23.11.2020

Samantekt samgöngu- og sveitarstjórnarráðuneytis til nefnda Alþingis vegna athugasemda er bárust varðandi 87. grein frumvarps um fjarskipti

Efnisyfirlit

Inngangur

Öryggisáskoranir vegna umbrotstíma í hátæknifjarskiptum

Samfélög nútímans standa nú og á komandi árum frammi fyrir miklum umbrotum sem eiga rætur að rekja til fjarskiptatækni. Samfélögin eru ekki einungis að styðjast við Netið og hátæknifjarskipti, þau eru orðin háð þeim og geta lamast að verulegu leyti án þeirra. Með 5G tækninni er gengið enn lengra í nýtingu þessarar tækni og jafnframt er stigið enn lengra í samþættingu Netsins og fjarskipta, sem verða í æ ríkari mæli háð Netinu. Sú spurning hefur því orðið æ áleitnari í mörgum ríkjum heims, *hversu langt er unnt að ganga í að útvista þekkingu og hlutum miðtaugakerfis eigin samfélags til annarra ríkja*. Alþjóðleg umræða endurspeglar að þetta sé í reynd orðið kjarninn í varnarmálum 21. aldar og þegar þjónusta og búnaður er fenginn erlendis frá, þá þurfi að gera ríkari kröfur um traust en fæst með hlítni við tæknistaðla og vottunum um að skilgreinda tæknilega öryggisgalla sé ekki að finna í viðkomandi búnaði.

Þróun innan Evrópu - Verkfærakistan

Þessi þróun hefur verið mjög áberandi innan Evrópu undanfarin tvö ár og stjórnvöld hafa fylgst grannt með henni[1]. Komið var á fót lokuðum vinnuhópi, *NIS Coordination Group*[2], sem gekkst fyrir könnun meðal Evrópuríkja á stöðu mála varðandi innleiðingu 5G og helstu öryggisógnum sem ríki töldu vera. Skýrsla með niðurstöðum var gefin út og jafnframt boðað að skýrsla með ráðleggingum yrði gefin út. Það var gert 29. janúar 2020, þá var gefin út skýrsla sem hefur verið kölluð ***Verkfærakistan***, (EU Toolbox)[3]. Á fundum eftir að *Verkfærakistan* var gefin út kom fram af hálfu fulltrúa ýmissa smærri ríkja Evrópu að þau hefðu kosið bindandi leiðbeiningar, t.d. í formi tilskipunar eða reglugerðar, frekar en verkfærakistu. Svar stærri ríkja var einfalt, í þessu máli væri verkfærakista frekar við hæfi en bindandi leiðbeiningar frá ESB <u>því öryggi miðtaugakerfis samfélagsins væri eitt helsta öryggis- og varnarmál 21. aldar</u> og það væri <u>á ábyrgð hvers ríkis</u>. Þótt leiðbeiningar verkfærakistunnar séu ekki bindandi og gefi ákveðinn sveigjanleika varðandi útfærslu lausna, þá er þeim fylgt eftir gagnvart ríkjum ESB (og hugsanlega munu þessar kröfum um eftirfylgni einnig síðar ná til EES). Ríkjunum er ætlað að gefa út skýrslur um hvernig brugðist hefur verið við leiðbeiningunum og er miðlæg eftirfylgni því meiri en varðandi ýmsar tilskipanir og reglugerðir sem eru bindandi. Þess má einnig geta að Atlantshafsbandalagið gerir einnig kröfur um að hvert ríki beri ábyrgð á og sinni uppbyggingu og öryggi eigin borgaralegra innviða[4]. Ríki Atlantshafsbandalagsins samþykktu árið 2016 skuldbindingu til að styrkja 7 megininnviði sína (*Seven Baseline Requirements*). Á varnarmálaráðherrafundi bandalagsins í október 2019 var samþykkt uppfærsla á viðmiði bandalagsins um viðnámsþol borgaralegra fjarskiptakerfa aðildarríkja, þar sem 5G fjarskiptakerfi eru tekin með (*Baseline Requirement for Resilient Civil Communication Systems*). Aðildarríki Atlantshafsbandalagsins samþykktu einnig árið 2016 skuldbindingu um netöryggi (e. *Cyber Defence Pledge*)[5], samkvæmt henni gangast öll aðildarríki undir ákveðna skuldbindingar um að efla netöryggi með ýmsum hætti, jafnframt fylgir bandalagið því eftir með virkum hætti að staðið sé við ákvæði skuldbindingarinnar. Að auki hefur öndvegissetur Atlantshafsbandalagsins í netöryggisfræðum í Tallinn gefið út skýrslu um öryggisógnir gegn 5G netum[6],

