RÍKISLÖGREGLUSTJÓRINN
GREININGARDEILD

TÖLVU- og NETGLÆPIR 2016

Skýrslan fjallar um helstu ógnir á sviði tölvu- og netglæpa og skilgreinir mikilvæga samfélagsinnviði í því sambandi.

Áhættu- og ógnarmat

29. mars 2016

Efnisyfirlit

1 Inngangur

Nýting tölvu- og nettækni mótar í síauknum mæli alla tilveru almennings og er um leið ein af grunnstoðum viðskiptalífs á Vesturlöndum. Tækninni fylgja sífellt auknir möguleikar nýsköpunar en um leið geymir hún ógnir við öryggi manna og afkomu. Tölvutækni virðast engin takmörk sett og þar með möguleikum mannsins til að nýta hana til góðs eða ills.

Tölvubyltingin hefur í raun gert manninum kleift að móta og skilja veruleika sinn á nýjan hátt. Nýtt og mikilvægt stig byltingar þessarar blasir nú við sem felst í nýtingu snjalltækja og gervigreindar; hversdagsleg tæki verða í auknum mæli nettengd, fyrirtækjum verður unnt að gjörbreyta samskiptum við viðskiptavini sína og öll upplýsingamiðlun og –skipti taka grundvallarbreytingum. Einstaklingurinn verður sífellt virkari þátttakandi á sviði hinna stafrænu upplýsinga og auðkenna. Af þeim sökum eru upplýsingar í nútímanum æ verðmætari varningur þar sem möguleikum fjölgar til að nýta þær innan hins frjálsa hagkerfis.

En líkt og jafnan þegar verðmæti eru annars vegar ásælast þau margir. Upplýsingar má með margvíslegu móti nýta í ólöglegum tilgangi og í auðgunarskyni; upplýsingum er unnt að stela, þær má selja, nýta sem skiptimynt, sem kúgunartæki, til skemmdarverka, til að ná fram hefndum og með þeim er jafnvel hægt að standa fyrir beinum árásum á mikilvægustu innviði samfélagsins.

Þessi skýrsla um tölvu - og netglæpi er unnin með tilliti til stefnu um net- og upplýsingaöryggi sem innanríkisráðuneytið gaf út í aprílmánuði 2015. Í þeirri stefnu er embætti ríkislögreglustjóra falið að „skilgreina með formlegum hætti helstu ógnir á sviði net- og upplýsingaöryggis og hverjir eru mikilvægir innviðir samfélagsins í því sambandi.“

Við gerð skýrslunnar hefur einkum verið stuðst við upplýsingar Evrópulögreglunnar (Europol), Alþjóðalögreglunnar (Interpol) og spár erlendra fyrirtækja á sviði net- og tölvuöryggis um helstu framtíðarógnir.

2 Útdráttur

Ríkislögreglustjóri hefur á undanförnum árum metið ógnina af tölvuglæpum á Íslandi, umfang þeirra og mögulega þróun auk þess að gefa út viðvaranir til almennings ef tilefni hefur þótt til.

Eitt af markmiðum ríkislögreglustjóra er að efla vitund og þekkingu hjá stofnunum, fyrirtækjum og almenningi á tölvuglæpum og hugsanlegum afleiðingum þeirra. Þessi skýrsla er m.a. hluti af þeirri vitundarvakningu.

Tölvu- og netglæpir hafa áhrif á allt samfélagið þar sem internetið er löngu orðið hluti af hversdagslegu umhverfi nær allra Íslendinga. Tölvu- og netglæpir einskorðast ekki við ákveðna samfélagshópa, þeir geta beinst gegn æðstu stjórn ríkisins, stofnunum, fyrirtækjum og almenningi öllum.

Umfang tölvu- og netglæpa á Vesturlöndum er um flest óþekkt þótt þess hafi verið freistað að leggja mat á þann fjárhagslega skaða sem þeir valda. Þar er um verulegar fjárhæðir að ræða. Illgerlegt er að leggja heildstætt mat á það tjón, þar sem birtingarmyndirnar eru fjölmargar og falla t.a.m. undir kostnað sem fyrirtæki bera í formi búnaðar og mannafla til að koma í veg fyrir innbrot í tölvukerfi og fjársvik af ýmsum toga.

Fyrirliggjandi upplýsingar erlendis frá benda til þess að kostnaður fyrirtækja og hins opinbera vegna tölvu- og netglæpa fari hratt vaxandi. Þann kostnað ber að lokum almenningur á einn veg eða annan. Má því fullyrða að samfélagið allt verði fyrir miklum fjárhagsskaða sökum þessarar starfsemi.

Bankar og fjármálafyrirtæki á Íslandi, sem annars staðar á Vesturlöndum, leggja aukna áherslu á öryggi þeirrar netþjónustu sem haldið er uppi. Samkvæmt þeim heimildum sem greiningardeild eru tiltækar færist tap banka og annarra fjármálafyrirtækja vegna tölvu- og netglæpa í vöxt í nágrannaríkjunum.

Almennt má ganga að því sem vísu að umfang tölvu- og netglæpa aukist í fyrirsjáanlegri framtíð á Íslandi líkt og annars staðar á Vesturlöndum. Notkun á stafrænni samskiptatækni fer stöðugt vaxandi. Sífellt fleiri sækja sér fjármálaþjónustu um internetið og stöðugt fjölgar þeim formum verslunar og viðskipta sem fram fara með stafrænum hætti. Mikill fjöldi fólks býr yfir þeirri þekkingu sem nauðsynleg er til að nýta net- og tölvutækni í glæpsamlegum tilgangi. Ekki þarf

heldur mikla tækniþekkingu til að fremja tölvuglæpi þar sem auðvelt er að kaupa sérsniðnar árásir og lausnir sem miða að því að gera hverjum sem er kleift að fremja tölvu- og netglæpi.

Greiningardeild telur brýnt að bæta menntun og fræðslu fyrir lögreglumenn varðandi tölvu- og netglæpi svo og að bæta aðgengi lögreglu að sérfræðiþekkingu og samvinnu við fagaðila í málum sem varða þennan flokk afbrota.

Stjórnvöld hafa brugðist við auknum kröfum í net- og tölvuöryggismálum með margvíslegum hætti. Öryggi mikilvægra innviða samfélagsins tengist net- og tölvuöryggi. Í skýrslunni eru mikilvægir innviðir settir í samhengi við upplýsinga- og netöryggi og farið yfir nokkrar sviðsmyndir í því samhengi. Í kafla 9.4 er áhættustigið varðandi árás á fjarskipta, net og upplýsingakerfi metið. Niðurstaðan er sú að litlar líkur eru taldar á stórárásum tölvu- og netglæpamanna á fjarskipta, net og upplýsingakerfi en afleiðingar slíkrar árásar væru í heild miklar eða mjög miklar.

3 Tölvu- og netglæpir

Helstu tegundir tölvuglæpa eru:

1. Þjófnaður á persónuauðkennum.
2. Fjársvik og tilraunir til blekkinga í hagnaðarskyni.
3. Ofbeldi gegn börnum á internetinu.
4. Tölvuinnbrot – „tölvuhakkarar“, aðgerðahópar, dulkóðun á gögnum.
5. Tölvuárásir – dreifðar netárásir/neitun á þjónustu (e. DDoS[1]), ruslpóstur, skemmdarverk, afskræmingar vefsíðna.
6. Árásir á samfélagsinnviði og mikilvægustu stofnanir með notkun spilliforrita/vírusa.
7. Njósnir og/eða stuldur á hugverkaréttindum.

Þróunin á sviði tölvu- og netglæpa er sérlega hröð. Sífellt koma fram nýjar og iðulega háþróaðar aðferðir til að fremja slíka glæpi og hugviti manna á þessu sviði virðast litlar skorður settar. Almennt skortir upplýsingar um umfang tölvu- og netglæpa. Kann þar að ráða einhverju hversu viðamikil þessi tegund glæpastarfsemi er og einnig vegur sú staðreynd þungt að mikill fjöldi brota

[1] Slíkar árásir má einnig nefna „álagsárásir“.

Tölvu- og netglæpir

Með hugtakinu „tölvu- og netglæpir“ er átt við afbrot einstaklinga eða skipulagða brotastarfsemi sem ýmist beinist gegn stafrænum upplýsinga- og miðlunarkerfum eða fer fram með því að nýta þau sömu kerfi.

Á Norðurlöndum er iðulega talað um „IKT-kriminalitet“ (þ.e. Informasjons- og kommunikasjonsteknologi) þegar fjallað er um þess háttar brotastarfsemi auk þess sem þekkt eru hin alþjóðlegu heiti „Computer Crime“ og „Cybercrime“.

er ekki tilkynntur lögreglu. Skipulagðir brotahópar koma í auknum mæli að tölvu- og netglæpum og eiga þeir auðvelt aðgengi að sérfræðiþekkingu.

Tölvu- og netglæpir eru síður en svo bundnir við skipulagða glæpahópa, þannig eru dæmi um unga áhugamenn sem gera tölvuárásir frá heimilum sínum, kaffihúsum eða öðrum stöðum þar sem auðveldlega má tengjast internetinu. „Brotavettvangurinn“ er því iðulega óljós og margvíslegur ekki síður en sjálft viðfang afbrotsins. Þannig er t.d. tölvuinnbrot í eðli sínu ólíkt hefðbundnu innbroti þar sem vettvangur brotsins er þekktur og afmarkaður. Í tilviki tölvuinnbrots getur afbrotamaðurinn verið staddur í annarri heimsálfu þar sem lagaumgjörð er önnur.

Tæknin hefur getið af sér nýjan hóp afbrotamanna, tölvu- og netglæpamenn, sem margir hverjir eru lögreglu ósýnilegir þar til þeir láta til skarar skríða.

Mikilvægt er að hafa í huga að ekki er þörf á mikilli tölvuþekkingu til að fremja tölvubrot; í mörgum tilvikum er unnt að kaupa án teljandi fyrirhafnar þá þekkingu sem nauðsynleg er og sömuleiðis menn til einstakra verka.

Um marga alvarlega brotaflokka sem fjallað er um í þessari skýrslu gildir að internetið og tölvutæknin hafa í senn skapað nýja möguleika við sjálfa framkvæmd afbrotanna og gefið þeim nýtt form. Sem dæmi um þetta má nefna að internetið hefur getið af sér nýja tegund ofbeldis gegn börnum.

Á vettvangi Alþjóðalögreglunnar (Interpol) og Evrópulögreglunnar (Europol) er nú lögð stöðugt þyngri áhersla á baráttu gegn tölvu- og netglæpum. Það helst í hendur við þróun undanliðinna ára; aukin umsvif tölvu- og netglæpamanna eru talin eitt erfiðasta verkefni lögregluliða á Vesturlöndum. Tölvu- og netglæpir tengjast flestum brotaflokkum t.a.m. skipulagðri glæpastarfsemi, ofbeldi gegn börnum, hryðjuverkum, fíkniefnaviðskiptum, vopnasölu og

peningaþvætti. Þeim fylgir einnig aukin þörf fyrir alþjóðlega samvinnu á sviði löggæslu líkt og áherslur Interpol og Europol eru til marks um.

