur samstarfs milli viðkomandi stjórnvalda sé skýr og ótvíræður.

Þá er eðlilegt við reglusetningu að hafa í huga að netöryggisgerðir ESB, þ.m.t. NIS, takmarka ekki svigrúm aðildarríkja til að setja reglur um grundvallar öryggishagsmuni sína, t.d. þjóðaröryggi og öryggis- og varnarmál. Því verða slíkir þættir almennt útfærðir sjálfstætt í íslenskum lögum og til viðbótar lágmarksreglum NIS o.fl. Það er því ljóst að innleiðing þeirra ESB-gerða nægir ekki ein og sér til að taka á net- og upplýsinga-öryggisáskorunum tengdum öryggis- og varnarmálum, eins og netöryggisstefnan gerir ráð fyrir að skuli gert.[90]

Loks skal áréttað að í skýrslu þessari er ekki tekin afstaða til þess hvernig skipan netöryggismála er best fyrir komið í stjórnkerfinu, svo sem hvað varðar verkaskiptingu ráðuneyta og stofnana, heldur er það tilgangur skýrslunnar að lýsa gildandi rétti og draga ályktanir af honum til að veita yfirsýn yfir lagalega hlið málaflokksins.

[90] *Netöryggisstefna Íslands 2022-2037*, bls. 6.

Viðauki - svör við spurningum HVIN um tilgreind atriði (júní 2024)

1. Skörun netöryggis við málaefnasvið ólíkra ráðuneyta og stofnana, m.a. UTN

Samkvæmt gildandi forsetaúrskurði um skiptingu stjórnarmálefna fellur „netöryggi“ undir málefnasvið HVIN. Netöryggi snertir þó óhjákvæmilega málefnasvið ýmissa annarra ráðuneyta og stofnana, beint og óbeint. Um það má vísa til ákvæða NIS-laganna nr. 78/2019, en þar er ýmsum ríkisstofnunum, sem heyra undir fleiri en eitt ráðuneyti, falið að gegna hlutverki eftirlitsstjórnvalda hver á sínu sviði, sbr. 11. gr. laganna, að því er varðar netöryggi mikilvægra innviða og stofnana samfélagsins, þar á meðal á sviði orku, samgangna, veitustarfsemi, heilbrigðisþjónustu og fjármálamarkaða. Þá má nefna að CER-tilskipunin (rekstraviðnám mikilvægra aðila) fellur undir málefnasvið DMR, og DORA-tilskipunin (viðnámsþróttur stafræns fjármálamarkaðar) fellur undir málefnasvið FJR. Þótt netöryggi sé þannig þverlægt viðfangsefni ber HVIN stjórnarfarslega ábyrgð á NIS-lögunum og netöryggi sem málaflokki í stjórnkerfinu almennt. Þá heyrir undir HVIN meginstjórnvaldið á sviði net- og fjarskiptaöryggis, Fjarskiptastofa. Af framangreindu leiðir að fyrrnefnd stjórnvöld verða að eiga með sér margvíslegt samstarf við framkvæmd verkefna sem snúa að netöryggi, eftir því sem við á hverju sinni og eins og fyrrnefnd löggjöf gerir beinlínis ráð fyrir að gert skuli í verulegum mæli. Um þetta má að auki nefna ákvæði um samstarf og upplýsingaskipti milli netöryggissveitar og fleiri aðila í reglugerð nr. 480/2021, auk ákvæða reglugerðar nr. 1720/2023 um netöryggisráð, sem á að fylgja eftir framkvæmd stefnu stjórnvalda á sviði net- og upplýsingaöryggis og vera vettvangur upplýsingamiðlunar og samhæfingar á því sviði.