---

[1] Sem dæmi má nefna að undanfarnar vikur hafa ýmsar evrópskar fjarráðstefnur tengdar öryggi farneta verið sóttar, t.d. Netöryggisráðstefnan í Prag 23.-24. september, *(European) Expert Meeting on 5G* (Þýskalandi), 6. október, *Together – safer, stronger, smarter* (ráðstefna um samvinnu í netöryggismálum, Póllandi) 8. október, *(European) Cybersecurity Conference* (Þýskalandi) 9. nóvember, *5G Techritory* ráðstefnan (Ríga, Lettlandi) 11.-12 nóvember.

[2] https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

[3] Formlegt heiti skjalsins er *EU Toolbox for risk mitigating measures* Skjalið sjálft: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

[4] Sjá t.d. https://www.nato.int/cps/en/natohq/topics_49158.htm

[5] https://www.nato.int/cps/en/natohq/official_texts_133177.htm

[6] *Huawei, 5G, and China as a Security Threat*, https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/

þessi skýrsla hefur haft töluverð áhrif á öryggisumræðu um 5G innan Evrópu og á öryggisúttektina sem *Verkfærakistan* byggir á.

Áherslur Verkfærakistunnar

Samkvæmt leiðbeiningum *Verkfærakistunnar* ber ríkjum að huga að tveimur mismunandi flokkum aðgerða til að efla öryggi 5G kerfa, annars vegar tæknilegum (*technical measures*) og hins vegar öryggisskipulagslegum (*strategic measures*). Þær fyrrnefndu endurspeglast að mestu leyti í tilskipuninni sem nefnd er *Kóðinn*, þær síðarnefndu eru aðgerðir vegna öryggishagsmuna og hafa í sjálfu sér ekkert með fjarskiptatæknina sem slíka að gera. Meginflokkar aðgerða *Verkfærakistunnar* eru:

1. Styrkja öryggiskröfur og eftirlitsstjórnvöld
2. Meta áhættusnið birgja (framleiðenda) og grípa til viðeigandi varúðarráðstafana (þetta gildir jafnt um fjarskiptafyrirtæki sem stjórnvöld)
3. Fjarskiptafyrirtæki reiði sig ekki á búnað frá einum birgi (framleiðanda), heldur hafi stefnu um fjölbreytni.

Tvíræðni öryggishugtaksins

Orðið „öryggi“ er notað í tvenns konar merkingu í frumvarpinu og *Verkfærakistunni* sem það byggir á. Heppilegra hefði verið að geta notað ólík orð. Hér verður reynt að aðgreina þessa merkingu með því að nota svipuð hugtök og í *Verkfærakistunni*:

- ***Tæknilegt öryggi*** – til að takast á við ógnir vegna tækninnar og þar sem beita má tæknilegum lausnum.
- ***Skipulagslegt öryggi*** – til að takast á við ógnir aðrar en þær sem bregðast má við með tæknilegum lausnum eingöngu. Einkum (en ekki eingöngu) er hér um að ræða ógnir af manna völdum, þar á meðal ógnir vegna hugsanlegrar misbeitingar búnaðar. Við slíkum ógnum verður ekki brugðist með tæknilegum lausnum nema að hluta. Þær ógnir sem hér um ræðir falla að mestu undir það sem ríki flokka sem *öryggis- og varnarmál* og lýsingar mótvægisaðgerða eru að verulegu leyti flokkaðar sem trúnaðarmál, enda myndu lýsingarnar annars gagnast þeim sem ógn þykir stafa af.