Auk þeirra birtingarmynda tölvu- og netglæpa sem hér hefur verið fjallað um veitir tölvutæknin færi á margs konar annarri afbrotastarfsemi. Henni er beitt við sölu og dreifingu fíkniefna; internetið er að auki nýtt til hótana og fjárkúgana, fjársvika og peningaþvættis, greiðslukorta-þjófnaða og annars konar þjófnaða á persónuupplýsingum og -auðkennum, sölu á þýfi, leit að „burðardýrum“ fyrir fíkniefni og mögulegum fórnarlömbum með tilliti til mansals. Um internetið er unnt að stela hugverkum, trúnaðarupplýsingum, hönnun og teikningum, halda uppi iðnaðarnjósnum og síðast en ekki síst geta brotamenn og –hópar nýtt þessa tækni til að auðvelda samstarf sitt og samskipti.

Internetið má nýta til árása á tölvukerfi fyrirtækja og stofnana í því skyni að skerða eða jafnvel lama starfsemi og/eða þjónustu þeirra. Svonefndir „hakkarar“ geta valdið miklum usla með innbrotum í tölvukerfi eða beinum árásum gegn þeim. Ljóst er að slíkar árásir gætu talist til hryðjuverka yrðu tölvukerfi sem lúta að mikilvægustu innviðum og stoðkerfum samfélagsins t.a.m. raforkumiðlun gerð óstarfhæf.

Umfang tölvubrota á Vesturlöndum er um flest óþekkt þótt þess hafi verið freistað að leggja mat á þann fjárhagslega skaða sem þeir valda. Þar er um miklar fjárhæðir að ræða. Ljóst er að illgerlegt er að leggja heildstætt mat á það tjón þar sem birtingarmyndirnar eru fjölmargar og falla t.a.m. undir kostnað sem fyrirtæki bera í formi búnaðar og mannafla til að koma í veg fyrir innbrot í tölvukerfi og fjársvik af öllum toga. Í skýrslu Sameinuðu þjóðanna frá árinu 2013 sem nefnist „Comprehensive Study on Cybercrime“ kemur fram að vera kunni að allt að 80% tölvubrota séu ekki kærð til lögreglu.

Tilkoma internetsins hefur skapað fjölmörg ný tækifæri til samskipta. Það hefur leitt til öflugrar atvinnu- og frumkvöðlastarfsemi og hjálpað til við að byggja ný samfélög og samskiptamáta sem ómögulegt var að ímynda sér fyrir tveimur áratugum eða svo. Sumir þeirra nýju samskiptamáta gera kleift að fela persónuauðkenni og staðsetningu þeirra sem eiga í samskiptum. Þannig er unnt að starfa nafnlaust á internetinu og t.a.m. miðla upplýsingum og fjármagni. Umhverfið á internetinu þar sem slík nafnlaus samskipti eiga sér stað kallast almennt „Darknet“ sem í þessari skýrslu verða nefnd huldunet.

Nafnleynd á internetinu hefur sérstakt aðdráttarafl fyrir glæpamenn og á undanförnum árum hefur glæpastarfsemi á huldunetum aukist til muna. Þetta á m.a. við um hátækniglæpi en jafnframt færist í vöxt að hefðbundnari glæpir s.s. viðskipti með ólögleg lyf og fíkniefni, falsaðar persónuupplýsingar og -skilríki og vopn fari fram í krafti nafnleysis á internetinu.

Huldunetin (e. darknets) sem fjallað er um í þessari skýrslu eru þau sem veita kaupendum og seljendum ólöglegrar vöru og/eða þjónustu nafnleynd. Til þess að ná fram leynd á staðsetningu og nafni eru internet-samskiptin flutt á milli fjölda mismunandi staðsetningapunkta (netþjóna/tölva) og samskiptaslóðinni eytt jafnóðum. Þetta kemur í veg fyrir að hægt sé að rekja upphafsstaðinn. Góð dæmi um slík netkerfi eru TOR (The Onion Router) og I2P (Invisible Internet Project).

Vandi lögreglunnar er ekki nafnleysið eitt og sér í samskiptum á huldunetum. Góðar, gildar og réttmætar ástæður geta verið fyrir því að fólk velur nafnleynd í samskiptum sín á milli. Má þar t.d. nefna réttinn til friðhelgi einkalífsins svo og tjáningarfrelsið. Skýrar vísbendingar eru um að notkun nafnlausra samskiptakerfa hafi aukist mjög eftir ágúst 2013 og helst það meðal annars í hendur við uppljóstranir um stórtæka söfnun erlendra ríkja og ákveðinna stofnana á þeirra vegum á rafrænum upplýsingum og nýtingu þeirra við eftirlit og hryðjuverkavarnir.

Huldunet (e. darknet)

Það sem almennir notendur verða venjulega varir við á internetinu er aðeins lítill hluti þess. Þetta er hinn opni hluti sem er efnisskráður og leitarvélar eins og Google geta flett upp og birt skráninguna. Sá hluti sem hefur ekki verið skráður á þann veg er kallaður „Deep Web“ eða „djúpvefurinn.“ Á honum er fjöldi stórra gagnagrunna, bókasöfn og vefsíður sem krefjast innskráningar frá viðurkenndum notendum. Huldunet eru hluti af djúpvefnum í þeim skilningi að beita verður sérstökum ráðstöfunum til að tengjast þeim. Flest huldunet þurfa sérstakan hugbúnað svo hægt sé að hafa samskipti innan þeirra. Það er m.a. ástæða þess að venjulegar leitarvélar geta ekki sótt upplýsingar um þau og hvers vegna þau eru falin þeim notendum sem ekki hafa hlaðið niður nauðsynlegum hugbúnaði. Hugtakið „huldunet“ vísar þannig til hóps sýndarnetkerfa sem notendur internetsins hafa skapað til þess að eiga í beinum millliliðalausum samskiptum með leynd og yfirleitt með nafnleysi. Sum þessara hulduneta er tiltölulega auðvelt að nálgast því hugbúnaðurinn sem krafist er til að nota þau stendur til boða á internetinu endurgjaldslaust.

Vandi löggæslunnar er sá að glæpamenn misnota nafnleysið. Í raun má segja að myndast hafi glæpamarkaður á netinu þar sem alls kyns ólögleg starfsemi er í boði. Þar á meðal viðskipti með ólögleg lyf og fíkniefni, sala á vopnum og stolnum vörum, ofbeldi gegn börnum, leigumorð, mansal og sala á stolnum greiðsluupplýsingum. Einnig stendur til boða að kaupa sem þjónustu fjölda tölvu- og netglæpa svo sem klæðskerasniðnar tölvuárásir á einstaklinga eða fyrirtæki/stofnanir (DDoS-árásir, lykilorðaþjófnaður, ruslpóstur o.fl.). Glæpamarkaðurinn á internetinu hefur tekið upp nafnlaust greiðslufyrirkomulag sem felst m.a. í rafrænni mynt þar sem bitcoin rafmyntin er sennilega best þekkt. Peningaþvætti stendur einnig til boða á internetinu.

Auk þess sem huldunetin geta þjónað glæpamönnum sem öruggur vettvangur brotastarfsemi veita þau einnig annars konar óæskilegum samskiptum öruggt skjól.

Á huldunetum geta menn hvaðanæva að úr heiminum með alls kyns fyrirætlanir og stundum glæpsamlegar hist, rætt saman og skipst á upplýsingum, hugsunum og reynslu á ýmsum sviðum afbrota svo sem ofbeldi gegn börnum og konum, hryðjuverk og öfgastarfsemi.

Um leið skapast grundvöllur til að ná til fleiri einstaklinga og þar með „normalísera“ eigin hegðun og hneigðir. Sem dæmi má nefna að á síðustu árum hafa iðulega vakið athygli mál varðandi myndbirtingar af ungum íslenskum stúlkum á erlendum netsíðum.

Löggæslustofnanir á borð við Interpol og Europol leggja aukna áherslu á varnir gegn og viðbrögð við tölvuglæpum. Þess er að vænta að aukin áhersla verði lögð á alþjóðlegt samstarf og samræmingu á þessu sviði löggæslunnar. Í iOCTA-skýrslum Europol 2014 og 2015 (e. Internet Organized Crime Threat Assessment) kemur fram að tölvuglæpir krefjist nýrrar nálgunar lögreglu. Sú nálgun kalli m.a. á mun öflugri alþjóðlega

Notkun hulduneta við brotastarfsemi

Erfitt er að meta umfang og áhrif notkunar á huldunetum í brotastarfsemi.

Í júlí 2013 voru um 800.000 notendur á dag á TOR-netkerfinu um allan heim. Fjöldi daglegra notenda var um 2,5 milljónir árið 2014 þar af voru um 30% búsett innan Evrópusambandsins (ESB).

Þann 30 júní 2014 voru 7.707 síður auðkenndar á TOR- netinu og 621 síða á I2P netinu. Frá 25. júní – 30. júní 2014 höfðu 1.502 þessara netþjónusta verið virkar á netinu.

Af þessum 1.500 síðum tengdust 292 misnotkun á börnum, 279 tengdust eiturlyfjum, 204 tengdust greiðslukortum, 133 tengdust fölsuðum vörum, 105 tengdust „tölvuinnbrotum“ (e. hacking), 83 tengdust vopnum, 72 tengdust svikum, 60 tengdust DDoS árásum, 18 tengdust fölsuðum auðkennis-skilríkjum og hryðjuverkum og átta síður tengdust „upplýsingaveiðum“ (e. phishing).

samvinnu lögregluliða. Evrópska tölvu- og netglæpamiðstöðin (e. European Cybercrime Center) sem Europol starfrækir er talin ágæt fyrirmynd að slíkri samvinnu lögregluliða.

Baráttan gegn tölvuglæpum krefst annarrar nálgunar lögreglu frá þeirri sem tíðkast hefur varðandi flesta „hefðbundna“ glæpi. Andstætt þeim heimi þar sem glæpamenn þurfa að vera til staðar á vettvangi glæps og geta yfirleitt aðeins framið eitt brot í einu (þ.e. rænt einn banka eða brotist inn í eitt hús í einu), geta glæpamenn á internetinu verið víðs fjarri fórnarlambinu og brotið gegn fjölda manna víðs vegar um heiminn með lítilli fyrirhöfn og áhættu í skjóli nafnleyndar og veikrar lagaumgjarðar.

Í mörgum ríkjum utan Vesturlanda er ekki fyrir hendi fullnægjandi lagaleg umgjörð til að tryggja skilvirka samvinnu á sviði lögæslu og dómstóla. Staðreyndin er sú að rannsóknaraðferðir lögreglu miðast við þjóðríkið og löggæslu innan landamæra þess sem er á skjön við hið landamæralausa eðli tölvuglæpa.

Samkvæmt skýrslum Europol er munurinn á lögum, lagaumhverfi og rannsóknarúrræðum innan ESB ásamt heimildum til að skiptast á upplýsingum í tengslum við tölvu- og netglæpi jafnvel svo mikill að hann getur valdið hindrunum í samstarfi (iOCTA 2014). Þetta gildir ekki aðeins um löggæslu heldur á þetta einnig við um einkageirann. ESB hefur brugðist við með því að efla lögreglusamvinnu innan Evrópu á sviði baráttunnar gegn tölvu- og netglæpum og meðal annars koma á fót Sameiginlegum aðgerðahóp gegn tölvu- og netglæpum (e. Joint Cybercrime Action Taskforce) auk þess að efla samstarf við einkageirann (iOCTA 2015). Enn vantar þó upp á samræmingu laga innan ESB að mati Europol (iOCTA 2015).