Öryggis- og varnarmál, sem heyra undir UTN, er dæmi um málaflokk sem getur haft snertiflöt við netöryggi. Um framkvæmd öryggis- og varnarmála er fjallað í varnarmálalögum nr. 34/2008. Lögin gilda um stjórnsýslu varnarmála á íslensku yfirráðasvæði og samstarf og samskipti íslenskra stjórnvalda við erlend ríki, hermálayfirvöld og alþjóðastofnanir á sviði öryggis- og varnarmála, sbr. 1. gr. laganna. Með hugtakinu öryggis- og varnarmál er vísað til mála sem snúa að samstarfi Íslands við önnur ríki og alþjóðastofnanir á sviði landvarna, sem og varna gegn öðrum hættum og ógnum sem steðjað geta að íslensku þjóðinni og íslensku forráðasvæði og eiga upptök sín í hinu alþjóðlega samfélagi, sbr. 17. tölulið 5. gr. laganna. Í lögunum er lögð áhersla á

„mikilvægi þess fyrir réttaröryggi borgaranna að aðgreina varnartengd verkefni frá borgaralegum verkefnum á sviði öryggisgæslu og löggæslu“.[91] Þannig er gert ráð fyrir aðskilnaði verkefna á sviði öryggis- og varnarmála frá öðrum verkefnum stjórnvalda sem eru *borgaraleg* í eðli sínu, svo sem löggæslu og almannavarna, sbr. 1. gr. og b-lið 2. gr. laganna. Með því er ætlunin að tryggja og auðvelda lýðræðislegt eftirlit með varnartengdri starfsemi og auka gagnsæi í framkvæmd varnartengdra verkefna.[92]

Á vefsíðu UTN er fjallað um netöryggisógnir sem eina tegund fjölþáttaógna (e. hybrid threats). Þar er m.a. rakið að netöryggi sé „allt í senn tæknilegt og praktískt innanríkismál, þjóðaröryggis- og varnarmál, utanríkis- og efnahagsmál“.[93] Hröð tækniþróun síðustu ára hafi leitt til þess að umfang netöryggismála sem hluta af utanríkis-, öryggis- og varnarmálum ríkja hafi aukist. Á síðustu árum hafi orðið vart við stóraukinn fjölda netárása af hálfu erlendra ríkja eða aðila tengdum ríkjum. Þá er rakið að NATO hafi skilgreint netið sem eitt aðgerðasviða bandalagsins og hafa ríki þess skuldbundið sig til að efla varnir innlendra kerfa og innviða. Þá geti netárás kallað á viðbrögð á grundvelli fimmtu greinar NATO-sáttmálans um sameiginlegar varnir. Geta til að takast á við netárásir sé hins vegar á ábyrgð og forræði hvers ríkis.

Af framangreindu má draga þá ályktun að ákveðnar tegundir netógna séu þess eðlis að þær varði öryggis- og varnarmál í framangreindum skilningi, sbr. málefnasvið UTN. Í settum lögum er þó ekki að finna sértæka afmörkun á því hvers eðlis netógn þurfi að vera til að hún geti talist varða öryggis- og varnarmál. Ályktun um það má þó draga af skilgreiningu varnarmálalaga á hugtakinu öryggis- og varnarmál, þ.e. að um sé að ræða ógn sem á upptök sín í hinu alþjóðlega samfélagi og getur steðjað að íslensku þjóðinni og íslensku forráðasvæði. Telja verður að auknar líkur séu á því að netógn falli undir öryggis- og varnarmál ef talið er að ógnin sé á ábyrgð erlendra stjórnvalda eða aðila sem starfa fyrir erlent ríki eða njóta stuðnings þess á einhvern hátt. Sama á við ef netógn er sérstaklega alvarlegs eðlis, t.d. beinist gegn mikilvægum innviðum eða stofnunum samfélagsins og er til þess fallin að valda miklum samfélagslegum skaða eða veikja áfallaþol samfélagsins. Enn fremur getur hið sama átt við ef ljóst er að tilgangur

[91] Athugasemdir með varnarmálalögum nr. 34/2008.
[92] Athugasemdir með varnarmálalögum nr. 34/2008.
[93] https://www.stjornarradid.is/verkefni/utanrikismal/oryggis-og-varnarmal/fjolthattaognir/

netárásar er pólitískur í eðli sínu, eða henni er gagngert ætlað að grafa undan grunnstoðum samfélagsins, sbr. fjölþáttaógnir.

Á hinn bóginn liggur fyrir að samkvæmt skilgreiningu varnarmálalaga á hugtakinu öryggis- og varnarmál þá falla „borgaralegar ógnir“ utan þess hugtaks. Því má ályktа að venjuleg afbrot sem framin eru fyrir tilstilli netsins snerti að jafnaði ekki öryggis- og varnarmál. Mörkin milli öryggis- og varnarmála í skilningi varnarmálalaga, og verkefna sem varða viðbrögð við „borgaralegum ógnum“, kunna þó að vera háð mati.