Tæknileg áhrif viðskiptaþvingana

Í skýrslu starfshóps samgöngu- og sveitastjórnarráðuneytis, utanríkisráðuneytis og dómsmálaráðuneytis um öryggi 5G kerfa sem birt var 11. febrúar 2020 var bent á að viðskiptaþvinganir geti haft áhrif á framleiðendur og birgja. Að mati bresku netöryggisstofnunarinnar NCSC hafa víðtækar viðskiptaþvinganir bandarískra stjórnvalda (ekki síst ákvæði frá í maí 2020) haft alvarleg áhrif á getu kínverskra fyrirtækja til að framleiða farnetsbúnað fyrir 5G, því bannið taki ekki eingöngu til íhluta heldur einnig til nýtingar á hönnun. Endurhönnun eininga í flóknum kerfum gerir öryggisúttektir erfiðari enda byggðar á hönnunarviðmiðum sem gilda ekki um endurhannaðan búnað[7]. Viðskiptaþvinganir bandarískra stjórnvalda leiddu því til þess að bresk stjórnvöld endurskoðuðu áhættumat sitt á Huawei sem birgi og töldu fyrirtækið ekki geta uppfyllt þær öryggiskröfur sem gera yrði til birgis búnaðar í breskum farnetskerfum. Þessi ákvörðun var kynnt 14. júlí 2020 ásamt tilvísuðu mati NCSC. Þann 1. október 2020 gaf bresk stofnun sem sér um tæknilegt eftirlit með nýtingu tækni Huawei í breskum fjarskiptainnviðum út árlega stöðuskýrslu, þessi fjallaði um árið 2019. Gerðar eru alvarlegar athugasemdir við tæknilegar lausnir og rýra eftirfylgni við fyrri ábendingar um þörf úrbóta Þess má geta að í skýrslu varnarmálanefndar breska þingsins um öryggi 5G sem birt var 13. ágúst 2020 var fundið að því að ákvörðun um útilokun Huawei frá breskum farnetskerfum hafi verið tekin á tæknilegum forsendum en ekki stjórnmálalegum. Hér verður ekkert mat lagt á réttmæti niðurstaðna

[7] Sjá almenna samantekt NCSC https://www.ncsc.gov.uk/blog-post/a-different-future-for-telecoms-in-the-uk og tæknilegri greinargerð https://www.ncsc.gov.uk/report/summary-of-ncsc-analysis-of-us-may-2020-sanction

fyrrnefndra greininga, en ljóst er að hér er ekki eingöngu um pólitískt mál að ræða heldur einnig tæknilegt, þótt rætur tæknilegra áhrifa kunni að vera pólitískar, þ.e. viðskiptaþvinganir.

Ný tækifæri vegna breytts tækniumhverfis – „Open RAN" fjölbreytnistefnan

Vaxandi óánægju hefur gætt alþjóðlega með það að þróun 5G tækni sé annars vegar bundin við kínverskt fyrirtæki og hins vegar tvö skandinavísk fyrirtæki. Bæði sé það óásættanleg fákeppni og ýmsum þróuðum tækniríkjum finnst óásættanlegt að eiga enga aðkomu að tæknilegri þróun varnarmála 21. aldar innan eigin lögsögu. Íslensk stjórnvöld hafa fylgst með þessari þróun og aukinni áherslu á nýjar opnari nálganir við hönnun fjarskiptakerfa (kölluð Open RAN stefna[8]), sem gera fleiri framleiðendum kleift að bjóða vélbúnað og hugbúnað við hönnun kerfa, mismunandi einingar frá mismunandi framleiðendum geti unnið saman. Vaxandi stuðningur er alþjóðlega við þessa nálgun og rannsóknasjóðir eru að stórauka fjárveitingar til að stuðla að örum framförum á þessu sviði. Þetta getur aukið samkeppni, hagræði og fjölbreytileika, en jafnframt kallar fjölbreytileikinn á hertari öryggiskröfur. Stór evrópsk fjarskiptafyrirtæki[9] hafa ákveðið að leggja áherslu á Open RAN fjölbreytnistefnuna, en framleiðendur núverandi kerfa[10] hafa bent á að um flókna samhæfingu verði að ræða og gera þurfi enn strangari kröfur vegna þess að mögulegur árásarflötur[11] verði mun stærri. Því hefur þó verið hafnað og bent á að verði fjölbreytnistefnan rétt innleidd með viðeigandi öryggisrannsóknum geti öryggi orðið meira en það sem núverand högun kerfa býður[12] Fjölbreytnistefnan nýtur mikils fylgis, enda er fyrirsjáanlegt að breytt 5G fjarskiptakerfi muni í framtíðinni ekki einungis reiða sig á ýmsan nýjan hátæknibúnað, heldur einnig hugbúnað. Boðaðar hafa verið fjárveitingar úr evrópskum rannsókna- og þróunarsjóðum á þessu sviði[13] og þarna gætu einnig verið tækifæri fyrir íslensk fyrirtæki sem geta lagt áherslu á hátækni og öryggi. Í Bandaríkjunum hefur einnig verið vaxandi áhersla á fjölbreytnistefnuna, enda sjá bæði stjórnvöld og hátæknifyrirtæki mikil tækifæri í því að komast aftur inn á fjarskiptamarkaðinn. Ástæða er því til að ætla að fjölbreytnistefnan muni hafa mikil áhrif í grannríkjum okkar á komandi árum. Þess vegna er mikilvægt að bæði stjórnvöld og fjarskiptafyrirtæki fylgist grannt með tækniþróuninni annars vegar og þeim öryggiskröfum (bæði tæknilegum og skipulagslegum) sem eru að mótast hins vegar, sérstaklega í Evrópu, og að báðar gerðir öryggiskrafna séu teknar með í áhættumat fyrirtækja.