Upplýsingar flæða hindrunarlaust á internetinu til milljóna manna og fyrirtækja. Lögregla býr hins vegar yfir fáum skilvirkum úrræðum til að fá aðgang að upplýsingum í því skyni að finna, og eftir atvikum handtaka, þá glæpamenn sem rýra öryggi almennings og skaða efnahagslega hagsmuni ríkisins og einkaaðila.

Tölvu- og netglæpir eru vaxandi vandi og munu að öllum líkindum halda áfram að aukast að umfangi auk þess sem tækniþróun mun veita ný tækifæri á þessu sviði afbrota. Því þarf að sporna við slíkri starfsemi með heildstæðri nálgun sem nær m.a. til lagaumhverfis og –úrræða, fjármögnunar og eflingar löggæslu.

Á undanförnum misserum virðist sem meiri harka hafi færst í tölvu- og netglæpi og tilvikum fjölgað um beinar hótanir gegn einstaklingum og fyrirtækjum. Þetta á við um DDoS-árásir og fjárkúganir t.d. með dulkóðun gagna í tækjum eða hótun um myndbirtingar af kynferðislegum toga. Telur Europol þessa þróun geta bent til þess að skipulögð glæpasamtök hafi náð fótfestu á þessum vettvangi.

Þróun tölvuglæpa bendir eindregið til verulegrar aukningar bæði hvað varðar umfang, tækni, fjölda og tegundir árása, fjölda fórnarlamba og efnahagslegan skaða.

4 Vaxandi ógnir

Eins og áður sagði er talið að ógnin af tölvu- og netglæpum fari vaxandi á Íslandi líkt og annars staðar á Vesturlöndum. Í skýrslum tölvuöryggisfyrirtækja auk skýrslna Europol um tölvu- og netglæpi eru helstu ógnir næstu ára taldar tengjast þeirri staðreynd að slíkir glæpir eru í æ ríkara mæli orðnir að söluvöru á internetinu og jafnvel boðnir sem þjónusta til sölu (e. Crime-as-a-Service, CaaS). Talið er að markaður fyrir slíka starfsemi fari vaxandi og haldi áfram að þróast og verða fullkomnari.

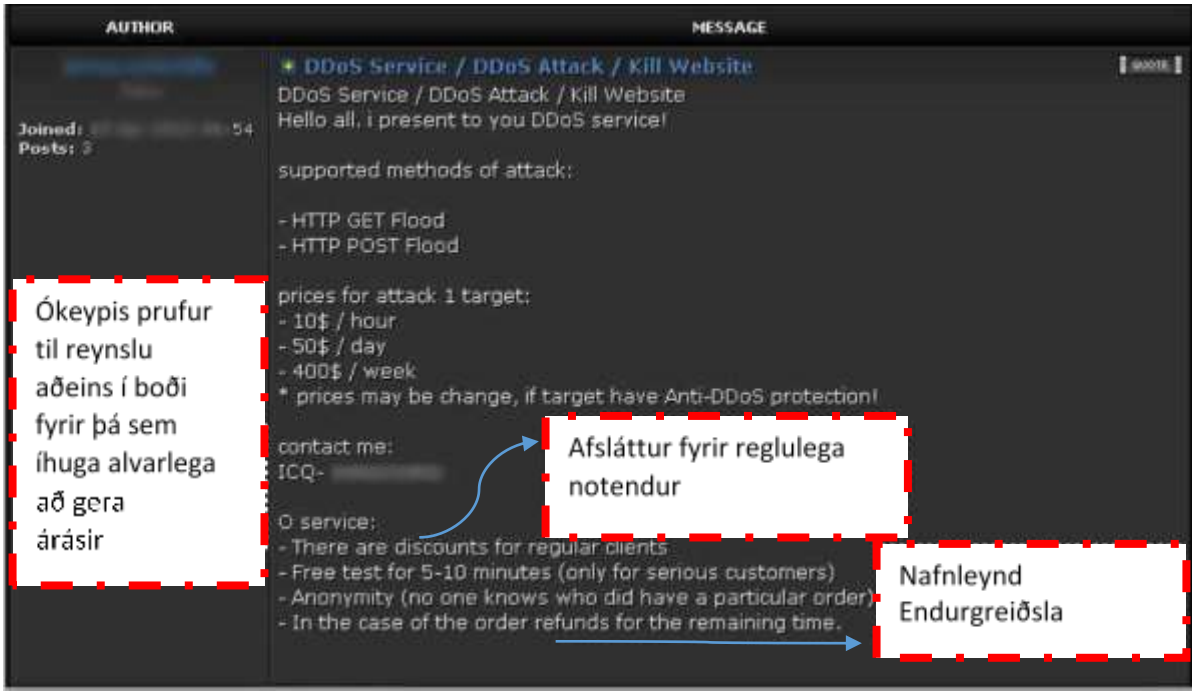
Aukin útbreiðsla og almenn eign á snjallsímum, fartölvum, spjaldtölvum og ýmsum snjalltækjum sem notuð eru í daglegu lífi og starfi er talin gefa glæpamönnum aukin tækifæri til að ráðast á og hagnýta þá veikleika sem þar kunna að finnast. Er það mat sérfræðinga í tölvu- og netöryggismálum að glæpamenn sækist eftir aukinni skilvirkni í tölvu- og netglæpum þ.e. meiri hagnaði í hvert skipti. Þetta er talið geta leitt til fjölgunar stórra árása á fjármálafyrirtæki og stóra söluaðila á netinu. Líklegt er talið að tölvuárásir verði þróaðri og nákvæmari og að tölvuglæpamenn muni leggja aukna áherslu á að þróa enn frekar „sálfræðina“ (e. social engineering) í afbrotum sínum.

4.1 Glæpir sem þjónusta

Net- og tölvuglæpir sem þjónusta til sölu (e. Crime-as-a-Service, CaaS); markaður fyrir slíka starfsemi fer vaxandi og heldur áfram að þróast og verða fullkomnari.

Tvö atriði í þróun tölvu- og netglæpa er vert að nefna; annars vegar „Glæpir sem þjónusta“ (e. Crime as a Service, CaaS) og hins vegar „nafnleynd“ (e. anonymisation). „Glæpir sem þjónusta“ er viðskiptaform glæpamanna í stafræna neðanjarðarhagkerfinu þar sem auglýst er til sölu margs konar þjónusta sem auðveldar hverjum sem er að fremja nánast hvaða tegund af tölvubroti sem er. Afbrotamenn geta nokkuð auðveldlega keypt slíka þjónustu sem m.a. felst í að leigja laumunet (e. botnet sjá umfjöllun á bls. 16), gera DDoS-árásir, þróa spilliforrit, stela gögnum og lykilorðum, eða að fremja tölvu- og netglæpi upp á eigin spýtur. Framboð á slíkri „glæpaþjónustu“ hefur gert að verkum að skipulögð glæpastarfsemi hefur í auknum mæli haslað sér völl á sviði tölvu- og netglæpa.

Á myndinni hér að neðan sést skjáskot af síðu sem býður upp á „tölvuglæpi til sölu“.



Sá fjárhagslegi ávinningur sem sérfræðingar í tölvu- og netglæpum hafa af því að bjóða þessa þjónustu örvar markaðssetningu tölvu- og netglæpa og „nýsköpun“ innan þess geira, ef svo má að orði komast, auk þess sem aðferðir til að fremja glæpina verða sífellt fágaðri. Samskipti

glæpamanna sem stunda tölvu- og netglæpi eru oft viðskiptalegs eðlis, standa iðulega yfir í stuttan tíma og geta jafnvel verið tilviljanakennd.

Tækni og hugbúnaður sem veitir nafnleynd er notaður á internetinu, nánar tiltekið á huldunetum, sem gera notendum kleift að miðla gögnum án þess að eiga það á hættu að samskipti þeirra séu rakin. Engan veginn er útilokað að þeir geti myndað samstæðan hóp sem fæst við tiltekin verkefni þó að almennt skorti uppbyggingu og stigveldisskipulag sem einkennir hefðbundna skipulagða glæpastarfsemi, að mati Europol.

Er það mat Evrópulögreglunnar að núverandi skilgreiningar á skipulagðri glæpastarfsemi endurspegli ekki glæpi innan stafræna neðanjarðarhagkerfisins og framganga glæpamanna á internetinu gefi vísbendingar um hvernig alvarlegir glæpir verða skipulagðir í framtíðinni.

Aukin útbreiðsla og almenn eign á snjallsímum, fartölvum, spjaldtölvum og ýmsum snjalltækjum sem notuð eru í daglegu lífi og starfi gefa glæpamönnum aukin tækifæri til að ráðast á og hagnýta þá veikleika sem þar kunna að finnast.

4.2 Aukin útbreiðsla snjalltækja

Árið 2013 var einn milljarður snjallsíma framleiddur í heiminum og á árinu 2015 er talið að um einn og hálfur milljarður slíkra tækja hafi verið settur saman. Glæpamenn eru snarir í snúningum, bregðast hratt við breyttu umhverfi/tækni og hafa þegar þróað aðferðir til að hagnýta veikleika í snjalltækjum.

Menn geyma sífellt meiri upplýsingar í þeim snjalltækjum sem þeir hafa meðferðis. Um leið eru þær upplýsingar persónulegri en áður. Fram til þessa hafa snjallsímar verið tiltölulega öruggir en nú virðist auðvelt að fá mikinn fjölda fólks til að hlaða niður smáforritum sem í raun eru spilliforrit og gefa þar með glæpamönnum aðgang að persónulegum upplýsingum á borð við lykilorð, bankareikningsnúmer, kennitölur o.s.frv. Þetta á augljóslega við um önnur snjalltæki en síma.

Netnotkun Íslendinga er ein hin mesta í Evrópu. Netnotkun hefur nú náð því stigi að nærri allir, 95% hið minnsta, nota internetið. Á árinu 2014 tengdist um helmingur Íslendinga internetinu í gegnum snjallsíma og önnur slík tæki. Ætla má að það hlutfall hafi hækkað á árinu 2015 og muni

enn vaxa 2016. Mjög margir nýta skýjalausnir og önnur geymslusvæði á internetinu til að vista gögn sín.

Hið sama á við um notkun og útbreiðslu samfélagsmiðla (e. social media) á Íslandi. Hún er ein hin mesta í heiminum miðað við höfðatölu. Rúmlega 70% Íslendinga nýta samfélagsmiðla og því fylgir að landsmenn treysta í sífellt auknum mæli á þessa tækni í daglegu lífi og viðskiptum. Facebook var fyrst nefnd til sögu á Íslandi í blaðagrein sem birtist árið 2006. Nú er notkun Facebook orðin slík í landinu að segja má að nær allir landsmenn eldri en 14 ára noti samfélagsmiðilinn.

Fyrirbrigði sem enginn þekkti fyrir tíu árum er nú ráðandi í samskiptum fólks á Íslandi og raunar um heim allan. Þetta dæmi er hollt að hafa í huga þegar leitast er við að móta stefnu í öryggismálum internetsins til langs tíma.
Um 85% íslenskra fyrirtækja hafa eigin vefsvæði og um 35% þeirra bjóða upp á að pöntuð sé þjónusta í gegnum internetið. Um fimmtungur fyrirtækja nýtir samfélagsmiðla við ráðningu starfsfólks og má víst heita að það hlutfall fari hækkandi.