Í settum lögum er ekki að finna sértæk fyrirmæli um hlutverk UTN varðandi öryggi gagnvart netógnum sem falla undir svið öryggis- og varnarmála. Á hinn bóginn má ráða af fyrirmælum varnarmálalaga að UTN skuli fylgjast með slíkum netógnum, og vera upplýst um þær, m.a. til að UTN geti sinnt því hlutverki að „skilgreina hættur sem kunna að steðja að íslensku yfirráðasvæði og íslenskum ríkisborgurum“, og miðla upplýsingum þar að lútandi áfram til annarra stjórnvalda og utanríkismálanefndar, eins og ráðgert er í 1. og 3. mgr. 23. gr. varnarmálalaga.

2. Eru samningar um upplýsingasamskipti milli CERT-IS, RLS og UTN nægjanlegir til að tryggja lögmæta miðlun upplýsinga og nægjanlegt samstarf í viðbragði við netöryggisógnum og -atvikum?

Um aðild netöryggissveitar að slíkum upplýsingasamningum má einkum vísa til ákvæða laga nr. 78/2019, laga nr. 70/2022 um fjarskipti og laga nr. 75/2021 um Fjarskiptastofu, auk reglugerðar nr. 480/2021. Í ákvæðum laga nr. 78/2019 og reglugerðar nr. 480/2021 er m.a. gert ráð fyrir ýmiss konar samstarfi og upplýsingaskiptum milli netöryggissveitar og RLS vegna verkefna á sviði netöryggis sem hafa jafnframt snertiflöt við lögbundin verkefni RLS vegna almannavarna. UTN hefur heimild á grundvelli 9. tölul. 7. gr. og 23. gr. varnarmálalaga nr. 34/2008 til samstarfs, úrvinnslu og miðlunar upplýsinga á sviði öryggis- og varnarmála, sbr. einnig reglugerð nr. 959/2012 um vernd trúnaðarupplýsinga o.fl. Í 4. mgr. 20. gr. laga nr. 78/2019 er beinlínis vísað til upplýsinga frá NATO o.fl. sem rennir stoðum undir lögmæti upplýsingaskipta milli stjórnvalda vegna netöryggis í tengslum við framkvæmd öryggis- og varnarmála.

Af framangreindu má draga þá ályktun að gildandi lög og reglur renni nægum stoðum undir lögmæti upplýsingasamninga milli netöryggissveitar, RLS og/eða UTN, að því gættu að framkvæmd þeirra sé í samræmi við ákvæði fyrrgreindra laga og reglna, auk almennra persónuverndarreglna. Gera verður þann almenna fyrirvara hér að ekki liggur fyrir hvernig framkvæmd umræddra samninga er nánar háttað, þar á meðal hvað varðar atviksbundið mat hlutaðeigandi stjórnvalda á lögmæti þess að miðla einstökum tegundum upplýsinga á grundvelli samninganna að teknu tilliti til trúnaðarstigs o.fl. Við mat á því hvort umræddir upplýsingasamningar feli í sér nægilegt samstarf í viðbragði við netöryggisógnum er m.a. rétt að horfa til þess hvort samningarnir tryggi nauðsynlegt flæði upplýsinga milli samningsaðilanna, sbr. einnig umfjöllun um heildarmynd netöryggismála undir lið 3 hér á eftir. Almennt séð leggja samningarnir ekki beinar skyldur á hlutaðeigandi stjórnvöld til að miðla sín á milli upplýsingum sem þýðingu hafa fyrir netöryggi eða viðbrögð við netógnum. Því getur sú staða komið upp að upplýsingar í fórum eins stjórnvalds, sem þýðingu hafa fyrir verkefni annarra stjórnvalda, flæði ekki til hinna síðarnefndu, með þeim afleiðingum að skortur verður á sameiginlegri yfirsýn yfir stöðu netöryggismála. Úr því má eftir atvikum bæta með skýrari samningsákvæðum um gagnkvæmar upplýsingaskyldur aðila og/eða með viðeigandi laga-/reglubreytingum.