---

[8] *Open RAN policy* á ensku, RAN er skammstöfun á *Radio Access Network*, https://www.openranpolicy.org. Sjá einnig https://www.openranpolicy.org/new-infographic-what-is-open-ran/ varðandi eintalda lýsingu á tæknilegum forsendum stefnunnar.

[9] Til dæmis **Vodafone**, **Deutche Telecom, BT**, **Orange** og fleiri, sjá: https://www.mobileeurope.co.uk/press-wire/15185-tip-shows-open-ran-is-gaining-global-momentum

[10] T.d. Ericsson, sjá „Security considerations of Open RAN", https://www.ericsson.com/4a4b77/assets/local/security/security-considerations-open-ran.pdf og https://www.ericsson.com/en/blog/2020/9/open-ran-security-5g

[11] Þetta er þýðing á enska hugtakinu „attack surface", sem notað er til að lýsa hvernig ráðast megi á kerfi með fjölbreyttari hætti eftir því sem þau verða stærri og samþættari, þá margfaldist iðulega veikleikar þeirra sem má þá nýta betur til árása.

[12] Þetta var t.d. áhersluatriði hjá tæknilegum forstjóra bresku netöryggisstofnunarinnar, NCSC, Dr. Ian Levy, í umræðum á 5G ráðstefnunni í Ríga, 12. nóvember 2020.

[13] Sjá t.d. https://ec.europa.eu/digital-single-market/en/news/europe-boosts-investment-eu70-million-5g-strong-focus-connected-transport-launching-11-new

Viðbrögð við umsögnum um 87. grein frumvarpsins

Í umsögnum virðist almennt ekki gerðar athugasemdir við þann grunn sem 87. grein hvílir á (þ.e. útfærslu samkvæmt leiðbeiningum *Verkfærakistunnar*).

Einnig virðist tekið undir þá lýsingu sem gefin var á fyrirkomulagi annars staðar á Norðurlöndum og í einni umsögn var það jafnvel gert með nákvæmari hætti en gert var í skýringum með frumvarpinu. Hins vegar verður að gera athugasemd við ýmsar ályktanir sem eru eða virðast vera dregnar, t.d. út frá því að sú löggjöf sem umsagnaraðilar hafi skoðað byggi einkum á hlutlægum tækni- og öryggiskröfum. Umfjöllunin virðist einkum taka mið af tæknilegu öryggi, en ekki því skipulagslega sem *Verkfærakistunni* og 87. greininni er einkum ætlað að taka á.

Ekki má horfa fram hjá öryggislöggjöf annarra Norðurlanda, hvernig henni er beitt og hver aðkoma öryggisstofnana viðkomandi ríkis er. Við slíkt mat verður að taka tillit til að slíkar upplýsingar eru að takmörkuðu leyti opinberar. Á Íslandi er hvorki sambærileg öryggislöggjöf við þá sem er annars staðar á Norðurlöndum, né heldur eru hér tæknilegar öryggisstofnanir eins og þar er að finna. Öryggiskröfur sem settar eru fram annars staðar á Norðurlöndum sem samspil fjarskiptalöggjafar og öryggislöggjafar þarf því nú að birta hérlendis innan regluverks fjarskipta.