Mikil og almenn notkun internets og snjalltækja á Íslandi felur í sér stóran „snertiflöt“ hvað varðar möguleika glæpamanna og -hópa. Þjóðin er að sönnu fámenn en víst má telja að nær allir landsmenn séu möguleg fórnarlömb tölvu- og netglæpamanna. Frá sjónarhóli glæpamanna má því ætla ástandið á Íslandi skapi mörg tækifæri. Af því leiðir að afar mikilvægt er að efla öryggisvitund almennings.

Snjalltækjavæðing samfélagsins er linnulaus og mun skapa glæpamönnum ný sóknarfæri. Þótt öryggisvitund fólks fari almennt vaxandi hvað tengingar við internetið varðar mun fjölgun snjalltækja í daglegu lífi fólks trúlega skapa glæpamönnum tækifæri til ýmissa afbrota, einkum fjárkúgunar og -svika. Í því samhengi er vert að hafa í huga að stórtækar árásir á mikinn fjölda snjalltækja einstaklinga á sama tíma sýnast heldur fjarlægur möguleiki þar sem stýrikerfi þeirra eru margvísleg og lúta hvorki stöðlun né samræmdri lagasetningu.

Á hinn bóginn eru nú þegar þekkt dæmi þess að nettengd snjalltæki hafi verið yfirtekin af glæpamönnum og þau notuð til að gera t.d. DDoS-árásir á fjármálafyrirtæki. Þannig munu öryggismyndavélar sem hafa sjálfstæða IP-tölu hafa verið yfirteknar og síðan nýttar til slíkra

stórárása um internetið. Aukin snjallvæðing tækja sem fólk notar í daglegu lífi skapar hættu á að þau verði nýtt til t.d. netárása á fyrirtæki og stofnanir.

4.3 Aukið umfang netglæpa

Tölvu- og netglæpamenn sækjast eftir aukinni skilvirkni í afbrotum þ.e. meiri hagnaði í hvert skipti. Þetta er talið geta leitt til fjölgunar stórra árása á fjármálafyrirtæki og stóra söluaðila á internetinu.

Á síðustu misserum hafa tölvu- og netglæpamenn unnið að því að þróa nýjar aðferðir til að stela greiðslukortum/greiðslukortaupplýsingum og komast yfir fé með sviksamlegum hætti. Tölvu- og netglæpamenn virðast hafa aukið árásir á banka, fjármálastofnanir og stórfyrirtæki en dregið úr árásum á einstaklinga. Öflugri laumunet (e. botnet) hafa komið til sögunnar þar sem glæpamenn notast við nafnleysi og huldunet s.s. TOR og I2P. Nú er svo komið að sérhönnuð laumunet eru seld gengjum eða glæpahópum (e. private botnets), einnig er hægt að leigja slík laumunet sem sýnir enn og aftur hvernig tölvu- og netglæpamarkaðurinn reynir stöðugt að færa út kvíarnar.

Árásir á stór fyrirtæki, banka og stofnanir hafa á undanförnum árum færst í aukana. Árásir sem gerðar voru árin 2014 og 2015 sýna svo ekki verður um villst að tölvu- og netglæpamenn leitast við að hámarka gróða með því að stela sem flestum greiðslukortaupplýsingum í einni árás. Í stað þess að eyða tíma í vefveiðar (e. phishing) á einstaklingum reyna tölvu- og netglæpamenn að komast inn í greiðslukerfi stórfyrirtækja eða stofnana þar sem þeir geta stolið upplýsingum um milljónir manna. Sókn íslenskra greiðslumiðlunarfyrirtækja á erlenda markaði getur aukið áhættu að slíkar árásir beinist gegn íslenskum fyrirtækjum.

Svo virðist sem tölvu- og netglæpamenn hafi einnig áhuga á persónulegum gögnum svo sem sjúkraskrám og skrám tryggingafélaga. Með því móti geta glæpamennirnir nálgast fórnarlömb sín á mun persónulegri hátt en ella og þannig fengið viðkomandi til að veita upplýsingar um t.a.m. greiðslukort og bankareikninga. Persónuleg gögn ganga einnig kaupum og sölum í undirheimum tölvuglæpa í sama skyni þ.e. að hafa fé af fólki. T.d. eru greiðslukortaupplýsingar seldar öðrum tölvu- og netglæpamönnum eða notaðar til að kaupa vörur á netinu sem svo eru endurseldar.

Líkur eru á að virkur, svartur markaður fyrir persónuupplýsingar úr ýmsum áttum (frá fyrirtækjum, opinberum aðilum o.s.frv.) skapist á huldunetum. Þannig kunna að verða til eins konar „vöruskemmur“ þar sem hýstar eru persónuupplýsingar af margvíslegum toga sem glæpahópar geta síðan keypt til að nýta í sérhæfðum árásum. Tölvu- og netglæpamenn kunna þannig að koma auga á nýja möguleika til fjárkúgunar.

Laumunet (e. botnet)

Laumunet eru net margra tölva, t.d. heimilistölva, sem sýktar hafa verið með spilliforriti sem gerir tölvu- og netglæpamanni kleift að stýra þeim öllum. Máttur laumuneta getur verið mikill þegar þau stýra mörgum tölvum á víð og dreif um internetið. Hægt er að nota þau til að gera netárásir samtímis frá mörgum stöðum. Kallast slíkt „skert þjónusta með dreifðri netárás“ (e. Distributed Denial of Service attacks - DDoS). Stundum er aðgangur að laumunetum leigður til utanaðkomandi aðila sem vilja fremja glæpi t.d. að koma nýju spilliforriti á markað sem nýtir sér *áður ókunna veikleika* (e. Zero-Day Attack). Ennfremur eru laumunetin notuð til að safna upplýsingum um einstaklinga, svo sem aðgangi að netbönkum. Með þessari tækni er stærstur hluti alls ruslpósts (e. spam) sendur.

Persónuupplýsingar verða sífellt verðmætari vara sem glæpamenn sækjast eftir á internetinu í vaxandi mæli. Greiðslukort missa verðgildi sitt hratt í undirheimum. Kortum geta menn lokað og fengið ný en enginn fær flúið eigin persónueinkenni t.a.m. sjúkra- og fjármálasögu. Þetta kann að skýra aukinn áhuga tölvu- og netglæpamanna á persónuupplýsingum. Á sama tíma fjölgar sífellt þeim tæknilegu lausnum sem nýttar eru til að inna greiðslur af hendi. Allar styðjast þær við persónauðkenni af einhverjum toga. Persónuauðkenni verða því sífellt verðmætari upplýsingar í huga tölvu- og netglæpamanna.

4.4 Nýjar árásaraðferðir

Tölvuárásir verða þróaðri og nákvæmari.

Margir Íslendingar hafa fengið tölvubréf á síðustu misserum sem í fyrstu virðist vera frá viðskiptabanka þar sem viðkomandi er beðinn um að smella á tengil sem færir viðskiptavin bankans á falsað vefsvæði. Þar er farið fram á persónulegar upplýsingar, notendanafn og leyninúmer. Slíkar aðferðir geta jafnvel beinst að einstökum aðilum innan stofnunar eða fyrirtækis

þar sem reynt er að fá viðkomandi til að hlaða niður skjölum sem innhalda trójuhest; sem er spilliforrit sem stelur upplýsingum, skaðar tölvuna eða snjallsíma (fartölvur/spjaldtölvur og önnur snjalltæki). Þegar starfsmaður hefur hlaðið niður skjalinu hefur árásarmaðurinn náð fótfestu innan netkerfis viðkomandi stofnunar eða fyrirtækis.

Á síðastliðnum árum hafa háþróaðar tölvuárásir í mörgum tilvikum byggt á vefveiðum (e. spear phishing) en þær eru ákveðin tegund svika á netinu þar sem einhver reynir að fá notendur til að gefa upp viðkvæmar upplýsingar á borð við aðgangsorð eða kreditkortaupplýsingar. Vefveiðar fara oft fram í gegnum tölvupóst, auglýsingar eða önnur samskipti s.s. vefspjall.

Nú, hins vegar, eru vísbendingar um að „vatnsbólsárásir“ færist í aukana. Slíkar árásir eru gerðar í tveimur áföngum; í fyrsta áfanga er leitað að lögmætri vefsíðu sem starfsmenn þeirrar stofnunar/fyritækis sem ætlunin er að ráðast á heimsækja reglulega þ.e. „vatnsbólið“. Veikleikar þeirrar vefsíðu, þekktir sem óþekktir (e. Zero Day), eru síðan nýttir til að koma spilliforriti þar fyrir sem bíður svo eftir að grunlaus fórnarlömb smelli á tengilinn og hlaði þannig niður trójuhesti.

4.5 Aukin áhersla á „sálræna“ þætti

Tölvu- og netglæpamenn munu leggja aukna áherslu á að þróa enn frekar „sálfræðina“ í afbrotum sínum. Áfram verður viðleitnin sú að skapa ótta hjá fórnarlambinu.

Á síðasta áratug hafa tölvu- og netglæpamenn nýtt hugbúnað til fjárkúgunar um internetið. Tölvum er lokað með dulkóðun um internetið þannig að eigandinn hefur ekki aðgang að gögnum sínum og lausnargjalds er krafist. Þessi fjárkúgunaraðferð er til í ýmsum myndum.

Líklegt er að tölvuglæpamenn hanni nýjar aðferðir við fjárkúgun og taki í auknum mæli mið af einstökum fórnarlömbum sínum hvort sem um einstakling eða fyrirtæki er að ræða. Orðspor er einstaklingum sem fyrirtækjum mikilvægt og hótanir tölvu- og netglæpamanna um að birta viðkvæmar upplýsingar munu reynast áhrifamiklar og ekki síður arðvænlegar fyrir þá sem að baki standa.

Tölvuhakkarar munu að líkindum beina spjótum í vaxandi mæli að stórfyrirtækjum í því skyni að birta upplýsingar sem fyrirtækjunum eru skaðlegar og leiða t.a.m. í ljós vafasama viðskiptahætti

og spillingu. Þessi þróun getur gert öðrum glæpamönnum kleift að beita sömu aðferðum til að komast yfir slíkar upplýsingar og nýta til fjárkúgunar.

Athyglisverðrar þróunar verður vart hvað netauglýsingar varðar. Sífellt færist í vöxt að notendur nýti búnað til að loka fyrir slíkar auglýsingar m.a. vegna hættu á að þær geymi tölvuóværu eða spilliforrit. Tölur frá Bandaríkjunum gefa til kynna mikla fjölgun þeirra sem nota búnað til að loka á netauglýsingar. Hagsmunum þessa lögmæta iðnaðar er því alvarlega ógnað. Því telst líklegt að auglýsendur leiti nýrra leiða til að koma vöru sinni á framfæri á internetinu. Með sama hætti munu netglæpamenn leita nýrra leiða til að nálgast fórnarlömb sín.

5 Tölvu- og netglæpir á Íslandi

Það er mat greiningardeildar að almennt megi ganga að því sem vísu að umfang tölvu- og netglæpa aukist í fyrirsjáanlegri framtíð á Íslandi sem annars staðar á Vesturlöndum. Viðbrögð lögreglu við auknum umsvifum tölvubrotamanna þurfa m.a. að felast í aukinni getu til að bregðast við þeim auk viðleitni til að vekja almenning og stjórnendur fyrirtækja til vitundar um þessa brotastarfsemi.