3. Eru til staðar nægjanlegar lagaheimildir fyrir eftirlitsstjórnvöld á grundvelli netöryggislaga, eða annarra laga, til að stjórnvöld nái heildstæðri mynd af stöðu netöryggismála, miðla upplýsingum um veikleika eða bresti í netöryggi mikilvægra innviða sín á milli, til samhæfingarstjórnvalds, CERT-IS, RLS, UTN ef slíkir veikleikar eða brestir varða almannahag, þjóðaröryggi eða alþjóðlegar skuldbindingar?

Samkvæmt 6. mgr. 14. gr. NIS-laganna nr. 78/2019 vaktar netöryggissveit og greinir atvik og áhættu tengda öryggi net- og upplýsingakerfa og mótar stöðumynd vegna netógna á hverjum tíma eftir því sem við kann að eiga. Stöðumati skal reglubundið miðlað til netöryggisráðs í samræmi við óskir þess. Nánari fyrirmæli um stöðumat er að finna m.a. í reglugerð nr. 480/2021. Þá er í gildandi lögum og reglugerðum gert ráð fyrir margvíslegu samstarfi og upplýsingamiðlun milli netöryggissveitar, Fjarskiptastofu, eftirlitsstjórnvalda og fleiri stofnana, hvort heldur í fyrirbyggjandi tilgangi eða sem viðbragð við framkomnum netógnum, sbr. einnig umfjöllun undir lið 1 hér að framan.

Af framangreindu fæst ekki séð að lagaheimildir skorti almennt til að stjórnvöld geti miðlað upplýsingum sín á milli um málefni tengd netöryggi. Þó getur það bitnað á heildaryfirsýn yfir málaflokkinn að framkvæmd NIS-laganna gagnvart mismunandi innviðum dreifist á mörg eftirlitsstjórnvöld, til viðbótar Fjarskiptastofu, en vera kann að sum þeirra stjórnvalda búi ekki yfir nauðsynlegri yfirsýn á sínum athafnasviðum eða miðli ekki slíkum upplýsingum til annarra eftirlitsaðila/stjórnvalda með skilvirkum hætti. Það ber þó að nefna að netöryggissveit hefur samkvæmt gildandi lögum víðtækar heimildir til upplýsingaöflunar í þágu hlutverks síns, og getur Fjarskiptastofa vegna netöryggissveitar m.a. óskað eftir að komið skuli á fót sjálfvirkri upplýsingamiðlun á milli kerfa hlutaðeigandi mikilvægra innviða og netöryggissveitar, sbr. 2. mgr. 17. gr. laga nr. 78/2019. Einnig hefur netöryggissveit heimild til að setja á fót samráðs- og sviðshópa, sbr. 18. gr. sömu laga.

4. Hvert er hlutverk UTN/DMR m.t.t. krafna NATO t.d. um áfallaþol fjarskipta. Hvernig skarast það hlutverk á við hlutverk Fjarskiptastofu varðandi öryggi fjarskiptaneta og þjóðaröryggis, og að breyttu breytanda, annarra stjórnvalda eftir því sem við á, svo sem á sviði heilbrigðisþjónustu o.fl.?

Áður hefur verið fjallað um afmörkuð verkefni UTN og DMR sem snerta þann víðfeðma málaflokks sem netöryggi er, sbr. umfjöllun undir lið 1 hér að framan. Fyrir liggur að NATO hefur skilgreint netið sem eitt aðgerðasviða bandalagsins og hafa ríki þess skuldbundið sig til að efla varnir innlendra kerfa og innviða. Í *seven baseline requirements for civil preparedness* frá 2016 er m.a. rætt um markmið um að *„strengthen and enhance, as a matter of priority, the protection of our national infrastructure and networks against the increasing threat and sophistication of cyber-attack“*.[94] Í nánari útfærslu á markmiði nr. 6 sem lýtur að borgaralegum fjarskiptakerfum (Resilient Civil Communications Systems) er ítarlega fjallað um matsþætti sem lúta að netvörnum og viðbragðsgetu í þessu sambandi. Meðal annars er gert ráð fyrir að komið sé á fót vettvangi með aðkomu opinberra og einkaaðila til að skiptast á upplýsingum, auka ástandsvitund og samhæfa viðbrögð (liður c). Þá er lögð áhersla á viðeigandi þjálfun og

[94] Sjá nánari upplýsingar, www.nato.int - What we do – Cyber defence.