Texti 87. greinar (og frumvarpsins) í heild snýst um almennar öryggiskröfur til farneta, þeim er ekki beint gegn neinu einu ríki eða framleiðanda. Ekki er um að ræða bann við búnaði frá einstökum ríkjum eða svæðum. Þær öryggiskröfur sem greinin snýst um ganga framar þeim sem lýsa má með einfaldri hlítni við staðla og eftir atvikum úttektum byggðum á þeim (þ.e. tæknilegu öryggi). Slíkar skipulagslegar öryggiskröfur endurspeglast í öðrum greinum frumvarpsins.

- Hér eru til umfjöllunar kröfur sem annars vegar lúta að því almannaöryggissjónarmiði, þeirri grunnkröfu að miðtaugakerfi samfélagsins megi ekki verða of háð búnaði og þjónustu eins birgis (framleiðanda) og geta lamast í heild eða að hluta ef þjónusturof verður. Þetta getur átt rætur að rekja til gjaldþrots eða annarra þátta sem hafa ekkert með tæknilegt öryggi búnaðar að gera en er lykilatriði varðandi rekstraröryggi. Almenn sátt hefur virst vera um þessa kröfu, einnig hjá þeim framleiðendum búnaðar sem eru ríkjandi á íslenskum markaði. Krafa um fjölbreytni búnaðar er einnig ein grunnkrafa Verkfærakistunnar.
- Hins vegar er um að ræða kröfur á grunni þjóðaröryggis og stafrænna varna samfélagsins, Hvaða kröfur um trausta birgja beri að gera til mismunandi hluta kerfis og þá með hliðsjón af hversu mikilvægir þeir eru fyrir öryggi samfélagsins. Hér dugir ekki heldur einföld hlítni við staðla varðandi einstaka hluta kerfis. Beita þarf heildstæðri öryggisnálgun á kerfið í heild og traust til birgja er lykilatriði.

Alls staðar annars staðar á Norðurlöndum (eins og í öðrum ríkjum heims) er gert ráð fyrir einhvers konar aðkomu tæknilegra öryggisstofnana byggðri á öryggislöggjöf viðkomandi ríkis. Það getur verið útfært með almennri öryggislöggjöf sem myndar grunn fyrir samráð fyrirtækja og öryggisstofnana, er að lokum leiðir til ákveðinnar niðurstöðu fyrirtækjanna (eins og í Noregi). Önnur leið er að öryggisstofnanir hafi beina formlega leið að t.d. útgáfu tíðniheimilda á grunni öryggislaga og geti þá jafnvel bannað einstaka framleiðendur (eins og gert hefur verið í Svíþjóð).
Mikilvægt er að átta sig á að jafnvel þótt ýmsar ákvarðanir hafi birst og orðið að fjölmiðlaefni síðustu vikur og mánuði, þá byggir þetta á alþjóðlegri þróun undanfarinna tveggja ára eins og að framan hefur verið rakið. Önnur Norðurlönd hafa verið samstíga í því að leggja stóraukna áherslu á öryggi og lágmarks sjálfræði í að tryggja miðtaugakerfi samfélags framtíðarinnar. Þótt lagalegt umhverfi sé mismunandi til að ná þessu markmiði, þá virðast öll skref hafa verið stigin með það í huga og engin stefnubreyting orðið.

Atriði í 87. grein frumvarps sem fundið er að í umsögnum

Þeir aðilar sem sendu inn umsagnir er snerta 87. grein frumvarpsins eru Samkeppniseftirlitið, Póst- og fjarskiptastofnun, fjarskiptafyrirtæki og einn umboðsmaður framleiðanda búnaðar. Enginn fulltrúi væntanlegra notenda hinnar nýju umbrotakenndu 5G tækni sendi inn umsögn. Það má hugsanlega skýra að hluta með því að Ísland hefur verið í fararbroddi á heimsvísu í ljósleiðaravæðingu landsins og þeirri þörf sem fyrsta fasa 5G-væðingar er ætlað að mæta í öðrum löndum hefur þegar verið mætt með ljósleiðurum hér. Umbreyting iðnaðar og stýringa stjórnkerfis samfélagsins tekur lengri tíma, enda snýst sú umbreyting ekki einungis um fjarskiptahlutann.