Tölvu- og netglæpir eru það birtingarform skipulagðrar brotastarfsemi sem líklegast er að beinist gegn almenningi á Íslandi. Þá er m.a. átt við tilraunir til fjársvika um internetið. Ennfremur geta tölvuþrjótar með innbrotum í tölvukerfi komist yfir viðkvæmar upplýsingar sem hugsanlega má nota gegn einstaklingum eða fyrirtækjum og varðað geta mikla hagsmuni líkt og fram kom í tölvuárás á vefsíðu fyrirtækisins Vodafone árið 2013 þegar yfir 70.000 skjölum um viðskiptavini var lekið á internetið. Skjölin munu meðal annars hafa geymt persónuupplýsingar á borð við kennitölur, nöfn, heimilisföng og í einhverjum tilvikum bankaupplýsingar, auk lykilorða.

Þá hafa aðgerðahópar „tölvuhakkara" látið til sín taka á Íslandi með árásum á vefsíður stofnana og fyrirtækja eins og rakið verður nánar hér á eftir.

Þekkt er að hingað til lands hringi aðilar erlendis frá og kynni sig sem starfsmenn alþjóðlegra tölvufyrirtækja. Tilgangurinn er jafnan sá að ginna viðtakandann til að hleypa glæpamanninum inn í tölvu sína í því skyni að komast þannig yfir lykilorð viðkomandi t.a.m. að bankareikningum auk þess sem glæpamaðurinn getur með þessu náð stjórn á tölvu þess sem fyrir afbrotinu verður. Slíkt skapar færi á margvíslegum afbrotum, oftar en ekki fjársvikum.

Íslenska lögreglan hefur ítrekað varað við svonefndum „Nígeríu-bréfum“ sem öll eiga það sameiginlegt að blekkja viðtakandann í því skyni að hafa af honum fé. Ímyndunarafli þeirra sem að þeim bréfasendingum standa virðast engin takmörk sett.

Ofbeldi gegn börnum á internetinu er sú birtingarmynd skipulagðra tölvu- og netglæpa sem hvað mest viðbrögð vekur í samfélaginu og er skilgreint sem tölvubrot samkvæmt hinum alþjóðlega Búdapest-sáttmála. Á undanförnum árum hefur efni sem sýnir gróft ofbeldi gegn börnum ítrekað fundist í tölvum íslenskra ríkisborgara.

Ofbeldi gegn börnum vekur óhug og enginn efi er á því að vilji almennings er sá að barátta gegn slíkri starfsemi njóti forgangs hjá lögreglu. Sala og dreifing á slíku myndefni er iðulega þaulskipulögð, alþjóðleg starfsemi sem fram fer um internetið. Á alþjóðavettvangi ganga sérfræðingar að því sem vísu að þessi starfsemi gefi af sér miklar tekjur.

Lögreglan á höfuðborgarsvæðinu hefur ákveðið að mynda nýja stöðu lögreglumanns sem ætlað er að takast sérstaklega á við hatursglæpi. Hatursglæpur er verknaður sem skilgreinist sem afbrot samkvæmt almennum hegningarlögum.

Í skýrslu ríkislögreglustjóra um hatursglæpi frá júlí 2008 kemur m.a. fram að hatursglæpir séu líklegir til að valda tilfinningalegum og sálrænum skaða. „Fórnarlömb hatursglæpa kunna að upplifa meiri kvíða, reiði, hræðslu, einangrun, öryggisleysi og þunglyndi. Hræðslan og kvíðinn sem hatursglæpir kalla fram ná lengra en til viðkomandi fórnarlambs. Hún nær einnig til fjölskyldu hans og þess hóps eða samfélags sem fórnarlambið tilheyrir. Meðlimum hópsins líður sem brotið hafi verið á þeim auk þess sem þeir eru minntir á að þeir séu varnarlausir og geti orðið fyrir barðinu á samskonar árás.“

Rétt þykir að nefna þróun í kynferðisbrotum sem tengist tæknivæðingu. Þekkt er að menn nýti hina ýmsu samfélagsmiðla til að nálgast ungmenni og fá þau til að bera sig fyrir framan vefmyndavélar eða senda viðkomandi nektarmyndir af sér. Myndunum er dreift á netinu, brotamenn skiptast á þeim og lýsa jafnvel eftir nektarmyndum af tilteknum stúlkum. Samkvæmt rannsókn Hildar Friðriksdóttur félagsfræðings sem greint var frá í byrjun marsmánaðar 2016 er að finna á internetinu þúsundir slíkra mynda af íslenskum stúlkum og eru margar þeirra undir lögaldri (visir.is, 2. mars 2016).

Á þessum vettvangi þekkist einnig svokallað hefndarklám, þar sem einstaklingar skiptast á myndum á internetinu af fyrrverandi mökum sínum eða öðrum, nöktum eða í kynferðislegum athöfnum. Hefndarklám er alvarlegt afbrot þar sem fórnarlömb þess geta beðið skaða af. Nokkur dæmi eru um slík mál hérlendis. Samstarf lögreglu við skólayfirvöld og félagsþjónustu er mikilvægt til þess að sporna gegn þessum brotum.

Markmiðið með dreifingu slíks efnis er þó ekki nauðsynlega jafnan hefnd. Þess þekkjast dæmi á Íslandi að menn hafi tekið upp og selt slíkt myndefni eingöngu í hagnaðarskyni.

Þótt kynferðisbrot tengd tæknivæðingu falli tæpast undir skipulagða brotastarfsemi í hefðbundnum skilningi þess hugtaks þar sem einstaklingar eru yfirleitt að verki en ekki hópur, má líta svo á að innan djúpvefsins (e. deep web) sé skapaður skipulagður vettvangur fyrir miðlun þessa efnis. Einstaklingar sem safnast saman á huldunetum djúpvefsins til að skiptast á og miðla efni mynda þannig jaðarsamfélög sem ýta undir og standa að slíkri dreifingu. Hið sama gildir um hópa sem hafa teygt sig hingað til lands og standa fyrir dreifingu á myndefni sem sýnir börn beitt kynferðislegu ofbeldi. Það að deila upplýsingum felur í sér ákveðið skipulag.

Tilvik þar sem myndefni er notað til kúgana, hvort sem það er til að fá viðkomandi til að samþykkja kynferðislegt samneyti eða láta af hendi fjármuni, geta einnig fallið undir brotastarfsemi sem krefst skipulags. Á síðustu tveimur árum hafa Lögreglunni á höfuðborgarsvæðinu borist tilkynningar um tvö slík mál auk þess sem upplýsingar liggja fyrir um eitt mál sem hefur ekki verið kært til lögreglu. Í öllum tilvikum er um að ræða erlenda aðila sem komist hafa yfir myndefni af viðkomandi og nýtt það til fjárkúgunar.

Íslensk tölvufyrirtæki bjóða vöru og þjónustu sína þ.m.t. hýsingarþjónustu fyrir tölvukerfi á alþjóðamarkaði. Við rannsókn bandarísku alríkislögreglunnar vegna svokallaðs „Silk Road-máls“, sem laut að markaði á hulduneti, kom í ljós að starfsemin var hýst á Íslandi. Fyrirséð er að ólögleg starfsemi haldi áfram á íslenskum upplýsingainnviðum.

Mikilvægt er að komast að hversu umfangsmikil notkun hulduneta er við framkvæmd brota á Íslandi. Jafnframt er mikilvægt að þekking lögreglumanna á tölvu- og netglæpum og viðbrögðum við þeim sé viðunandi. Ljóst er að viðbrögð lögreglu vegna tilkynntra brota þurfa að vera samræmd, fagleg og fylgja skýrum verklagsreglum. Þannig má tryggja góða þjónustu og traust

almennings. Auk þessa þarf lögreglan að búa yfir viðeigandi sérþekkingu á sviði tölvuöryggis eftir starfsvettvangi.

Fyrirliggjandi upplýsingar erlendis frá benda til þess að kostnaður fyrirtækja og hins opinbera vegna tölvubrota fari hratt vaxandi. Þann kostnað ber að lokum almenningur á einn veg eða annan. Má því fullyrða að samfélagið allt verði fyrir gríðarmiklum fjárhagsskaða sökum þessarar starfsemi.

6 Hryðjuverkaógn

Hryðjuverkasamtök nýta internetið í auknum mæli í öllum þáttum starfsemi sinnar. Með tilkomu internetsins hafa öfgafullir einstaklingar og hryðjuverkasamtök greiðan aðgang að almenningi um heim allan. Erlendis færist aukinn þungi í umræðu um nauðsyn þess að lögreglu verði gert kleift að rannsaka tölvunotkun manna sem grunaðir eru um að undirbúa hryðjuverk og/eða hafa tengsl við hryðjuverkasamtök.

Á síðustu misserum hefur athygli manna á Vesturlöndum einna helst beinst að hryðjuverkasamtökunum Ríki íslams, sem leitast við að ná til ungs fólks á Vesturlöndum jafnt í þeim tilgangi að fá viðkomandi að halda til átakasvæða í Mið-Austurlöndum og/eða til að fremja hryðjuverk í eigin heimalandi. Vitað er að hluti þess unga fólks sem gengur til liðs við samtökin hefur kynnst áróðri þeirra á internetinu og í kjölfarið tekið ákvörðun um að fara til Sýrlands/Írak og berjast með Ríki íslams eða framið/ráðgert hryðjuverk til stuðnings samtökunum.

Í skýrslu greiningardeildar sem nefnist „Mat ríkislögreglustjóra á hættu af hryðjuverkum og öðrum stórfelldum árásum“ og birt var í febrúar 2015, segir að internetið og samfélagsmiðlar séu nú meginfarvegur þeirrar boðunar sem öfgamenn halda uppi á Vesturlöndum hvort sem er í nafni trúar eða stjórnmálaskoðana. Aldrei áður hafi svo margir átt greiðan aðgang að boðskap og áróðri herskárra öfgamanna. Í skýrslunni segir meðal annars:

> *„Hryðjuverkasamtök nýta sér internetið til fullnustu. Skiptir þá engu málstaðurinn eða hversu skipulögð starfsemin er. Internetið og samfélagsmiðlar eru nýtt til að skipuleggja aðgerðir, ákveða skotmörk og ná til fólks í þeim tilgangi að fá það til að styðja málstaðinn, jafnvel með því að gangast fyrir hryðjuverki.“*

Að auki eru samfélagsmiðlar nýttir til að halda uppi samskiptum, gefa fyrirskipanir og skapa samkennd með notendum. Fjölgun þeirra einstaklinga í Evrópu sem gerast hallir undir öfgafulla hugmyndafræði eða stjórnmálastefnu er að nokkru leyti rakin til samfélagsmiðla. Það á ekki síst við um einstaklinga sem einir og óstuddir laðast til fylgis við slíka hugmyndafræði (e. self-radicalization). Notkun á internetinu og samfélagsmiðlum í þeim tilgangi að miðla öfgafullri hugmyndafræði er vitaskuld ekki bundin við herskáa íslamista. Hópar sem hatast við innflytjendur og múslima nýta sér einnig tæknina til að koma boðskap sínum á framfæri. Hið sama gildir um aðra öfgamenn.