álagspróf auk forgangsröðunar og yfirsýnar (liðir d, e og g) svo og að upplýsingamiðlun til viðeigandi NATO-einingar sé í föstum skorðum ef árás er gerð á borgaraleg fjarskiptakerfi sem geta haft áhrif á kjarnaverkefni NATO (liður f). Einnig er fjallað um málsmeðferð til að leggja mat á áhættu sem fylgir erlendu eignarhaldi eða útvistun starfsemi út fyrir landsteinanna (liður h).

Þá má nefna að í grunnstefnu NATO frá 2022 (e. Strategic Concept) er lögð áhersla á mikilvægi þess að aðildarríki dragi úr veikleikum og fækki sviðum þar sem þau eru háð öðrum, þ.m.t. að því er varðar mikilvæga innviði, aðfangakeðjur, orkubirgðir og heilbrigðiskerfi. Þá er varað við því að andstæðingar NATO leitist við að nýta sér það að aðildarríkin eru opin, samtengd og stafræn.

Geta til að takast á við netárásir er á ábyrgð og forræði hvers ríkis, þó að NATO og NATO-ríkin starfi saman og styðji hvert við annað á þessu sviði með ýmsum hætti, m.a. með fræðslu og upplýsingaskiptum. Ekki liggja fyrir upplýsingar um annað en að skipulag netöryggismála hér á landi uppfylli almennt séð þær kröfur sem felast í skuldbindingum ríkisins á grundvelli NATO-samstarfsins. Á hinn bóginn kann að þurfa að taka skýrari afstöðu til þess á hvaða grundvelli Fjarskiptastofa tekur þátt í samvinnu á vegum NATO á sviði netöryggis ef svo ber undir, eftir atvikum samhliða t.d. UTN. Þá er m.a. haft í huga að Fjarskiptastofnun sinnir borgaralegum verkefnum í grunninn, en slík verkefni eru undanskilin hugtakinu öryggis- og varnarmál í varnarmálalögum, sbr. umfjöllun undir lið 1 hér að framan.

Í þjóðaröryggisstefnu og lögum nr. 98/2016 er gengið út frá þeim skilningi á hugtakinu þjóðaröryggi að það vísi til öryggis gagnvart „ógnum sem kynnu að valda borgurum, stjórnkerfum og grunnvirkjum samfélagsins stórfelldum skaða hvort sem það væru innri eða ytri ógnir af mannavöldum eða vegna náttúruhamfara“. Þá taki þjóðaröryggisstefnan til „hnattrænna, samfélagslegra og hernaðarlegra áhættuþátta og felist í virkri utanríkisstefnu, almannaöryggi og varnarsamstarfi við önnur ríki“. Framkvæmd stefnunnar er jafnframt talin kalla á skilvirka samhæfingu hlutaðeigandi ráðuneyta og stofnana sem bera ábyrgð á framkvæmd þjóðaröryggisstefnunnar annars vegar og stefnu í

almannavarna- og öryggismálum hins vegar.[95] Í upphafi þjóðaröryggisstefnunnar er jafnframt tilgreint að Alþingi feli „ríkisstjórninni“ að fylgja stefnunni. Af framangreindu er ljóst að þjóðaröryggismál eru þverlægt viðfangsefni. Meðal áhersluþátta þjóðaröryggisstefnunnar eru stafrænt fullveldi og að auka net- og upplýsingaöryggi á öllum sviðum samfélagsins með samhæfðum aðgerðum, áframhaldandi uppbyggingu á eigin getu og með samstarfi við önnur ríki, auk varna gegn ógnum við stjórnskipun, stjórnkerfi og fjarskipti, þ.m.t. fjarskiptatengingar við útlönd.

Af framangreindu má ráða að hugtakið þjóðaröryggi er afmarkað með nokkuð víðtækum hætti í þjóðaröryggisstefnunni og hefur það skörun við hugtakið öryggis- og varnarmál í varnarmálalögum nr. 34/2008, sbr. umfjöllun undir lið 1 hér að framan. Sömuleiðis má draga þá ályktun að þjóðaröryggi og netöryggi skarast með ýmsum hætti, eins og ráðið verður af fyrrgreindum áhersluþáttum þjóðaröryggisstefnunnar viðvíkjandi net- og upplýsingaöryggi og áfallaþoli samfélagsins. Það gildir m.a. um netöryggi á þeim sviðum sem falla undir NIS-lögin nr. 78/2019, enda lýtur gildissvið þeirra einkum að mikilvægri samfélagslegri og efnahagslegri starfsemi sem felld er undir hugtakið mikilvægir innviðir í lögunum. Með öðrum orðum má færa rök fyrir því að ógnir við netöryggi mikilvægra innviða sé málefni sem snerti þjóðaröryggi, a.m.k. ef ógn er veruleg, svo sem leiðir af efni þjóðaröryggisstefnunnar sjálfrar.

Meðal hlutverka Fjarskiptastofu er að „stuðla að öryggi og viðnámsþrótti fjarskiptainnviða, almanna- og þjóðaröryggi og samhæfðum viðbrögðum við sérstakar aðstæður“, sbr. 2. mgr. 8. gr. laga nr. 75/2021. Lagaákvæðið, sem lögfest var með lögum nr. 17/2022, felur í sér áréttingu á að hlutverk Fjarskiptastofu á sviði netöryggis hafi snertiflöt við þjóðaröryggi í hinum breiða skilningi þjóðaröryggisstefnunnar. Í greinargerð með lögum nr. 17/2022 er áréttað að grundvallarstarfsemi ríkisvaldsins og mikilvægra innviða byggist m.a. á virkni og öryggi fjarskiptaneta og fjarskiptaþjónustu og varði því þjóðaröryggi. Fjarskiptasamband sem varðar varnarmál og fjarskiptasamband við útlönd telst teljist varða þjóðaröryggi. Þá séu almannahagsmunir í fjarskiptum bæði fólgnir í tiltækileika þjónustunnar, ekki síst alþjónustu í fjarskiptum og möguleika til að ná sambandi við neyðarþjónustu, svo og leynd fjarskipta. Þá kemur fram í greinargerðinni

[95] Þjóðaröryggisstefna fyrir Ísland, sbr. einnig greinargerð með lögum nr. 98/2016 um þjóðaröryggisráð.

að þótt eitt meginmarkmið frumvarpsins sem varð að lögum nr. 17/2022 sé að „skýra lagagrundvöll Fjarskiptastofu til yfirsýnar og aðhalds með fjarskiptastarfsemi á forsendum almannahagsmuna og þjóðaröryggis“, sé „ekki um alveg nýjan þátt í starfseminni að ræða“, sbr. gildandi lög um fjarskipti og lög nr. 82/2008 um almannavarnir.[96]

Fjarskiptastofa, þ.m.t. netöryggissveit, leysir framangreind verkefni af hendi að nokkru marki í samstarfi við önnur þau stjórnvöld sem koma að málaflokknum með einum eða öðrum hætti, sbr. umfjöllun undir lið 1 hér að framan. Því er ljóst að skörun er milli hlutverks Fjarskiptastofu og annarra hlutaðeigandi stjórnvalda, þ.m.t. eftirlitsstjórnvalda samkvæmt NIS-lögunum nr. 78/2019, þ.m.t. um netöryggi á sviði orku og heilbrigðisþjónustu. Enn fremur er fyrir hendi skörun milli verkefna Fjarskiptastofu og hlutverks UTN og DMR vegna netöryggis innan málefnasviða þeirra ráðuneyta, sbr. einnig umfjöllun undir lið 1 hér að framan. Ekki liggur fyrir hvort Fjarskiptastofa og/eða önnur þau stjórnvöld sem í hlut eiga hafi sett sér verklagsreglur um samráð/samstarf og/eða valdmörk í tilvikum þar sem skörun virðist vera milli verkefna þeirra á sviði netöryggis, en dæmi eru um slíkar verklagsreglur á öðrum sviðum.[97]

[96] Athugasemdir með lögum nr. 17/2022.

[97] Loks skal áréttað að í skýrslu þessari er ekki tekin afstaða til þess hvernig skipan netöryggismála er best fyrir komið í stjórnkerfinu, svo sem hvað varðar verkaskiptingu ráðuneyta og stofnana, heldur er það tilgangur skýrslunnar að lýsa gildandi rétti og draga ályktanir af honum til að veita yfirsýn yfir lagalega hlið málaflokksins.