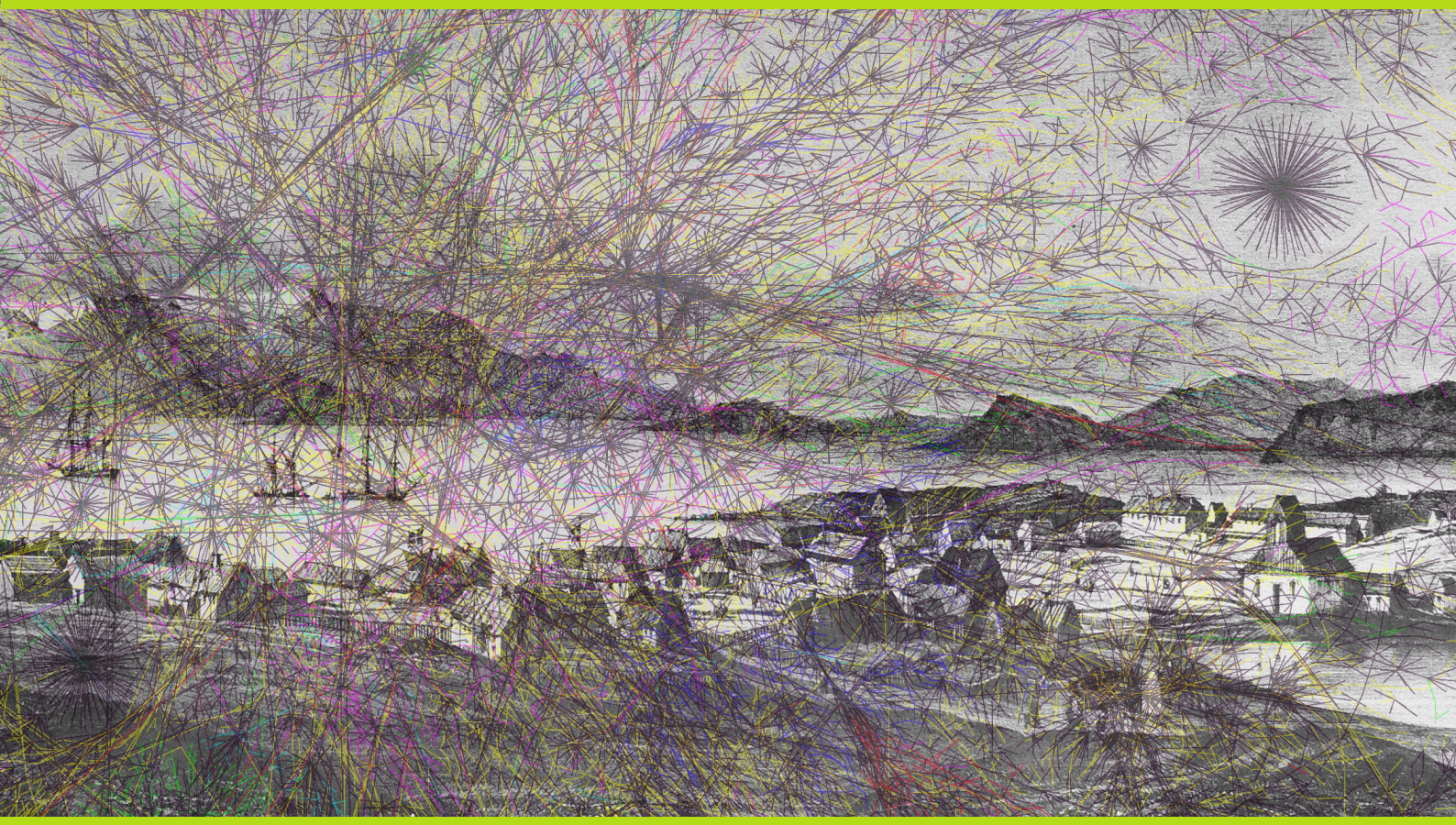
INTERNATIONAL MODERN MEDIA INSTITUTE



IMMI Skýrsla

Netöryggi Íslands

Hraðyfirferð yfir ástand mála og tillögur til Þjóðaröryggisnefndar

Smári McCarthy

Herbert Snorrason

Inngangur

Þessi skýrsla er unnin með hraði að ósk Valgerðar Bjarnadóttur, formanns þjóðaröryggisnefndar, til að stikla á stóru varðandi netöryggi, rafrænan hernað og annað sem snýr að varnarmálum Íslands. Skýrslan byggir á drögum að skýrslu sem IMMI hefur verið að vinna fyrir varnarmálaráðuneyti Bretlands, en er ekki jafn ítarleg. Til að mynda er ekki farið yfir mál sem snúa að öryggi ljósleiðaraneta innanlands, sæstrengja, tengipunkta sæstrengja erlendis, tölvubúnað sem ríkið notar til að fylgjast með lofthelgi og landhelgi, hliðarverkanir vegna stefndra árása á önnur ríki á Ísland, hliðarverkanir vegna stórfelldra árása á nágrannaríki á samskiptagetu Íslands, og þar fram eftir götunum. IMMI getur unnið ítarlegri skýrslu um þessi mál sé þess óskað.

Fjarskipti er tiltölulega nýleg list í sögulegu samhengi. Semaforufjarskipti hófust 1792 með ljósluktum, ritsímar voru teknir í notkun 1837, og útvarpsútsendingar voru fyrst framkvæmdar í upphafi 20. aldar. Síðan þá hafa komið til sögunnar tölvur og stafrænar skeytasendingar, og síðan um 1970 hefur útbreiðsla símkerfa, ljósleiðara, gervihnatta og annarrar fjarskiptatækni á heimsvísu, samhliða örri útbreiðslu á síminnkandi tölvum með sífellt meiri reiknigetu, orðið til þess að Internetið er orðið hornsteinn í alþjóðlegum viðskiptum, fjölmiðlun og almennum samskiptum. Nánast hver einstaklingur er með örsmáan nettengdan síma í vasanum. Meðal sími í dag hefur meiri reiknigetu en allar tölvur heims höfðu samanlagt um 1980, og hraðari nettengingu en allt Ísland hafði 1996.

Það er ekki óraunhæft að áætla að fyrir 2030 fari samanlögð reiknigeta allra tölva í heiminum umfram samanlagða reiknigetu allra mannvera í heiminum[1]. Öryggisógnirnar sem fylgja slíku fyrirkomulagi eru töluverðar - hvort heldur fyrir einstaklinga, fyrirtæki, ríki eða mannkynið í heild.

[1] Þessu hefur verið spáð um árabil, til dæmis af Charles Stross.

Efnisyfirlit

Áhættuþættir fyrir Ísland

Almenn öryggisviðmið

Innan íslensku stjórnsýslunnar er engin sérfræðiþekking á upplýsingaöryggi, og þess eru dæmi að alvarlegar öryggisglufur séu beinlínis opnaðar af rekstraraðilum tölvukerfa. Þannig eru lykilorð sem er úthlutað til starfsmanna stjórnarráðsins afar fyrirsjáanleg og mælt á móti notkun á dulkóðun tölvupósts. Þetta er sérstaklega alvarlegt í ljósi þess að hagsmunir Íslands fara ekki ætíð saman við hagsmuni nágrannaþjóða okkar, en yfirgnæfandi meirihluti fjarskipta fara í gegnum sæstreng til Skotlands. Í Bretlandi starfar aftur stofnun sem hefur það yfirlýsta hlutverk að hlera öll fjarskipti sem fara í gegnum Bretland í leit að upplýsingum sem varða hagsmuni ríkisins. Þannig má hæglega ímynda sér að bresk stjórnvöld hafi getað komist yfir samskipti milli íslenskra stjórnvalda og samningsnefnda í IceSave deilunni, meðal annars sökum þess að vefpóstkerfi stjórnarráðsins bauð ekki upp á dulkóðun þegar þær samningaviðræður áttu sér stað. Í flestum nágrannaríkja okkar er að finna stofnanir sem hafa það hlutverk að aðstoða við upplýsingaöryggi í starfi ríkisstofnana, en enga slíka sérfræðiþekkingu er að finna í íslensku stjórnsýslunni.

Þrátt fyrir verulega öryggisgalla á hugbúnaði, og þrátt fyrir stefnu stjórnvalda um upptöku á frjálsum hugbúnaði (sem er að jafnaði öruggari en séreignarhugbúnaður), þá hefur tölvurekstrarsvið stjórnarráðsins ítrekað komið í veg fyrir notkun starfsmanna á öruggari hugbúnaði sem og frjálsum hugbúnaði. Þetta, samhliða verulegum skorti á almennri þekkingu starfsmanna ríkisins á grundvallarþáttum tölvuöryggis gerir það að verkum að búast má við því að flest gögn í fórum stjórnarráðsins og ríkisstofnana séu í hættu.

Bókhaldskerfi ríkisins

Um það hefur verið rætt frá því að skýrsla lak frá Ríkisendurskoðun haustið 2012 að verulegir annmarkar eru á öryggi í bókhaldskerfi ríkisins, svokölluðum Orra. Þannig kom fram að ekki væri haldið nægilega vel utan um aðgangsheimildir, ekki væri nægileg aðgreining á hlutverkum notanda eftir stofnunum og réttindum þeirra innan stofnana til að stofna, samþykkja og greiða reikninga, og þar fram eftir götunum.

Til viðbótar kemur fram í skýrslu sem PriceWaterHouseCoopers gerðu 2008 að fjölmargir öryggisgallar voru í kerfinu þá, sem flesta hverja mætti búast við að væri hægt að laga. Hinsvegar höfðu sumir öryggisgallarnir með það að gera hvernig hefðir hafa myndast í kringum notkun hugbúnaðarsins, ekki síst þeim gífurlega fjölda notanda sem voru í kerfinu sem samsvöruðu ekki starfsmannaskrá stofnana, og þeim fjölda nafnlausra tilraunanotanda sem höfðu víðtækar heimildir.

Ljóst er að rétt viðbrögð við þessum upplýsingum eru að ráðast í heildarendurskoðun á öllum reikningum sem bókaðir hafa verið í kerfinu frá því að kerfið var tekið í notkun, en ekki er ljóst hvort eða hversu verulega þessir gallar hafa verið misnotaðir, né heldur hvort slík misnotkun, ef hún hafi átt sér stað, hafi eingöngu átt sér stað innan frá stjórnarráðinu og stofnunum þess eða hvort utanaðkomandi árásaraðilar hafi getað nýtt sér galla til að færa til fjárhæðir í heimildarleysi, stunda peningaþvætti, eða annað.

Þó það sé gífurlega ólíklegt að kerfið hafi verið misnotað verulega af utanaðkomandi aðilum í langan tíma án þess að neinn tæki eftir því, þá er staðan vægast sagt óljós. Íslenska ríkið gæti þess vegna hafa verið með beinum hætti að fjármagna hryðjuverk frá árinu 2003 án sinnar vitundar eða vilja, en það verður ekki séð nema með heildarendurskoðun.

Öryggi sérkerfa stofnana

Alvarlegir öryggisgallar á ýmsum sérkerfum stofnana sem geta orðið til þess að viðkvæmar upplýsingar gætu komist í rangar hendur. Margar stofnanir nota vegna starfsemi sinnar sérþróuð forrit til að halda utan um upplýsingar svo sem sjúkraskrár, málaskrár, nemendaskrár, tryggingaskýrslur, og hvaðeina, ásamt því að mörg sérforrit eru notuð í tengslum við sértækan vélbúnað af ýmsu tagi, svo sem GPS búnað, röntgentæki og annað þvíumlíkt.

Ólíkt almennt notuðum kerfum fá sérkerfi sjaldnar rýni öryggissérfræðinga, og vegna síns eðlis hafa frekar tilhneygingu til að breytast ört og án utanaðkomandi öryggisúttektar. Ætla má að í einhverjum þessarra kerfa gætu leynst öryggisgallar sem gætu leitt til gagnataps, leka á persónuupplýsingum, eða opnað fyrir bakdyr sem gæti skapað grundvöll fyrir stærri árás á kerfi á vegum stofnunarinnar eða ríkisins alls.

Bókhaldskerfið Orri er ágætis dæmi um þessa hættu, en meðal annarra sérkerfa sem ætti að taka til skoðunar væri sjúkraskráarkerfið Saga, en ýmsir hafa óformlega dregið athygli að vankönturn á öryggisþáttum þess kerfis.

Eftirlit og hlerun á fjarskiptum

Mikilvægt er að hafa í huga að ekki er aðeins ástæða til að óttast árásir utan frá. Þannig er einnig umtalsvert áhyggjuefni að víðtæk hlerun á fjarskiptum starfsfólks tíðkast í ýmsum stofnunum. Í þessum tilvikum er ekki aðeins fylgst með ódulkóðaðri umferð, heldur er jafnvel ráðist gegn dulkóðuðum tengingum - þar á meðal við netbanka. Þeim sem hafa aðgang að umræddum kerfum er þannig gert kleift að afla persónulegra upplýsinga um gríðarlegan fjölda fólks. Óljóst er hvort ákvæði um þagnarskyldu starfsmanna fjarskiptavirkja eigi við í slíkum tilvikum.

Almennt eftirlit með fjarskiptum

Í 3. mgr. 42. gr. laga um fjarskipti (77/2003) er ákvæði sem kallar á að fjarskiptafyrirtæki stundi almennt eftirlit með fjarskiptum allra, en að þau gögn séu geymd í 6 mánuði. Ákvæðið var tekið upp árið 2005 þegar þáverandi samgönguráðherra fram frumvarp með breytingunum að ósk ríkislögreglustjóra, en var útfært að fyrirmynd umræðu sem hafði þá staðið yfir í ráðherraráði ESB um að umferðargögn yrðu varðveitt í 12-36 mánuði, sbr. skjal ráðherraráðsins nr. 8958/04.

Í frumvarpinu voru færð rök fyrir því að varðveisla á öllum upplýsingum um fjarskipti allra aðila á landinu væru nauðsynleg til að sönnunargögn á refsiverðu athæfi væru til staðar við upphaf rannsóknar, frekar en að þeim yrði aflað sem hluti af rannsókn. Með tilskipun 2006/24/EC var samskonar gagnageymd tekin upp í Evrópusambandinu, en hefur síðan þá verið

hnekkt með dómsúrskurðum stjórnarskrárdómstóla í Rúmeníu[2], Þýskalandi[3] og Tékklandi[4], og hæstaréttar í Kýpur[5].

Gagnageymd er í raun forvirk rannsóknarheimild sem skapar alvarlega hættu fyrir friðhelgi einkalífsins. Þessi hætta hefur verið gerð ljós af ýmsum aðilum, til dæmis í umsögn persónuverndarfulltrúa evrópusambandsins 31. maí 2011[6], þar sem segir að ekki hefur verið sýnt með nægilega skýrum hætti fram á nauðsyn gagnageymdar, að gagnageymd hefði verið framkvæmanleg á vegu sem ganga síður gegn persónuverndarsjónarmiðum, og að tilskipunin hafi skilið eftir of mikið svigrúm fyrir túlkun að hálfu ákæruvaldsins. Það er ekki hægt að sjá annað en að öll þessi atriði eigi líka við í íslenska tilfellinu.

Þar sem að fylgst er með öllum fjarskiptum allra með þessum aðgerðum er um leið fylgst með fjarskiptum lögreglu, landhelgisgæslu, ráðherra, þingmanna, og forseta; starfsmönnum utanríkisþjónustu, fulltrúum almannavarna og öðrum þeim sem hafa með þjóðaröryggisráðstafanir Íslands að gera. Árásaraðilar, skipulögð glæpasamtök og aðrir gætu nálgast gögnin með innbrotum, ýmist í gegnum tölvukerfi eða gagnaver fjarskiptafyrirtækja, og notað þau gegn íslenskum þjóðaröryggishagsmunum á ótal vegu.

Til dæmis væri með þessu hægt að fylgjast með ferðum eða ferðavenjum einstakra þingmanna eða ráðherra og nota það til að gera beina árás á viðkomandi, hvort sem það væri aftaka, mannrán, eða annað, eða það væri hægt að afla með þessum gögnum upplýsingar um þau mál sem verið er að rannsaka innan ráðuneyta. Til að mynda, ef kæmi fram í fjarskiptaskrá tengt IP tölu sem tilheyrði utanríkisráðuneyinu að starfsmaður eða starfsmenn þar hafi nýlega byrjað að gera margar fyrirspurnir til leitarvéla eða vefsíðna um upplýsingar um tiltekið land, ráðamenn þess, viðskiptavenjur og annað, mætti draga þá ályktun með auðveldum hætti að verið sé að undirbúa opinbera heimsókn þangað, gerð viðskiptasamnings við landið, eða eitthvað álíka. Jafnvel með slíkri fólginni þekkingu mætti valda verulegu tjóni á Íslenskum hagsmunum, bæði beinum hagsmunum Íslands sem og þjóðaröryggi landsins.

---

[2] http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

[3] https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011

[4] http://www.edri.org/files/DataRetention_Judgment_ConstitutionalCourt_CzechRepublic.pdf

[5] http://www.supremecourt.gov.cy/Judicial/SC.nsf/All/5B67A764B86AA78EC225782F004F6D28?OpenDocument

[6] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-06_Data%20Retention%20Report_EN.pdf

Hervæðing Internetsins

Í október 2011 á þingfundi NATO í Búkarest var lögð fram ályktun um netöryggi sem lagði til möguleikana á kínetíska[7] gagnárás sem svar við rafræni árás, í skilningi 5. gr. NATO samningsins. Síðan hefur verið staðfest að þetta sé stefna NATO[8], og að skilyrðin fyrir því að slík gagnárás sé framkvæmd séu leynileg, að sögn til að koma í veg fyrir að árásaraðilar gangi eins langt og þeir geti án þess að uppfylla öll skilyrðin fyrir slíkri gagnárás.

Þetta er eitt af mörgum dæmum um þjóðlegar, alþjóðlegar og yfirþjóðlegar ákvarðanir í átt að aukinni hervæðingu netsins. Bandaríkin hafa stofnað sérstaka herdeild, US Cyber Command, kínverjar hafa stundað rafrænar árásir gegn bandarískum tæknifyrirtækjum á borð við Google og Adobe, NATO hefur stofnað Cooperative Cyber Defence Center of Excellence (CCDCOE) í Tallinn eftir að stórvirk rafræn árás var gerð á Eistland árið 2006 sem lamaði fjarskiptakerfi landsins, og bæði Indland og Pakistan hafa stofnað “netheri”. Hervæðing Internetsins er í fullum gangi.

Afleiðingar þessa eru alvarlegar. Internetið er í dag um 8 trilljón dollara hagkerfi[9], sem kann að verða fyrir skaða ef hernaður á netinu verður algengur. Nú þegar verða netviðskipti fyrir barðinu á allskyns öryggisvandamálum sem koma til vegna óöruggra kerfa og kerfisbundinni misnotkun á þeim öryggisgöllum. Kreditkort, sem dæmi, eru eðli sínu samkvæmt óörugg og hafa um langa hríð verið skotmark fyrir skipulagða glæpastarfsemi. En eðli áhættunar breytist verulega þegar ríki skerast í leikinn. Skipulögð glæpastarfsemi er skaðleg, en þar sem markmið skipulagðra glæpa er að hámarka ávinning glæpamannana hafa þeir náttúrulega tilhneigingu til að reyna að vernda kerfið sem þau byggja sínar tekjur á. Það verður mun erfiðara að stunda kreditkortasvindl á netinu ef netið sjálft liggur niðri vegna stórfelldra netárása. Herir hafa hinsvegar minni áhyggjur af hagkerfinu sem þeirra aðgerðir eiga sér stað á, svo lengi sem markmiðum hernaðaraðgerðanna er náð.

Það er töluverð hætt á að hernaðarbrölt á netinu muni skaða hagkerfið sem er þar fyrir. Einstaklingar og fyrirtæki gætu orðið á milli í stríðsrekstri þjóða þar sem ýmsar aðferðir, svo sem Denial of Service árásir, 0-dags og óendanleika-dags gallar, og aðrar nethernaðaraðferðir eru notaðar til að hnekkja á löndum, þeirra innviðum, og þeirra hagkerfum.

Hvað er þjónustuneitun?

Denial of Service, eða þjónustuneitun, á sér stað þegar kerfi fær á sig svo margar beiðnir að það annar ekki eftirspurn. Dæmi um þetta væri ef hópur fólks ákveður að koma í veg fyrir að tiltekinn verslun geti stundað viðskipti, og mynda langa biðröð við afgreiðslukassana þar sem þeir bera upp tímafrekar fyrirspurnir til starfs-fólksins. Í raunveruleikanum eru takmörk fyrir því hversu mikið er hægt að gera þetta, þar sem það þarf stóran fjölda einstaklinga til að

[7] Það er að segja, hefðbundinn hernaður með skotvopnum, sprengjum og tilheyrandi.

[8] At OSCE Internet Freedom conference in Dublin, Ireland, 19. June 2012. Video: http://www.osce.org/cio/91575

[9] Internet matters: The Net’s sweeping impact on growth, jobs, and prosperity; McKinsey Global Institute May 2011

framkvæma svona árás. Á netinu er þetta auðvelt, þar sem tölvurnar sjá um alla vinnuna – árásartölvan sendir bara tugir þúsunda beiðna í einu.

Dreifð þjónustuneitun er þegar margar tölvur, hugsanlega þúsundir talsins – oft undir stjórn árásaraðila í gegnum Trojuhest eða annarskonar víruss, taka sameiginlegan þátt í árás gegn einni þjónustu.

Hvað eru 0-dags og óendanleika-dags gallar?

0-dags galli (0-day vulnerability) er áður óþekktur galli á hugbúnaðarkerfi. Þegar veirur, ormar og öðrum rafrænum árásartólum er beitt byggja þau oftar en ekki á áður óþekktum göllum, því ólíklegara er að búið er að laga þá, sem gerir það líklegara að tólið nái mikilli útbreiðslu áður en það uppgötvast.

Óendanleika-dags gallar (infinity-day vulnerability) er þekktur galli á hugbúnaðarkerfi sem höfundar hugbúnaðarins hafa ákveðið að laga ekki. Ástæðurnar fyrir því geta verið margar, til dæmis að nýrri útgáfa af hugbúnaðinum hafi lagað gallan og þau vilja síður viðhalda eldri útgáfum, eða að gallinn er eiginleiki í hönnun hugbúnaðarins sem er ekki hægt að laga án þess að endurhanna hugbúnaðinn frá grunni.

IPv4, IPv6 og höfuðlén

Internet Protocol (IP) er samskiptastaðall sem gefur hverju nettengdu tæki einstaka tölu. Útgáfa 4 af staðlinum, IPv4, hefur 232, eða um 4 milljarðar tölur. Þessum tölum hefur nánast öllum verið úthlutað, sem þýðir að netið getur ekki lengur stækkað nema að nýr staðall verði notaður. IPv6 staðlinum er ætlað að taka við þessu hlutverki, en meðal úrbóta er stækkað “rými”, upp á 2128 tölur, sem er nóg til að setja milljónir tölva á hvern fermeter á jörðinni. Upptaka á IPv6 hefur tafist verulega af ýmsum ástæðum, ekki síst vegna áhugaleysis stórra netbakbeina, svokallaðra Tier 1 neta.

Mannverum finnst erfitt að muna tölur. Til að auðvelda samskipti var lénskerfið DNS hannað, en í því eru höfuðlén landa (ccTLD) á borð við .is, og almenn höfuðlén (TLD) á borð við .com skilgreind, og umsjónaraðilar þeirra selja svo lén þar undir, á borð við “immi.is” eða “althingi.is”. Þessi nöfn eru í rauninni ekkert annað en tilvísanir á IP tölur, og því mætti líka á IP tölur sem sambærilegar við símanúmer, og lénakerfið sem sambærilegt við símaskrá.

Dæmi um nýlegan nethernað

Flame veiran miðaði að því er virðist að því að kortleggja tölvukerfi Íranska ríksins, þá sérstaklega þau sem snúa að olíuviðskiptum, varnarmálum og rekstri innviða. Þessi vírus hafði að því er virðist engan annan tilgang en að hjálpa bandarískum stjórnvöldum (sem hafa viðurkennt að hafa búið til veiruna) að skilja hvar veikleikar gætu fundist í tölvukerfum Írans.

Stuxnet veiran hafði það hlutverk að brjóta sér leið inn í Siemens iðnaðartölvur sem eru meðal annars notaðar á Íslandi til að stýra hverflum í vatnsaflsvirkjunum, en eru notaðar í Natanz kjarnorkuverinu í Íran til að stjórna skilvindum sem notaðar voru til að hreinsa úran. Stuxnet hraðaði á skilvindunum þangað til þær gáfu sig og skutu álrörum með úrani á

miklum hraða í gegnum skilvindusalina, sem olli miklum skaða.

FinFisher er eftirlitshugbúnaður sem Gamma International bjó til, en hann sýkir tölvur notanda og fylgist með aðgerðum þeirra, en ef eitthvað gerist sem stjórnandi hugbúnaðarins hefur merkt sem áhugavert er komið skilaboðum til stjórnandans næst þegar tölvan er nettengd. Fyrir byltinguna í Egyptalandi hafði ríkisstjórn Hosni Mubarek gert samning um notkun á hugbúnaðinum gegn Egypskum notendum.

Bundestrojan er hjáheiti á njósnahugbúnaði sem þýska ríkisstjórnin lét útbúa til að sýkja tölvur bæði þýskra borgara og annarra sem þau höfðu áhuga á því að hafa eftirlit með sem áttu leið í gegnum landið. Bæði lögregla og landamæraeftirlitsaðilar settu hugbúnaðinn inn á tölvur sem þeir skoðuðu, en hann skilaði skýrslum til baka með upplýsingum um staðsetningu og notkun tölvunnar.

Miðaðar og ómiðaðar árásir

Rafrænar árásir geta verið ýmist miðaðar eða ómiðaðar. Ómiðuð árás gæti til dæmis verið árás sem miðar að því að safna upplýsingum um sem flesta aðila. Þetta gæti verið forrit sem liggur á netbeini (e. router) og hlerar samskipti í leit að kreditkortanúmerum eða lykilorðum, eða vefsíða sem lítur út fyrir að vera frá opinberum aðila og óskar eftir persónu-upplýsingum.

Miðuðum árásum er yfirleitt beint gegn tiltekinni persónu, fyrirtæki, stofnun eða ríki, oft með það markmið að nálgast upplýsingar frá þeim eða vinna þeim skaða.

Í dæmunum á undan eru Bundestrojan og FinFisher dæmi um ómiðaðar árásir, en Stuxnet og Flame eru dæmi um miðaðar árásir.

Þess ber að geta að miðaðar árásir hafa tilhneygingu til að fara úr böndunum. Þó svo að Stuxnet hafi verið miðað að Natanz kjarnorkuverinu uppgötvaðist veiran fyrst þegar hún fór að dreifast til Indónesíu og Pakístan, en hún hefur einnig fundist á tölvum á Indlandi, Bandaríkjunum, Azerbaijan og víðar.

Áhrif á ríki og fyrirtæki

Hættan á að nethernaður sé sérstaklega miðaður á einstaklinga eða fyrirtæki eykst eftir því sem hagsmunirnir aukast og baráttan verður harðari. Ríkisstjórn eða hryðjuverkahópur gæti séð sér hag í því að miða árásum á viðskiptavefi eða vefþjónustur, sem form af hagrænni þjónustuneitun. Þetta er sérstaklega algengt í nethernaði milli Íslamskra og vestrænna aðila – þó svo að vestrænt hugarfar gengur gjarnan út frá því að ríkið sé uppspretta valds, sem gerir það að verkum að vestrænn hernaður miðar að því að hefta framkvæmdargetu ríkisins, þá hefur íslömsk heimssýn gjarnan viðskipti sem miðju alls, og eru árásir þá frekar miðaðar á markaði og samkomustaði. Þetta endurspeglast ekki síst í nethernaði, en svo dæmi sé tekið var veira að nafni Gauss staðin að því að brjótast inn í bankakerfi í Lebanon, að því er virðist í leit að upplýsingum um peningaþvætti að hálfu Hezballah.

Samhliða þessari hættu er hætta á því að markaður fyrir 0-dags galla verði til. Sögulega séð hafa fáir aðilar haft beinan hagnað af þróun og sölu á 0-dags göllum og tóllum sem nýta þá galla, en þeir sem höfðu ávinning af því höfðu oftast tengingar við skipulagða

glæpastarfsemi eða tölvuöryggi, eða unnu í akademísku umhverfi. Með frekari hervæðingu á netinu skapast möguleikar á fjárhagslegum ávinningi á framleiðslu og sölu á netvopnum: forritarar gætu leiðst út í það að búa vísvitandi til vandfundna galla í hugbúnaði sem þeir koma að því að framleiða, og selja upplýsingar til hæstbjóðanda um eðli gallana. Hæstbjóðandi kann þá að vera “vinveitt” ríkisstjórn, eða einhver annar, svo sem alræðisstjórn, hryðjuverkahópur, skipulagður glæpahópur, keppinautar fyrirtækisins, og svo framvegis.

Eina raunhæfa leiðin til að halda verði á 0-dags göllum lágu til frambúðar – og þar með að stuðla að því að gallarnir séu síður þróaðir eða þeir seldir – er að stunda eingöngu varnarhernað.

Jonathan Evans, forstjóri bresku leyniþjónustunnar MI5, hefur fullyrt opinberlega að MI5 berst við “ótrúlegt” magn af netárásum, sem eiga uppruna sinn bæði hjá ríkjum og glæpahópum. Evans sagði að þetta sé “ógn við heilindi, trúnað og aðgengi upplýsinga ríkisins, en einnig ógn við fyrirtæki og akademískar stofnanir,”[10] en hann bendir á að aukin tíðni netárása skapar nýjar ógnir fyrir ríkisstjórnir og fyrirtæki, sem almennt hafa ekki þróað almennilegar varnir.

[10] http://www.bbc.co.uk/news/uk-18586681

Internetið og ríkið

Internetið er ómiðstýrt og hefur ekki neitt eitt stjórnkerfi. Að mestu leyti er það dreift og að hverri ákvarðanatöku koma margir aðilar. Þetta er ekki galli, heldur mikilvægur eiginleiki sem hefur gert öran vöxt netsins mögulegan og komið í veg fyrir eftirlit og ritskoðun að einhverju leyti.

Þó eru veikir punktar í stjórnkerfi netsins. Eitt þeirra er ICANN (Internet Corporation for Assigned Names and Numbers), sem starfar undir lögum í Kalíforníu undir sérleyfi frá bandaríska viðskiptaráðuneytinu. Þó svo að ICANN sé stjórnað af mörgum aðilum á heimsvísu, og hafa bæði ríki og hagsmunaaðilar aðkomu að ákvarðanatöku innan ICANN, eru í raun lítil takmörk fyrir þeim þrýstingi sem bandarísk stjórnvöld geta beitt ICANN.

ICANN stjórnar útgáfu á höfuðlénum (TLD og ccTLD) og IP tölum. Einstök höfuðlén eru gefin út með leyfissamningum til fulltrúa ríkja í tilfelli ccTLD (svo sem .is), og til fyrirtækja með rekstrarsamning í tilfelli TLD (svo sem .com). Hvert slíkt fyrirtæki setur svo sína eigin stefnu um notkun léna undir höfuðléninu. IP tölur eru afturámóti veittar út í stórum blokkum til svæðisstjórna á borð við Evrópsku svæðisstjórnina RIPE (Réseaux IP Européens), sem svo gefa út smærri blokkir til fyrirtækja sem starfa á svæðinu, oftast netþjónustuaðila. Netþjónustuaðilarnir gefa svo út einstakar IP tölur eða smærri blokkir.

Til að flækja málin frekar eru allur fjarskipta-búnaður á heimsvísu á einn eða annan hátt á valdi ITU, alþjóðafjarskiptasambansins. Þó svo að völd ITU séu í raun takmörkuð setja þau staðla sem fjarskiptafyrirtæki fylgja, og stjórna alþjóðlegum viðmiðum um gjaldskrár í fjarskiptabakbeinum. Nýlega hafa verið ýmsar hreyfingar, sérstaklega með stuðingi Rússlands, Kyrgyzstan og Kína, í átt að því að víkka út vald ITU yfir netið, meðal annars með breytingum á gjaldskrám. ITU hefur auk þess óskað eftir að helmingurinn af öllum IP tölum í nýja IPv6 númerakerfinu verði afhent ITU, en það myndi láta ITU standa jafnfætis ICANN varðandi völd yfir IP netum.

Áhrif sameinuðu þjóðanna á netinu eru svo til engin. Reglulega hafa sameinuðu þjóðirnar gert tilraunir til að auka vægi sitt í áhrifum í ákvarðanatöku á netinu, nýlegast með stofnun Internet Governance Forum, sem miðar að því að bjóða ríkjum og hagsmunaaðilum að hittast reglulega til að ræða um hvernig Internetinu verður stjórnað. Því hefur gjarnan verið mætt með ákveðnu vandlæti að hálfu þeirra sem telja að ríki eigi ekkert erindi í stjórnun netsins, en vegna þessa vandlætis, sem og almenns skorts á raunverulegu valdi, hefur IGF orðið svo til ekkert úr verki á undanförnum sjö árum.

Geta ríkja til að stjórna netinu er eins og sést afar takmörkuð, en þó reyna sum ríki það sem þau geta í gegnum ICANN, ITU, IGF og fleiri ámóta fyrirbæri.

Það sem ríkin eru að reyna

Ýmis ríki, til að mynda Rússland og Kína, hafa lýst áhuga á því að brjóta netið niður á þann hátt að þjóðríki hafi meira vald yfir einstökum hlutum þess, en að þetta megi gera ýmist með alþjóðlegu samkomulagi eða með venju, en skilningur ríkir um að þetta sé eina raunverulega

leiðin til að hafa stjórn á því efni sem sett er fram á netinu.

Sum ríki hafa sýnt fram á getu sína til að stjórna vélbúnaði sem er staðvær innan þeirra landamæra, svo sem Kína með sínum mikla eldvegg og Egyptaland á tíma Mubareks, sem dró til baka allar BGP auglýsingar, sem gerir það að verkum að það verður ómögulegt að “rata” um netið og fjarskipti falla niður.

Sum ríki hafa eins og áður segir hafið virka þróun á rafrænum vopnum á borð við vírusa og annan hugbúnað, til að framkvæma beinar árásir á innviði, upplýsingakerfi eða netkerfi, stunda njósnir eða eftirlit, og skaða tölvukerfi.

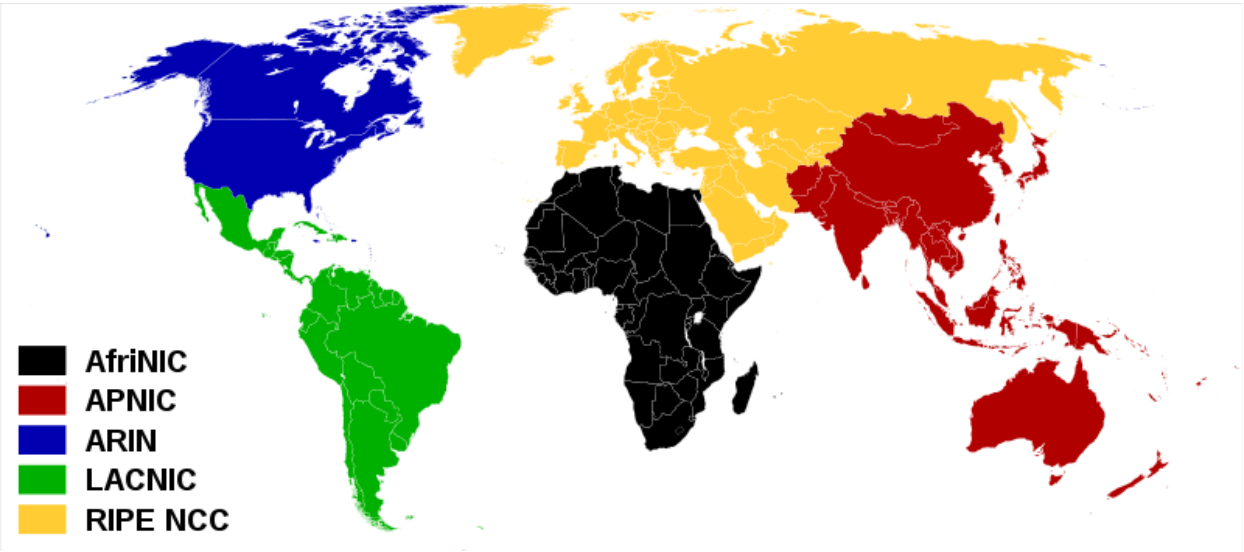
Fjöldi ríkja sem stundar ritskoðun á netinu eykst stöðugt. Blaðamenn án landamæra telja í dag 12 lönd sem “óvini netsins”, en 14 til viðbótar eru talin vera “eftirlitssamfélög”. Þó svo að flest þeirra landa séu á miðaustur-löndum, mið-Asíu, eða suðaustur-Asíu, eru tvö sem standa út úr: Frakkland og Ástralía.
Tvö lönd, Chile og Niðurlönd, hafa tekið upp lög sem tryggja hlutleysi netsins, en þar er tilgangurinn að koma í veg fyrir að fjarskipta-fyrirtæki takmarki aðgang að ákveðnu efni í fjárhagslegum, viðskiptalegum, eða pólitískum tilgangi.

Það sem ríkin ættu að gera

Ekkert ríki hefur í dag heildstæða upplýsingastefnu, sem nær yfir alla þætti upplýsingaréttar, aðgangs að upplýsingakerfum, regluverks um refsingar og bætur fyrir ákveðnar tegundir af upplýsingabrotum, og svo framvegis. Afleiðingin af þessu er fjöldinn allur af innbyrðis ósamkvæmum ákvæðum varðandi aðgengi ríkis, almennings og annarra aðila að upplýsingum, og margvíslegum ákvæðum sem er auðvelt að misnota, hvort sem það eru lög um opinber leyndarmál, meiðyrðalög, eða lög sem heimila eftirlit með fjarskiptum.

Þar sem upplýsingar hafa sögulega verið séðar sem leynileg gögn í fórum ríkisins annarsvegar, og úttak fjölmiðla hinsvegar, hafa ríkin engan grundvöll til að skilja netið. Skorturinn á almennri upplýsingaheimspeki innan ríkisvaldsins leiðir ríki gjarnan til að líta á innri og ytri ógnir og samfélagslega þróun, sem á rætur sínar að rekja til aukins aðgengis að upplýsingum, með því að reyna að takmarka eða koma í veg fyrir aðgang að upplýsingum eða upplýsingatækni, eða að auka eftirlit með því. Þetta ætti ekki að vera tilfellið. Annars vegar er upplýsingaaðgengi orðið að hornsteini í félagslegum og borgaralegum réttindum, en hinsvegar er áframhaldandi aðgengi að óritskoðuðum og óhleruðum upplýsingakerfum orðið mikilvægur þáttur í þjóðaröryggi hvers lands.

Vegna þessa mikilvægis upplýsingatækninnar er þörf á almennum alþjóðlegum sáttmála sem tryggir frið á netinu.



Regional Internet Registries

Hættur og viðbrögð metin með OSI líkaninu

OSI líkanið er greiningarlíkan sem lýsir mismunandi þáttum fjarskipta eftir eðli þeirra og tilgangi. Í líkaninu eru sjö lög (layers), en einhver samskiptastaðall verður að vera notað um hvert þeirra til að samskipti geti átt sér stað. Sem dæmi um talmál manna væri “physical layer” hljóðhimnur og raddbönd og það að hljóð geti borist um loftið, “data link layer” er þar sem tveir einstaklingar koma saman til að tala saman, “network layer” er þar sem þeir bera skilaboð áfram í munnmælum, og svo framvegis upp að “application layer”, þar sem raunverulegt umræðuefni er tekið til tals.

Hér er tafla sem lýsir nokkur dæmi fyrir hvert lag um hvaða samskiptastaðlar eiga sér stað á laginu fyrir rafræn samskipti, hver stjórnar því lagi, í þeirri merkingu að hafa getu til að hafa áhrif á það sem fer þar um, hvaða ógnir eru til staðar fyrir lagið, og hvaða viðbrögð eru möguleg til að minnka hættuna á ógnum á því lagi.

Lag	**Tilgangur**	**Dæmi**	**Stjórnun**	**Ógn**	**Viðbrögð**
Application	Eiginlegt efni samskiptanna	HTTP, DNS, SIP, BGP	Þeir sem þróa hugbúnað, sér í lagi stýrikerfi.	Vírusar, ormar, trojuhestar, gallar á hugbúnaði, 0-dags og óendanleika-dags gallar.	Kóða-endurskoðun, hönnunar-endurskoðun, vírusvarnar-hugbúnaður, getu-takmarkanir, frjáls hugbúnaður.
Presentation	Mál samskiptanna.	MIME, SSL, ASCII, PGP, MPEG	Staðlaráð, þeir sem þróa hugbúnað	Málfræðilegar árásir, dulmálsfræðilegir gallar	“Full recognition before processing,” Endurskoðun á dulmáls-kerfum.
Session	Utanumhald um samtal	TCP, SOCKS	Framleiðendur stýrikerfa	Gallar á hugbúnaði, 0-dags og óendanleika-dags gallar.	Kóða-endurskoðun, hönnunar-endurskoðun
Transport	Sending skilaboða og staðfesting á móttöku	TCP, UDP, SPX	Framleiðendur stýrikerfa og netbúnaðar	Gallar á hugbúnaði, 0-dags og óendanleika-dags gallar.	Kóða-endurskoðun, hönnunar-endurskoðun
Network	Ávarp og tilvísun í	IP, IPsec, ICMP, IGMP	ICANN	Anonymity violations,	Lauknet

	réttan aðila			network reshaping	
Data Link	Tvö tæki í samskiptum sín á milli.	PPP, PPTP, Ethernet	Netþjónustu-veitendur, símafyrirtæki, netrekstrar-aðilar	Rafrænt eftirlit, rammainnskot[11]	Dulkóðun
Physical	Eðlisfræðileg boðskipti	802.11, 100Base-TX, X.25	Framleiðendur örstýringa	Gallar í kísilkubbum,, killswitches	Endurskoðun örstýringa, frjáls vélbúnaður.

[11] Rammainnskot, eða “frame injection”, er þegar líkt er eftir haus (header) á ramma af fjarskiptagögnum í hlassi (payload) fjarskiptanna. Ef hlassið er ódulkóðað getur þetta valdið því að móttökubúnaður í þráðlausum fjarskiptum lendi í villu og telji fjarskiptin hafa reikað í tíma. Þá getur árásaraðili sem stjórnar hlassi fjarskiptanna náð völdum yfir móttökubúnaðinn og þar með öll frekari samskipti.

Vernd í hverjum punkti

Þó að hervæðing Internetsins í árásarskyni sé vissulega hættuleg braut að feta, getur verið að hervæðing í varnarskyni sé lykilatriði. Í grannfræðilegu tilliti er Internetið jaðar Internetsins. Innri hluti þess er holur, eða ekki til, svipað og innri hluti Klein-flösku. Segja má að Internetið sé hávíð víðátta án innra byrðis.

Þar sem hver hnútur (þ.e., tölva eða tæki tengt við net) er aðgengilegur utan við netkerfið vegna þess að þeir eru staðsettir einhversstaðar er eina skynsamlega varnarstefna Internetins algjör hervæðing í varnarskyni. Herlaus svæði geta ekki verið til. Þetta gæti verið að breytast, en aukin notkun sýndarþjóna gerir lagskipta kerfi þar sem innri hlutar þess eru aðeins aðgengilegir úr næsta lagi fyrir ofan. Þrátt fyrir þetta er alltaf hægt að skipleggja árás á ytra lagið - eins og t.d. að taka vélbúnaðinn úr sambandi - en þar er um gereyðingaraðferð að ræða. Engu að síður virðist skynsamlegra frá öryggissjónarmiði að verja Internetið allsstaðar frekar en á einhverjum tilbúnum jaðri.

Í þessu sambandi má benda á samanburðinn milli Rússlands árið 1812 og Frakklands árið 1940. Hervæðing Rússlands hafði náð því marki að landið hafði enga raunverulega varnarlínu, heldur var viðvarandi og djúpstæð vera hersins á nær öllu landsvæðinu. Þetta hægði gífurlega á sókn Napóleons, sem gat aldrei ráðist á neinn stakan stað til að ná yfirráðum yfir rússum. Í Frakklandi síðari heimsstyrjaldarinnar var aftur á móti lítið mál fyrir þýska herinn að ná yfirhöndinni þegar þeir höfðu komist fram hjá varnarlínunni á landamærunum.

Nokkur munur er á að verja allt í stafrænu umhverfi og í efnisheimunum. Í efnisheimi getur hver borg haft nákvæmlega eins varnarkerfi, og árásarmaðurinn er engu að síður takmarkaður af birgðum sínum, hvort sem það eru matvæli eða skotfæri. Í netheimum er tími hinsvegar eina raunverulega takmörkunin í vegi þess sem ætlar að brjótast inn í einsleitt safn eininga. Einsleitni er því höfuðsynd varna á Internetinu: Ef árás virkar á einn hnút, og margir hnútar eru einsleitir, virkar árásin á marga hnúta. Samskonar fyrirbæri má sjá í líffræði þar sem stórir hópar klónaðra einstaklinga eru svo viðkvæmir fyrir sjúkdómum sem geta sýkt jafnvel einn einstakling að eina hugsanlega leiðin til að bjarga nokkrum er algjör einangrun í sóttkví. Slík einangrun er óraunhæf, en liggur engu að síður til grundvallar algengustu öryggisaðferðum netheima í eldveggjum og niðurhólfun.

Lausn líffræðilegra kerfa er fjölbreytni. Einstaklingar eru ólíkir á ýmsan hátt, og heildin fær þannig ákveðna vörn gegn árásum.Goerner, Ulanowicz og Lietaer hafa bent á að í öllum sjálfstýrandi kerfum sé til staðar ákveðið jafnvægi milli skilvirki og fjölbreytileika, sem ákvarðar lífvænleika heildarinnar.[12] Þessi mæling á lífvænleika kerfisins er í vissum skilningi dreiflægt jafngildi sveigjanleika kerfis - í einföldu máli, hversu mikla röskun kerfið þolir áður en það bilar.

---

[12] Sally J. Goerner, Bernard Lietaer, Robert E. Ulanowicz: *Quantifying economic sustainability: Implications for free-enterprise theory, policy and practice*; Ecological Economics, 69 (2009) 76–81.

Málið snýst þannig um lífvænleika kerfisins: Hvers konar nálgun getur her eða þjóðaröryggisstofnanir ríkis tekið til að verja grunninnviði, fjarskiptagetu og almennt öryggi gegn árásaraðilum?

Fyrst verðum við að gangast við því að árásir geta komið úr óvenju mörgum áttum, til að mynda fjandsamlegum ríkjum, hryðjuverkamnnum, skipulögðum glæpasamtökum, mótmælahreyfingum eða jafnvel forvitnum unglingum. Hvatning þeirra getur verið pólitísk, hernaðarleg, fjármálaleg, fræðslule eða félagsleg. Árásinni getur verið beint að innviðum ríkisins eða einkaaðila, líkt og Stuxnet ormurinn sem var beint gegn Natanz úranauðgunarstöðinni í Íran. Þeim getur einnig verið beint gegn einstaklingum, fyrirtækjum, og frjálsum félagasamtökum.

Árásir geta einnig hafa víðtækari áhrif en ætlast var til. Áhrif Stuxnet voru til dæmis ekki takmörkuð við tölvurnar í Natanz, heldur sýktust einnig tölvur í Indónesíu og Indlandi. Ófyrirsjáanlegt eðli flókinna kerfi í ríku umhverfi þýðir að jafnvel mjög hnitmiðaðar árásir geta beinst gegn röngum aðilum.

Í ljósi þessa fjölbreytileika, svo ekki sé minnst á óstöðugleika, óvissu, flækjustig og tvíræðni rafræns hernaðar, er engin allsherjarlausn möguleg. Við getum hins vegar útilokað aðferðir sem byggja á því að útbúa ákveðna verjanlega fasta punkta á borð við eldveggi. Öll tæki sem ekki eru sjálf öryggispunktar skapa veikleika í öllu kerfinu, í upphafi með því að stefna sjálfum sé í voða og síðan sem stökkpallur fyrir frekari árásir.

Tillögur að aðgerðum

Rétt viðbrögð stjórnvalda væru að taka til greina öryggi alls þess hluta netsins sem eru innan sinna landamæra (óháð tilgangi eða stjórnun þeirra nethluta), og að auki alla þá hluta netsins sem eru í samskiptum við þau tæki. Þetta leiðir af sér að varnarsvæði Íslands í net- og upplýsingaöryggismálum er Internetið í heild sinni, en að sama gildi um aðrar þjóðir.

Til að nálgast lausn á þessu væri eðlilegt að fjármagna ýmis verkefni til að auka heildaröryggi kerfisins. Benda má á t.d.:

- Endurskoðun á frjálsum hugbúnaði. Það væri ekki viðeigandi fyrir ríkisstjórnir að fjármagna endurskoðun á séreignarhugbúnaði, sem ætti að falla undir skuldbindingar hugbúnaðarframleiðandans. Að auki ætti að hvetja til aukinnar notkunar á hugbúnaði sem er opinn til skoðunar og jafningjaþróunar, þar sem ólíklegra er að öryggistengdur freistnivandi, á borð við að forritari þiggi greiðslur frá þriðja aðila fyrir að setja öryggisgalla í kerfi án vitundar vinnuveitanda, komi upp í slíku kerfi. Þar að auki hefur frjáls hugbúnaður jafnan brugðist betur við öryggisgöllum sem upp hafa komið.

- Tölvuöryggisþjálfun fyrir almenning, hugsanlega sem hluta af upplýsingatækni í almmena menntakerfinu. Líkast til mætti draga verulega úr fjölda öryggisatvika með því t.d. að þjálfa fólk markvisst í því að uppfæra stýrikerfi sín reglulega.

- Ríkið gæti boðið upp á eða fjármagnað verkefni þar sem fólk getur komið með sínar tölvur í “netfærnipróf,” sem myndi svipa til haffærniprófs hjá skipum. Í prófinu yrði prófað gegn algengum öryggisgöllum og og leiðbeiningar gefnar um hvernig

ætti að sneiða hjá þeim. Það ætti alls ekki að gera “netfærniskírteni” að skyldu fyrir almenning eða einkafyrirtæki, en hinsvegar ætti þetta að vera nauðsynlegur þáttur í rekstri tölvukerfa á vegum ríkisins. Slíkt próf ætti að vera óháð stýrikerfi, en taka á atriðum svo sem innbrotsáhættu, hættu á að kóði sé keyrður á tölvu með skipun frá annarri tölvu, og tilvist vírusa og annars skaðlegs hugbúnaðar. Það mætti jafnvel gera prófið sjálft opinbert, þó svo að það gæti gert árásaraðilum auðvelara fyrir að brjótast inn í kerfi kæmi á móti að það myndi auka þrýsting á öryggissérfræðingum að þróa viðbætur við prófið, lagfæringar á göllum. Ennfremur tryggir opið próf að fólk sem vill láta tölvurnar sínar undirgangast prófið, en vilja ekki afhenda ríkisstofnun eða ríkisstyrktum aðilum tölvuna, geti enn notað prófið.

- Bjóða upp á verðlaun fyrir afhjúpun áður óþekktra öryggisgalla. Þrátt fyrir að einhver hætta sé á að til verði freistnivandi við þetta getur vel skipulagt verkefni af þessu tagi dregið úr hættunni á því að þeir sem uppgötvi veikleika noti þá á óæskilegan hátt. Slíkt verkefni gæti orðið afar dýrt, en nýlegt mat verðleggur 0-dags galla sem nýta má yfir netið á í kringum 200.000 bandaríkjadali. Hugsanlegt er að verðlaunakerfi geti ýtt verðum á svarta markaðnum upp. Þörf er á ítarlegri athugun áður en slíku verkefni er hrint í framkvæmd.