Slíkar vefsíður eru hýstar víða um heim og m.a. var vefsíðu samtakanna Íslamska ríkið (ISIS) sem hýst hafði verið hér á landi og hafði íslenskt lén lokað í október 2014. Vefurinn nefndist khilafah.is og var skráður á Íslandi í september það ár. Ríkisstjórnir á Vesturlöndum hafa tekið upp samstarf við helstu samfélagsmiðla um að loka fyrir aðgang ISIS og annarra hryðjuverkasamtaka. Er þetta liður í þeirri baráttu sem fram fer á alþjóðavettvangi gegn hryðjuverkaógninni og viðleitni til að hefta áróður slíkra samtaka á internetinu. Í febrúar 2016 hafði t.d. um 125.000 Twitter-reikningum verið lokað frá miðju ári 2015 (guardian.com, 5. febrúar 2016).

7 Aðgerðahópar á internetinu

Hópar „aðgerðasinna“ eða „hakkara“ (e. hactivists) hafa látið til sín taka á síðustu árum. Tölvuárásir slíkra einstaklinga eða hópa hafa vel skilgreind pólitísk markmið (t.d. náttúruvernd, mannréttindi) en hafa ekki hingað til falið í sér beina ógn við almannaöryggi og helstu innviði samfélagsins. Nokkrir forsprakkar slíkra hópa hafa hlotið refsidóma.

Aðgerðahópurinn „Anonymous“ hefur á undanförnum misserum haft í hótunum við íslensk fyrirtæki og stofnanir. Raunar hefur hópurinn lokað um stund vefsíðum íslenskra stjórnvalda (nóvember 2015, janúar 2016) og fyrirtækja með DDoS-árásum. Árásirnar voru gerðar til að mótmæla því að íslensk stjórnvöld heimili hvalveiðar og hefur veitingastöðum sem bjóða fram hvalkjöt verið bætt á lista yfir „skotmörk“ hópsins.

Athygli vekur á hinn bóginn hversu auðveldlega einstaklingar/hópar geta líkt eftir árásum „aðgerðasinna“. Nefna má sem dæmi árásina á Ashley Madison-stefnumótasíðuna sumarið 2015 sem augljóslega var ekki framin í nafni pólitískrar hugmyndafræði. Hópurinn sem þar var að verki

beitti vel þekktum aðferðum hópa á borð við „Anonymous“. Hópurinn krafðist þess að síðunni yrði lokað. Þegar ekki var orðið við þeirri kröfu birti hópurinn afar persónulegar og í sumum tilvikum niðurlægjandi upplýsingar um milljónir manna. Ashley Madison-árásin er dæmi um aðgerð hóps sem felur í sér hótun og kúgun þótt fjármuna sé ekki krafist.

Hvatinn að baki slíkum árásum getur því verið margvíslegur þótt kúgun af einhverjum toga fari jafnan fram. Þá er hugsanlegt að hópur/einstaklingur leitist við að fela hefðbundinn tölvu- og netglæp með því að tengja hann málstað af einhverjum toga. Hugsunin kann að vera sú að valda einfaldlega sem mestum usla og óþægindum. Eins er hugsanlegt að kúgun gagnvart fyrirtæki sé í raun dulin árás samkeppnisaðila.

Slíkar árásir geta, líkt og dæmin sanna, valdið einstaklingum og fyrirtækjum miklum miska, og eftir atvikum fjárhagslegu tjóni, í þeim tilvikum sem birtar eru persónulegar upplýsingar um t.a.m. viðskiptavini.

8 Njósnir og stuldur hugverkaréttinda

Njósnir eru stundaðar af þjóðríkjum, fyrirtækjum og einstaklingum í því skyni að komast að afstöðu og/eða verðmætum annarra. Í vaxandi samkeppni þjóða og fyrirtækja til að tryggja vöxt, aðgang að fjármagni og tækniþróun beita þjóðir og fyrirtæki njósnum í því skyni að öðlast forskot. Þekkingarverðmæti íslenskra stofnana og fyrirtækja eru eftirsóknaverð á alþjóðamarkaði, má sem dæmi nefna hugvit tengt heilbrigðisvísindum og jarðhitafræðum. Mikill hluti þeirrar þekkingar er drifinn áfram af hagnýtingu upplýsingainnviða. Þessi þekkingarverðmæti eru því jafnvel í enn viðkvæmari stöðu en önnur verðmæti gagnvart njósnum/iðnaðarnjósnum sem fara fram í gegnum upplýsingakerfi.

Glati íslenskt atvinnulíf samkeppnisforskoti sem byggir á þekkingu verða efnahagslegar afleiðingar þess neikvæðar jafnt fyrir viðkomandi fyrirtæki og samfélagið allt.

9 Net- og upplýsingaöryggi vegna mikilvægra innviða samfélagsins

Mikilvægir innviðir landsins eru í vaxandi mæli sjálfvirkir og samtengdir (e. interlinked). Þetta skapar nýja veikleika m.t.t. bilunar í tölvubúnaði, bæði hugbúnaði og vélbúnaði sem getur orsakast af mannavöldum, tölvuárásum og náttúruhamförum. Sú altæka tenging sem internetið felur í sér gerir að verkum að skipulagðir hópar jafnt sem einstaklingar geta aflað sér bæði búnaðar og þekkingar til þess að gera tölvuárásir á mikilvæga innviði. Að sögn Evrópulögreglunnar 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. Aukinni nettengingu innviða fylgir þannig aukin áhætta.

Stórfelldar tölvuárásir á mikilvæga innviði eru fátíðar á Vesturlöndum. Með öðrum orðum eru þetta atburðir sem lýsa má sem fátíðum en mjög alvarlegum þ.e. með tilliti til afleiðinga. Þannig má líkja slíkum árásum við náttúruhamfarir.

Þótt árásir séu fátíðar er það mat Evrópulögreglunnar og fleiri sérfræðinga á sviði tölvuöryggis að ógnin sé engu að síður viðvarandi. Í framtíðinni megi búast við auknum árásum á þá aðila sem safna persónuupplýsingum um neytendur og selja þær öðrum (e. data broker). Hið sama gildi um kerfisbúnað og fjarskiptakerfi sem hægt er að ráðast gegn með dreifðri netárás (DDoS) og þannig skerða eða lama þjónustu. Slíkar árásir gætu talist ógn við mikilvæga samfélagsinnviði.

Að auki er sú hætta jafnan til staðar að einstaklingar komist inn í viðkvæm tölvukerfi. Í slíkum tilvikum þarf ekki nauðsynlega að vera á ferð glæpamaður í leit að fjárhagslegum ávinningi; viðkomandi kann að brjótast inn í tölvukerfi einfaldlega vegna þess að hann er fær um það, hann kann að stunda njósnir innan viðkomandi kerfis eða vilja vera innan kerfisins til þess að geta síðar látið til skarar skríða á einn veg eða annan.

Þá er fyrir hendi sá möguleiki að hópar eða einstaklingar ráðist á mikilvæga innviði í því skyni að framfylgja pólitískum markmiðum eða í nafni tiltekins málstaðar. Alvarleg árás af slíkum toga gæti talist hryðjuverk.

Mikilvægustu innviðir samfélagsins hafa fram til þessa ekki vakið áhuga „hefðbundinna“ tölvu- og netglæpamanna. Ástæða þessa er talin sú að þar er ekki fyrir hendi sú hagnaðarvon sem mótar

hefðbundna brotastarfsemi á þessu sviði. Að frátöldum þeim möguleika að glæpamenn kunni að ráðast gegn mikilvægum innviðum í skyni fjárkúgunar eða til að selja aðgangsupplýsingar að stjórnkerfum til áhugasamra er það svo að fjárhagslegur ábati er mun meiri á öðrum sviðum tölvuglæpa.

Af þessu leiðir að fjöldi árása á mikilvæga innviði er og verður mun minni en á önnur „skotmörk“. Tölvu- og netglæpamenn eru mun fleiri en þjóðríki. Ógn við mikilvæga innviði er og verður til staðar en hún mun helst verða bundin við þjóðríki og því verður þessu vopni að öllum líkindum beitt með tilliti til skýrra pólitískra markmiða og stefnu.

Þannig sökuðu stjórnvöld í Úkraínu Rússa um að bera ábyrgð á tölvuárás sem gerð var 23. desember 2015 með þeim afleiðingum að dreifing rafmagns til um 80.000 kaupenda í Úkraínu stöðvaðist í um sex klukkustundir. Að sögn Reuters-fréttastofunnar er þetta fyrsta þekkta tilvik þess að dreifingarnet fyrir raforku sé gert óvirkt með tölvuárás sem talið er að hafi verið framkvæmd með spilliforriti. Samkvæmt tiltækum upplýsingum kallast spilliforrit þetta „BlackEnergy“. Reynist ásakanir stjórnvalda í Úkraínu réttar sýnir árásin að Rússar búa nú yfir talsverðri getu á sviði tölvuárása og almennt sýnir þessi atburður að unnt er að valda beinum skaða á mikilvægum innviðum og búnaði með tölvuárás.

Fjarlægur virðist sá möguleiki að þjóðríki gangist fyrir tilefnislausri tölvuárás á mikilvægustu samfélagsinnviði Íslands. Á hinn bóginn kunna mikilvægustu innviðir að vera „skotmörk“ þjóðríkja í átökum, deilum eða spennuástandi. Á vettvangi Atlantshafsbandalagsins (NATO) er gengið út frá því að stöðugt fari fram tilraunir til að komast inn í netkerfi bandalagsins. Er þá einkum horft til mikilvægra stýrikerfa og njósna.

Möguleg ógn við mikilvægustu inniviði Íslands yrði að öllum líkindum tengd þróun á sviði alþjóðamála; miklu spennuástandi í samskiptum austurs og vesturs eða beinum ófriði. Í því efni yrðu orkukerfi landsins trúlega helsta skotmarkið og á spennutímum er því ráðlegt að líta svo á að sú áhætta sé viðvarandi.

James Clapper, æðsti stjórnandi leyniþjónustustofnana Bandaríkjanna (e. Director of National Intelligence), sagði er hann kom fyrir leyniþjónustunefnd fulltrúadeildar Bandaríkjaþings í september 2015, að í framtíðinni kynnu að færast í vöxt aðgerðir sem miðuðu að því að breyta

fyrirliggjandi stafrænum upplýsingum til þess að spilla réttleika gagna (e. integrity) og þar með réttmæti (e. validity) ákvarðana sem á þeim væru byggðar.

Í máli Clappers kom fram að hann teldi Rússa, Kínverja, Norður-Kóreu og Íran vera þau þjóðríki sem helst ógnuðu Bandaríkjunum á sviði tölvu- og netöryggis. Lýsti hann yfir að herafli Rússa ynni að því að mynda sérhæfða deild til netaðgerða sem miðuðu að því að ná stjórn á mikilvægum innviðum andstæðingsins.

9.1 Tölvuöryggi á Íslandi

Erfitt er að gera grein fyrir umfangi tölvu- og netglæpa, þar sem ætla má (skv. skýrslu SÞ 2013) að mikill fjöldi tölvu- og netglæpa sé ekki kærður til lögreglu.