Meint útilokun einstakra framleiðenda frá íslenskum farnetskerfum

Í ýmsum umsögnum virðist gengið út frá því að ákvæði 87. greinar leiði til þess að ákveðinn framleiðandi verði útilokaður frá íslenskum farnetsmarkaði og virðist þá einkum horft til 3. mgr. Hvorki í greininni né greinargerð kemur þó fram að það standi til, enda er engu þar beint gegn ákveðnum framleiðanda, ríki né heimssvæði. Hins vegar getur mat á skipulagslegu öryggi samkvæmt 3. mgr. leitt til takmarkana á notkun búnaðar í tilteknum viðkvæmum hlutum fjarskiptakerfis. Slíkar takmarkanir byggja á auknum kröfum um traust til þessa búnaðar, framleiðanda búnaðar og þeirrar þjónustu sem hann veitir. Kröfur um traust vegna skipulagslegs öryggis er auðveldara að formfesta þegar um er að ræða ríki sem Ísland á í öryggissamstarfi við heldur en þegar slíkan grunn skortir. Rétt er að árétta að slíkar kröfur hafa ekkert með tæknilegt öryggi að gera og athugasemd um að gengið sé fyrir fram út frá að búnaður frá slíkum löndum sé (tæknilega) öruggari er því ekki réttmæt. Hugsanlegar takmarkanir byggja ekki á því að eintakir framleiðendur, ríki eða heimssvæði séu sett á svartan lista. Mat á þörf skipulagslegs öryggis getur komið í formi trúnaðarupplýsinga til utanríkisráðuneytis, upplýsinga sem ekki eru veittar sé ekki unnt að tryggja trúnað þeirra. Á grunni þeirra getur utanríkisráðherra veitt umsögn um þessa þörf til samgöngu- og sveitarstjórnarráðherra sem tekur lokaákvörðun í málinu. Ákvörðun í þessu máli krefst því samstöðu þessara tveggja ráðherra og með 4. mgr. á að tryggja að utanríkisráðherra geti miðlað þeim trúnaðarupplýsingum, þar á meðal tæknilegum, sem ákvörðun þarf að byggjast á áfram til samgöngu- og sveitarstjórnarráðherra, sem annars þyrfti að taka ákvörðun án þess að vera í aðstöðu til að kynna sér tæknilegar forsendur málsins. Almennt hafa ríki ákvæði í lögum til að tryggja trúnað um upplýsingar er varða öryggi ríkisins. Slík ákvæði er að finna í íslenskum upplýsingalögum og stjórnsýslulögum. Þar er þó jafnframt að finna ákvæði um að skjóta megi ágreiningi um trúnaðarflokkun til kærunefndar. Á þeim grunni er ekki unnt að tryggja erlendum ríkjum að trúnaður muni ríkja um viðkvæmar tæknilegar upplýsingar sem þau vilji deila með íslenskum stjórnvöldum[14]. Því er 4. mgr. nauðsynleg.

Meint einokun sem afleiðing beitingar 87. greinar og skerðing samkeppnishvata

Athugasemdir voru gerðar um að 87. greinin gæti stuðlað að einokun eins framleiðanda á íslenskum fjarskiptamarkaði (einn aðili tók jafnframt fram að það væri ekkert athugavert við að farnetskerfi á Íslandi væru meira eða minna háð búnaði frá öðrum framleiðanda). Rétt er að benda á að almenn þróun á 5G farnetsmarkaði virðist vera í átt til „Open RAN“ fjölbreytnistefnunnar. Það er sú sýn sem íslensk stjórnvöld horfa til þótt þau ráði litlu um alþjóðlega þróun þessara mála. Stefnan felur í sér mikið uppbrot á framleiðslu 5G búnaðar og gefur mörgum framleiðendum vél- og hugbúnaðar kost á að vera með, hugsanlega einnig á Íslandi. Stefnan felur jafnframt í sér ákveðna ógn við stöðu þeirra beggja framleiðenda sem eru nú ríkjandi á íslenskum farnetsmarkaði. Í 2. mgr. 87 gr. er gerð krafa um fjölbreytni búnaðar. Þetta er í fullu samræmi við framangreinda fjölbreytnistefnu og ein af

[14] Á stjórnarfundi evrópsku netöryggisstofnunarinnar ENISA, 18. – 19. október var t.d. fjallað sérstaklega um þær lagalegur kröfur sem miðlun tæknilegra trúnaðarupplýsinga til og frá stofnuninni þarf að byggjast á, t.d. upplýsingar um dulritunarlykla og fleira.