Rannsóknir á tölvuöryggi á Íslandi (t.d. KPMG 2013, Deloitte 2014) sýna að miklir veikleikar eru til staðar hjá hérlendum fyrirtækjum. Í skýrslu um netöryggismál á Íslandi sem fyrirtækið Wapack Labs gaf út árið 2013 kom fram það mat að ýmsu væri ábótavant í tölvuvörnum landsins. Fyrst nefnir fyrirtækið að CERT-ÍS, netöryggissveit Póst- og fjarskiptastofnunar, sé enn á byrjunarreit og Íslendingar því háðir erlendri sérfræðiþekkingu á þessu sviði. Því sé hugsanlegt að Íslendingar reynist hvorki færir um að bregðast við beinum tölvuárásum né að koma í veg fyrir umfangsmiklar aðgerðir t.d. DDoS-árásir á vegum erlendra þrýstihópa/baráttusamtaka.

Í skýrslunni er fullyrt að Íslendingar hafi þegar orðið fyrir tölvunjósnum sem beinst hafi gegn Alþingi. Hér er vísað til tölvu sem fannst í húsakynnum Alþingis árið 2010 og talið er að nýtt hafi verið til afritunar gagna. Rannsókn lögreglu leiddi ekki til niðurstöðu í því máli.

Miðlægt hlutverk Seðlabanka Íslands í fjármagnsflutningum eftir hrun fjármálakerfisins haustið 2008 er einnig talið skapa hættu á árásum, enda er rafræn greiðslumiðlun burðarás verslunar og þjónustu.

Raunar telja höfundar skýrslunnar að Seðlabanki Íslands sé það skotmark í landinu sem líklegast sé til að draga að sér tölvuglæpamenn. Nefnd eru dæmi um árásir á seðlabanka Bandaríkjanna, Rússlands, Ástralíu og Eistlands. Talið er að Anonymous-samtökin hafi staðið að baki árásinni á bandaríska seðlabankann en líkur hafa verið leiddar að því að Rússar hafi staðið fyrir árásinni á seðlabanka Eistlands.

Ennfremur er í skýrslunni vikið að samskiptum íslenskra og kínverskra fyrirtækja á sviði fjarskipta og bent á fréttir þess efnis að kínverska fyrirtækið Huawei Technologies gæti hugsanlega tengst kínverska stjórnarhernum, nánar tiltekið þeirri deild sem fer með tölvunjósnir.

Þá er vikið að áliðnaðinum á Íslandi og sagt að hann geti orðið fyrir skakkaföllum af völdum samkeppnisaðila, aðgerðarsinnaðra umhverfisverndarmanna (e. environmental hacktivism) auk þess sem ekki verði útilokuð skemmdarverk um internetið (e. cyber sabotage).

Í skýrslunni er varað við þeirri hættu að glæpamenn visti ólöglegt efni á netþjónum á Íslandi eða fremji afbrot á internetinu í skjóli íslenskra laga. Þessu til staðfestingar má nefna að hryðjuverkasamtökin Íslamska ríkið skráðu vefsíðu samtakanna á íslensku léni til skamms tíma þar til því var lokað í október 2014.

Ef ekki er brugðist við viðleitni hryðjuverkasamtaka til að miðla áróðri um internetið getur slík skráning, og eftir atvikum hýsing, augljóslega rýrt traust og skaðað orðspor viðkomandi ríkis í alþjóðlegu samstarfi.

9.2 Stefna stjórnvalda

Stjórnvöld hafa með margvíslegum hætti brugðist við auknum kröfum nútímans í net- og tölvuöryggismálum. Ríkislögreglustjóri ber ábyrgð á að skilgreina ógnir á sviði net- og upplýsingaöryggis og hverjir séu mikilvægir innviðir samfélagsins í því sambandi.

Á undanförnum árum hefur almannavarnadeild embættisins staðið fyrir áhættumati vegna mikilvægra innviða samfélagsins með tilliti til náttúruhamfara. Sú vinna deildarinnar nýtist með ýmsum hætti þegar hugað er að öryggi mikilvægra innviða m.t.t. tölvu- og netárása.

Í stefnu almannavarna- og öryggismálaráðs frá júní 2015 eru mikilvægir innviðir samfélagsins skilgreindir (bls. 36) og þeim skipt í eftirfarandi flokka.

- Fjarskipti, net- og upplýsingakerfi.
- Orkukerfi.
- Heilbrigðisþjónusta.
- Matvæla-, fæðu-, neysluvatns- og fráveitukerfi.

- Löggæsla, viðbúnaðar og neyðarþjónusta.
- Samgöngukerfi.
- Æðsta stjórn ríkisins.
- Fjármálakerfi.

Í stefnunni er lögð áhersla á gerð viðbragðsáætlana um netöryggi og vernd mikilvægra innviða samfélagsins og bent á innbyrðis tengsl atburða er tengjast mikilvægum samfélagsinnviðum. Þar kemur fram að nútímasamfélag er mjög berskjaldað fyrir truflun á fjarskiptum, netöryggi og upplýsingakerfum.

Svo til allir mikilvægir innviðir treysta á stafræn net- og upplýsingakerfi í störfum sínum og rof á þeirri starfsemi getur haft mjög mikil áhrif líf og heilsu íbúa og samfélagslegt öryggi. Því er mikilvægt að treysta áfallaþol almannavarnakerfisins til að takast á við hvers kyns áhættu sem ógnað getur þessum innviðum.

Innanríkisráðuneytið gaf út stefnu um Net- og upplýsingaöryggi í aprílmánuði 2015 og er stefnan hugsuð til ársins 2026. Að auki voru birtar fyrirhugaðar aðgerðir árin 2015–2018 til að ná megi þeirri sýn sem fram er sett í stefnunni. Framtíðarsýnin er sú að:

> *„Íslendingar búi við Net sem þeir geti treyst og þar séu í heiðri höfð mannréttindi, persónuvernd ásamt frelsi til athafna, efnahagslegs ávinnings og framþróunar. Örugg upplýsingatækni sé ein meginstoð hagsældar á Íslandi, studd af öflugri öryggismenningu og traustri löggjöf. Jafnframt sé samfélagið vel búið til að taka á netglæpum, árásum, njósnum og misnotkun persónu- og viðskiptaupplýsinga“.*

Jafnframt eru í net- og upplýsingaöryggisstefnu innanríkisráðuneytisins tilgreind 16 verkefni sem stuðla eiga að bættu net- og upplýsingaöryggi á Íslandi. Þar er m.a. kveðið á um að netöryggisráð skuli móta tillögur til að samræma og innleiða öryggisviðmið og skilgreina kröfur til birgja varðandi upplýsingaöryggi kerfa og þjónustu.

Meginmarkmið sem tilgreind eru í stefnu stjórnvalda eru:

1 **Efld geta**. Almenningur, fyrirtæki og stjórnvöld búi yfir þeirri þekkingu, getu og tækjum sem þarf til að verjast netógnum.

2 **Aukið áfallaþol**. Bætt geta til greiningar, viðbúnaðar og viðbragða eru lykilþættir í bættu áfallaþoli. Áfallaþol upplýsingakerfa samfélagsins og viðbúnaður verði aukinn þannig að hann standist samanburð við áfallaþol upplýsingakerfa á Norðurlöndum. Þetta sé t.d. gert með bættri getu við greiningu á ógnum, samvinnu og með því að öryggi verði órjúfanlegur þáttur í þróun og viðhaldi net- og upplýsingakerfa.

3 **Bætt löggjöf**. Íslensk löggjöf sé í samræmi við alþjóðlegar kröfur og skuldbindingar á sviði netöryggis og persónuverndar. Jafnframt styðji löggjöfin við nýsköpun og uppbyggingu þjónustu sem byggir á öryggi, t.d. hýsingu.

4 **Traust löggæsla**. Lögregla búi yfir eða hafi aðgang að faglegri þekkingu, hæfni og búnaði til að leysa úr málum er varða net- og upplýsingaöryggi.

Í stefnunni segir að hæfni lögreglu til að fást við glæpi tengda net- og upplýsingaöryggi verði bætt með aukinni þekkingu og reynslu ásamt efldri innlendri og alþjóðlegri samvinnu ásamt þeim búnaði sem til þarf.

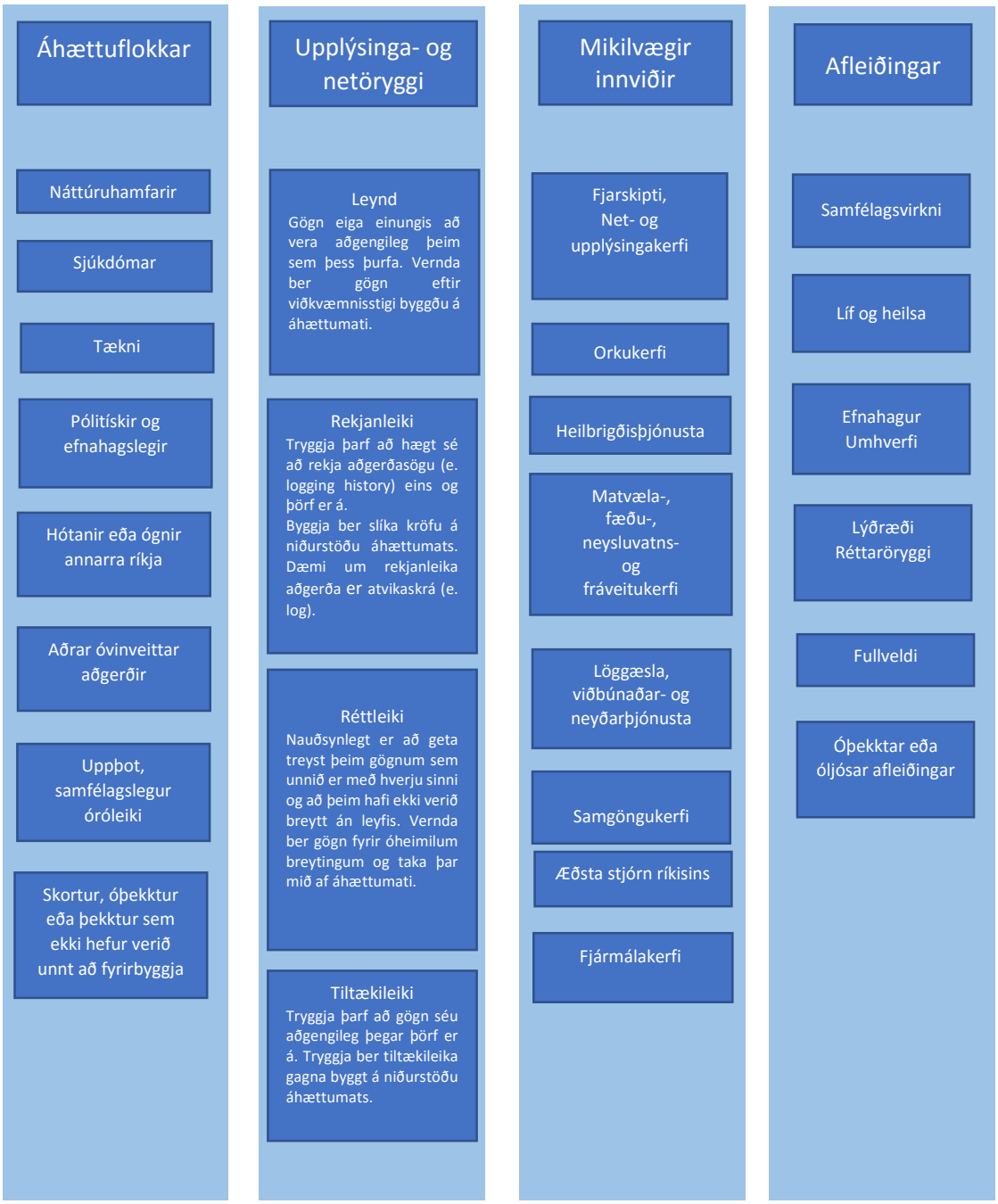
Embætti ríkislögreglustjóra er falið að móta „endurmenntunaráætlun“ til a.m.k. tveggja ára þar sem skipulagt er hvernig uppbygging þekkingar eigi að fara fram. Hún feli í sér hvers konar námskeið, æfingar, kynnisferðir og beina ráðgjöf/leiðsögn fyrir þann „kjarnahóp“ innan lögreglunnar sem bera mun hitann og þungann af verkefnum á þessu sviði. Við mótun þessarar endurmenntunaráætlunar verði tekið mið af löggæsluáætlun þannig að aðgerðin falli einnig að þeirri áætlun.

9.3 Öryggi mikilvægra innviða samfélagsins

Í stefnunni segir að ríkislögreglustjóra beri að skilgreina helstu ógnir á sviði net- og upplýsingaöryggis og hverjir séu mikilvægir innviðir samfélagsins í því sambandi.

Á skýringarmyndinni hér á eftir er þetta gert í samræmi við stefnu almannavarna- og öryggismálaráðs frá júní 2015 en í henni er, líkt og sagði hér að framan, mikilvægum innviðum

samfélagsins skipt í átta flokka sem taldir eru upp í þriðja dálki skýringarmyndarinnar. Annar dálkur er byggður á viðteknum grunnþáttum tölvuöryggis þ.e. leynd, rekjanleika, réttleika og tiltækileika. Í fyrsta dálki eru áhættuflokkar og hinn síðasti afleiðingar atburða eða verknaða.



Á skýringarmyndinni má rekja ógnir sem hafa áhrif á upplýsinga- og netöryggi með tilliti til mikilvægra innviða og hvaða grunnþættir samfélagsins yrðu fyrir áhrifum. Hún getur einnig lýst

tölvu- og netárásum t.a.m. á fjármálastofnun þar sem gögnum um viðskiptavini væri stolið. Árásin sem slík myndi falla undir „tækni“ í fyrsta dálki. Áhrifin hvað upplýsinga- og netöryggi varðar kæmu aðallega fram í „leynd“ í öðrum dálki. Hvað mikilvæga innviði varðar myndi árásin aðallega falla undir „net- og upplýsingakerfi“ sem og „fjármálakerfi“ í þriðja dálki og afleiðingarnar myndu einkum varða „efnahag og umhverfi“ í fjórða dálki og jafnvel „samfélagsvirkni“ í mjög alvarlegum tilfellum.

Hvað náttúruhamfarir varðar liggja fyrir greiningar almannavarnadeildar ríkislögreglustjóra. Ljóst er að náttúruhamfarir hafa einkum áhrif á tiltækileika á sviði upplýsinga- og netöryggis en geta haft mun víðtækari afleiðingar á mikilvægustu samfélagsinnviði.

„Sjúkdómar“ er áhættuþáttur sem horfa má til t.d. í tilviki mjög alvarlegrar inflúensu. Áhrifin á upplýsinga- og netöryggi myndu einkum lúta að „tiltækileika“ og rekstri kerfa vegna veikindaforfalla. Áhrifin á mikilvæga innviði gætu hins vegar orðið mjög mikil og að því leyti eru sjúkdómar og náttúruhamfarir líkir áhættuflokkar samkvæmt þessari skýringarmynd. Mjög skæð inflúensa gæti einnig haft alvarlegar afleiðingar á helstu grunnsviðum samfélagsins eins og þeim er lýst í fjórða dálki.

Hvað varðar áhrif árása „tölvuhakkara“ á tölvu- og netkerfi stjórnvalda ber að taka fram að íslensk stjórnvöld hafa orðið fyrir slíkum árásum. Árás sem slík fellur undir „aðrar óvinveittar aðgerðir“ og „tækni“ í fyrsta dálki. Áhrif á upplýsinga- og netöryggi falla einkum undir „tiltækileiki“ þ.e. í tilviki DDoS-árásar. Árásin snertir einkum „net- og upplýsingakerfi“ og „æðstu stjórn ríkisins“ í þriðja dálki og í fjórða dálki snerta afleiðingar einkum „samfélagsvirkni“.

Árás „tölvuhakkara“ á opinber upplýsingakerfi svo sem sjúkraskrár gæti hins vegar haft aðrar og fleiri afleiðingar. Árásin sem slík myndi falla undir „aðrar óvinveittar aðgerðir“ og „tækni“ í fyrsta dálki. Áhrif á upplýsinga- og netöryggi myndu falla undir „leynd“ og í alvarlegustu tilvikum einnig „tiltækileika“ og „réttleika“. Árásin myndi einkum snerta „net- og upplýsingakerfi“ og „heilbrigðisþjónustu“ í þriðja dálki og í fjórða dálki myndu afleiðingar einkum snerta „samfélagsvirkni“ og „líf og heilsu“ en jafnframt gætu afleiðingar slíkrar stórárásar „tölvu-hakkara“ verið „óþekktar eða óljósar“ t.a.m. í því tilviki að safnað væri saman persónuupplýsingum um mikinn fjölda fólks og þær seldar þriðja aðila. Sá gæti síðan nýtt þessar upplýsingar til margvíslegra árása gegn einstaklingum og hópum sem þá myndu falla undir aðra áhættuflokka samkvæmt skýringarmyndinni.

Tölvuárás að undirlagi erlends ríkis á orkukerfi Íslendinga myndi samkvæmt líkaninu falla undir „hótanir eða ógnir annarra ríkja“. Áhrifin á upplýsinga- og netöryggi yrðu augljóslega mjög mikil og myndu snerta alla fjóra grunnþætti þess. Áhrif á mikilvægustu innviði yrðu sömuleiðis mjög mikil og myndu varða „orkukerfi“, „net- og upplýsingakerfi“, „samgöngukerfi“, „fjármálakerfi“, „löggæslu og viðbúnaðar- og neyðarþjónustu“ og „æðstu stjórn ríkisins“. Í raun myndi slík árás fela í sér ógn við alla mikilvægustu innviði samfélagsins og áhrif í fjórða dálki myndu sömuleiðis varða „samfélagsvirkni“, „líf og heilsu“, „efnahag og umhverfi“ og „fullveldi“.

9.4 Áhættustig

Fullyrða má að tiltekin þjóðríki búi yfir getu til að halda uppi njósnum og beita spilliforritum í net- og tölvukerfum. Einkum eru það orkudreifingar- og net- og upplýsingakerfi sem talin eru í hættu gagnvart slíkum árásum.

Stórárás á innviði samfélags er „verkefni“ sem krefst mikillar þekkingar, getu og búnaðar. Fáir hafa getu til að standa fyrir slíkum árásum og telja verður að hún sé að miklu leyti bundin við þjóðríki, líkt og áður sagði. Af þessu er sú ályktun dregin að ekki verði útilokað að slík árás verði gerð á Ísland en á hinn bóginn telst hún ekki mjög líkleg. Sem fyrr sagði er vandséð hvaða ástæða ætti að liggja baki slíkri árás á friðartímum.

Áhættumat gefur vísbendingar um líkur á tiltekinni atburðarás og mögulegar afleiðingar. Í eftirfarandi töflu er leitast við að bregða ljósi á líkur og afleiðingar stórárása á innviðinn *fjarskipta-, net- og upplýsingakerfi* sem gæti valdið truflun fyrir aðra mikilvæga innviði. Almennt gildir um slíka stórárás að líkur á henni eru litlar en afleiðingar yrðu miklar og jafnvel mjög miklar.

Áhættu má skilgreina á grundvelli vaxandi líkinda eða aukinnar ógnar. Í töflunni vísa því „mjög litlar líkur“ til þess að engin þekkt ógn sé til staðar. Sú er augljóslega ekki raunin þar sem geta til slíkra árása er án vafa til staðar. Hugsanleg og þekkt ógn er því fyrir hendi og þess vegna teljast líkur til staðar en þær eru metnar litlar.

Nokkur óvissa ríkir um líkur á árás á innviðinn *fjarskipta-, net- og upplýsingakerfi* og afleiðingar hennar. Við það bætist að gerandi, að öllum líkindum þjóðríki, þarf að búa yfir getu til að framkvæma slíka árás og hafa uppi áform um hana. Ógn af hálfu þjóðríkja eða hryðjuverkasamtaka getur breyst hratt og erfitt er að segja fyrir um líklega þróun á alþjóðavettvangi.

Samkvæmt töflunni hér á eftir hefði stórárás á innviðinn *fjarskipta-, net- og upplýsingakerfi* miklar eða mjög miklar afleiðingar á alla grunnþætti samfélagsins að undanskildu umhverfi og náttúru. En líkt og gildir um líkurnar er óvissa til staðar. Myndu öll greiðslukerfi verða óvirk, viðskiptalífið stöðvast og samgöngur fara úr skorðum? Eða er hugsanlegt að sveigjanleiki og viðbragðsgeta samfélagsins myndi reynast mun meiri en flestir ætla? Haustið 2008 varð íslenskt samfélag fyrir miklu áfalli þegar fjármálakerfi þjóðarinnar hrundi. Afleiðingar þess urðu vissulega mjög miklar en á hinn bóginn tókst að halda mikilvægustu innviðum samfélagsins gangandi.

Líkur á stórri tölvuárás á innviðinn fjarskipta-, net og upplýsingakerfi							
		Mjög litlar	**Litlar**	**Meðal**	**Miklar**	**Mjög miklar**	**Skýring**
Fyrir liggja upplýsingar um þekkta og mögulega hættu en líkur á að hún raungerist eru litlar.			x				Fáir aðilar ráða yfir getu en engar upplýsingar liggja fyrir um áform.
Mat á afleiðingum							
Samfélagsgildi	**Afleiðingar**	**Mjög litlar**	**Litlar**	**Meðal**	**Miklar**	**Mjög miklar**	**Skýring**
Samfélagsvirkni	Félagsleg og sálræn viðbrögð					x	Skortur á upplýsingum og viðbrögðum stjórnvalda skapar áhyggjur og spennu.
	Áhrif á daglegt líf				x		Skertur aðgangur að síma- og netþjónustu og greiðslumiðlun. Tafir í fólks- og vöruflutningum.
Líf og heilsa	Dauðsföll				x		Fjölgun dauðsfalla vegna skertra möguleika á neyðaraðstoð og sjúkraflutningum.
	Alvarlega slasaðir og sjúkir			x			Fjölgun tilfella vegna rangrar/ófullnægjandi meðhöndlunar.
Efnahagur	Beinn skaði				x		Viðgerðar- og varahluta-kostnaður vegna tölvu- og netkerfa.
	Óbeinn skaði					x	Tekjutap, kostnaður vegna seinkunar, minni framleiðslu og viðskipta.
Umhverfi	Varanlegur skaði						Á ekki við
	Tjón á menningar-verðmætum						Á ekki við
Lýðræði *Réttaröryggi* *Fullveldi*	Skerðing grunngilda og stjórngetu ríkisins				x		Árás gegn mikilvægustu innviðum sem geta ríkisins til stjórnunar hvílir á. Ógn við starfsemi grunnstofnana. Skerðing á réttindum einstaklinga og grunngildum lýðræðis.
Heildarmat á afleiðingum					x		Í heild miklar til mjög miklar afleiðingar.