grunnkröfum *Verkfærakistunnar*. Erlendis verður ekki séð að hún hafi vakið neikvæð viðbrögð (t.d. ekki hjá þeim framleiðendum sem eru ríkjandi hérlendis). Í umsögnum var gerð athugasemd við 2. mgr. og ákvæði hennar þótti of takmarkandi. Í Verkfærakistunni og í löggjöf flestra ríkja er þessari kröfu þó beint að sérhverju fjarskiptafyrirtæki. Stjórnvöldum var vel ljóst að einstök fjarskiptafyrirtæki gætu átt erfitt með að byggja upp kerfi með búnaði frá fleirum en einum framleiðanda. Þess vegna er 87. greinin (með vísan til 78. greinar) útfærð þannig að fjölbreytnikrafan gildi um farnet á Íslandi í heild og að henni sé ekki beint gegn einstökum fyrirtækjum. Jafnframt að hún sé ekki afturvirk heldur taki til uppsetningar á nýjum búnaði. Krafa um fjölbreytni og væntanlega þróun markaðar á grunni fjölbreytnistefnunnar eru því hvorki áfangar til einokunar né skerðingar samkeppnishvata.

Meintur skortur á gagnsæi og skýrum viðmiðum í kröfum 87. greinar

Í ýmsum umsögnum er minnst á að öryggiskröfur þurfi að vera skýrar og það þurfi að skilgreina með ítarlegum hætti hvaða öryggishagsmuni sé verið að vernda. Þetta eru skiljanleg sjónarmið, en hafa verður í huga að iðulega ríkir ákveðinn trúnaður um skipulagslegar öryggisráðstafanir (ólíkt þeim tæknilegu) sem ætlað er að vernda öryggi ríkis og samfélags gegn mannlegum ógnum. Sá grunnur sem byggt er á er þó skýr, það er fyrst og fremst *Verkfærakistan* svokallaða og hvernig önnur ríki á Evrópska efnahagssvæðinu hafa beitt henni. Þar er fjallað ítarlega um áhættugreiningu sem þurfi að gera og síðan til hvaða aðgerða þurfi að grípa, bæði til að taka á tæknilegum ógnum og skipulagslegum.

Spurningar geta einnig skiljanlega vaknað varðandi hvernig skuli skilgreina *viðkvæma hluta kerfa*. Póst- og fjarskiptastofnun mun koma að þeirri skilgreiningu, en almennt er þá átt við einingar sem hafa ákveðið stjórnunarhlutverk í farnetskerfinu. Þar sem tæknin er nú í örri þróun og hugbúnaður víða að taka við af vélbúnaði í ýmsum kerfishlutum, þá liggur ekki fyrir nú sameiginleg skilgreining Evrópuríkja á hvaða hlutar teljist viðkvæmir. Bretar hafa gefið nokkuð nákvæma lýsingu[15] á nálgun sinni og um áramót er von á nýju bresku fjarskiptafrumvarpi. Boðað er að í því verði nákvæmar skilgreiningar á ýmsum þáttum er snúa að öryggi farnetskerfa og líklegt er að mörg önnur Evrópuríki taki mið með einhverjum hætti af þeim tæknilegu viðmiðum sem þar koma fram.

Rétt er að benda á að tilvísaðar heimildir um kröfur hafa einnig verið aðgengilegar fyrirtækjum og birgjum þeirra og því nýtanlegar við þeirra eigin áhættu- og markaðsgreiningu.

Meintur skortur á fagmennsku í öryggismati og aðkomu hagsmunaaðila að því

Ýmsar umsagnir vísa til þess beint eða óbeint að tryggja þurfi fagmennsku við gerð þeirra umsagna sem ákvörðun samkvæmt 3. mgr. er byggð á og að faglega þekkingu á öryggi farnetskerfa sé að finna hjá fjarskiptafyrirtækjunum og Póst- og fjarskiptastofnun. Þá er greinilega verið að vísa til *tæknilegs öryggis*, ekki þess *skipulagslega*. Það skipulagslega öryggi sem 3. mgr. greinarinnar byggir á er á ábyrgð hvors af þeim tveimur ráðherrum sem þar eru tilgreindir. Viðkomandi ráðherra getur eftir atvikum leitað ráðgjafar við sína umsögn eftir því sem ástæða er til og sama gildir um samgöngu- og sveitastjórnarráðherra sem tekur á móti umsögninni.

[15] Sjá: *NCSC advice on the use of equipment from high risk vendors in UK telecoms networks* (endurskoðað 14. júlí 2020) https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks