MAÍ 2023

FJÖLÞÁTTAÓGNIR

GRD | Greiningardeild ríkislögreglustjóra

EFNISYFIRLIT

TILEFNI SKÝRSLU

Greiningardeild ríkislögreglustjóra (GRD) hefur í skýrslum sínum til stjórnvalda og samstarfsaðila frá árinu 2018 fjallað um *fjölþáttaógnir* (e. Hybrid threats), *fjölþáttaátök* (e. Hybrid conflict) og *fjölþáttahernað* (e. Hybrid warfare) en verulegur hluti þeirra ógna sem til fjölþáttaógna teljast falla beint undir lögbundið hlutverk GRD sem er m.a. að meta hættu og áhættu vegna brota er falla undir X. og XI. kafla almennra hegningarlaga nr. 19/1940, með síðari breytingum og veita ráðgjöf um viðbúnað sem hefur þýðingu fyrir hagsmuni ríkisins og þjóðhagslega mikilvæga starfsemi.[1]

Í áhættumati GRD vegna fjölþáttaógna frá árinu 2019 segir:

> **„Möguleg ógn við þjóðaröryggi Íslendinga myndi, að mati greiningardeildar ríkislögreglustjóra, tengjast þróun á sviði alþjóðamála og þar með NATO aðild Íslendinga og varnarsamstarfi við Bandaríkin; miklu spennuástandi í samskiptum austurs og vesturs eða beinum ófriði. Því er það svo að fyrirbrigði á borð við „fjölþátta-ógnir" verða ekki tekin ein og sér út úr heildarmyndinni og mikilvægi þeirra upphafið eða því hafnað. Þvert á móti verður einungis lagt mat á þær ógnir með hliðsjón af ríkjandi ástandi; hvað Ísland varðar einkum í samskiptum austurs og vesturs og þeim pólitísku og hernaðarlegu markmiðum sem að baki slíkri árás gætu búið.**

Hinar umfangsmiklu breytingar í öryggis- og varnarmálum Evrópu sem orðið hafa frá því að skýrslan kom út, um mitt ár 2019, gera að verkum að GRD telur nauðsynlegt að meta og greina stöðu mála varðandi fjölþáttaógnir upp á nýtt.

1 404/2007 – Reglugerð um greiningardeild ríkislögreglustjóra. (island.is)

HELSTU FORSENDUR

Hernaðarógn og spenna hefur ekki verið meiri í Evrópu frá árum seinni heimstyrjaldar. Vægðarlaus hernaður Rússa í Úkraínu í kjölfar ólöglegrar innrásar þeirra þann 24. febrúar 2022 hefur breytt grunnforsendum varðandi öryggis- og varnarmál á Vesturlöndum.[2]

Ísland hefur tekið virkan þátt í aðgerðum NATO til að styrkja varnargetu Úkraínu m.a. með beinum fjárframlögum, þjálfun auk þess að útvega sjúkragögn og vetrarfatnað. Sömuleiðis tekur Ísland þátt í þvingunaðgerðum alþjóðasamfélagsins gegn Rússum vegna hernaðar þeirra í Úkraínu.[3]

Rússnesk stjórnvöld hafa skilgreint Ísland sem óvinveitt ríki og talsmenn þeirra gagnrýnt málflutning íslenskra ráðamanna. Sömuleiðis hafa Rússar á síðustu árum aukið hernaðarumsvif á norðurslóðum.[4,5]

Tugum milljarða íslenskra króna hefur verið varið til uppbyggingar varnartengdra mannvirkja í Keflavík undanfarin ár vegna breyttrar stöðu á Norður-Atlantshafi. Enn frekari framkvæmdir varðandi rekstur, viðhald og endurbætur varnarmannvirkja á Íslandi og önnur uppbygging eru deiglunni á næstu árum.[6,7]

Ólögleg upplýsingaöflun Rússa fer vaxandi innan Evrópu þ.m.t. á Norðurlöndum. Í Danmörku og Noregi er ólögleg upplýsingaöflun erlendra ríkja þ.m.t. rafræn/stafræn talin ógn við þjóðaröryggi og geti m.a. beinst gegn mikilvægum innviðum. Rússar eru taldir beina ólöglegri upplýsingaöflun og stafrænum árásum gegn ríkjum sem styðja Úkraínu. Hópur netþrjóta sem tengjast Rússlandi eru taldir ábyrgir fyrir netárásum og tilraunum til ólöglegrar upplýsingaöflunar á Íslandi.[8, 9, 10, 11, 12, 13, 14, 15, 16]

2 290622-strategic-concept.pdf (nato.int)
3 Government of Iceland | War in Ukraine – Iceland's response
4 Russian government approves list of unfriendly countries and territories – Russian Politics & Diplomacy – TASS
5 „In the past few years, Russia's military activities in the region that impact on neighbouring countries have markedly increased"; Russia in the Arctic. Development Plans, Military Potential, and Conflict Prevention (swp-berlin.org)
6 Herinn vill milljarða fjárfestingu (mbl.is)
7 0689.pdf (althingi.is)
8 French government warns of increased risk of Russian espionage (lemonde.fr)
9 Russia is rebuilding its spy networks throughout Europe (lemonde.fr)
10 'Tip of the iceberg': rise in Russian spying activity alarms European capitals | Financial Times
11 Switzerland's Security 2022: The Federal Intelligence Service publishes its latest situation report (admin.ch)
12 Russia Increased Cyber Espionage Against Countries Supporting Ukraine, Microsoft Says – WSJ
13 In a Wary Arctic, Norway Starts to See Russian Spies Everywhere – The New York Times (nytimes.com)
14 NTV-2022 (pst.no)
15 vsd_uk.pdf (pet.dk)
16 Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression – Microsoft On the Issues

Haustið 2022 voru unnin mörg skemmdaverk innan Evrópu m.a. á mikilvægum innviðum sem tengjast orkuflutningum, samgöngum og samskiptum. Sömuleiðis hefur orðið vart við drónaflug nálægt orkuinnviðum og rússneskar skipaferðir í nágrenni sæstrengja og orkuinnviða á hafi úti. Mörg ríki Evrópu hafa brugðist við með því að efla öryggisgæslu og varnargetu.

Í ljósi ofangreindrar þróunar og vegna ábendinga um mikilvægi þess að skilgreina hugtakið fjölþáttaógnir[17] og skapa sameiginlegan skilning á eðli og pólitískum áhrifum helstu fjölþáttaógna[18] hefur greiningardeild ríkislögreglustjóra ritað hættumat ásamt ítarlegri umfjöllun um hugtakið og eðli fjölþáttaógna.

17 Samtal um þjóðaröryggi: Fjölþáttaógnir (stjornarradid.is)
18 Norraen_utanrikis_og_oryggismal_2020_net.pdf (stjornarradid.is)

FJÖLÞÁTTAÓGNIR

Hugtökin *fjölþáttahernaður og -ógnir* (e. hybrid warfare, hybrid threats), hafa verið ofarlega á baugi í umræðum um öryggis- og varnarmál á Vesturlöndum síðustu sextán ár hið minnsta. Í þeirri orðræðu hefur mátt greina mismunandi merkingu og skilning á hugtökunum þá einkum hvort þau eru túlkuð þröngt eða vítt.

Þröng túlkun felur í sér að áskilið er að hvert það ríki sem stendur frammi fyrir „fjölþáttaógn" standi um leið frammi fyrir hefðbundinni hernaðarógn af hálfu erlends ríkis eða pólitískra hópa. Það kallar með öðrum orðum á að skilgreindur óvinur sé, hið minnsta, til staðar og hann sé í senn fær um að framkalla samsettar ógnir þ.m.t. hefðbundna hernaðarógn og líklegri en ekki til að búa yfir ásetningi um einmitt það. Með öðrum orðum að samhæfðar séu beinar hernaðarlegar aðgerðir og aðgerðir sem ekki notast við herafla til að ráðast á skilgreindan óvin í nafni pólitískra langtímamarkmiða.

Víð túlkun hugtakanna hefur rutt sér til rúms hin síðari ár og má m.a. sjá dæmi víðrar túlkunar í nýjustu matsskýrslu þjóðaröryggisráðs á ástandi og horfum í þjóðaröryggismálum: „Hugtakið fjölþáttaógnir vísar til samhæfðra og samstilltra aðgerða óvinveittra ríkja eða aðila tengdum ríkjum sem beita fjölbreyttum aðferðum, á skipulagðan hátt, til að nýta sér kerfislæga veikleika ríkja og/eða stofnana þeirra."[19] Í víðri túlkun hugtaksins eru hvorki hefðbundin hernaðógn né hefðbundnar hernaðaraðgerðir ófrávíkjanlegar forsendur þess að aðgerðir geti talist fjölþátta.

19 0689.pdf (althingi.is)

HVAÐ ERU FJÖLÞÁTTAÓGNIR

Í skýrslu fjölþjóðlegs verkefnis á þessu sviði frá árinu 2017 segir í formála að allir séu sammála um að „fjölþáttahernaður" sé áhyggjuefni en enginn skilji hvað í honum felist.[20]

Á sínum tíma kaus GRD að nota samsetta orðið fjölþátta yfir hybrid lið hugtakanna en þá höfðu ýmsir íslenskir sérfræðingar og áhugamenn um öryggis- og varnarmál þegar fjallað um hugtökin á opinberum vettvangi m.a. undir öðrum nöfnum s.s. „blandaðar ógnir", „blandað stríð" og „blönduð átök."

Hugtakið *fjölþáttaógnir* er iðulega notað til að ná utan um samtengt eðli áskorana (t.d. hryðjuverkaógn, kynþáttastríð, fólksflutninga, veikar stofnanir), margbreytileika gerenda (hefðbundinn herafla, herflokka, glæpahópa) og fjölbreytileika viðtekinna og óhefðbundinna aðferða sem beitt er (hernaði, alþjóðasamskiptum, tækni).

Þannig má segja að *fjölþáttaógnir* séu samsettar úr mismunandi þáttum sem fléttast saman og mynda á þann veg flóknari og marghliða ógn. „Fjölþáttaátök" (e. „Hybrid conflict") og „fjölþáttahernaður" (e. „Hybrid war") eru tvær ólíkar kvíar þar sem ríki eða pólitískir hópar beita fjölþáttaaðgerðum til að ná fram markmiðum sínum.

Með öðrum orðum lýsir hugtakið fjölþáttaógnir samtengdu eðli áskorana, margbreytileika gerenda og fjölbreytileika aðferða. **Segja má að hugtakið sé myndlíking, sem beitt er til að ná utan um ógnir, togstreitu og það flækjustig sem fylgir breyttu umhverfi alþjóðamála og tæknivæddri samfélagsgerð**.

Björn Bjarnason, fyrrverandi ráðherra, fjallar um *fjölþáttaógnir* í skýrslu sinni *Norræn utanríkis- og öryggismál* frá árinu 2020.[21] Og lýsir þar í stórum dráttum ýmsum eiginleikum *fjölþáttaógna* og aðferðum sem ríki og aðrir gerendur beita í *fjölþáttahernaði*. Í skýrslunni nefnir Björn sem dæmi aðgerðir og aðferðir á borð við: „*njósnir; áhrif á inntak upplýsinga; afskipti af kosningum; hugverkaþjófnað; nýtingu á veikleikum í grunnvirkjum á borð við orkuflutningsleiðir; efnahags- og viðskiptatengdar fjárkúganir; aðför að alþjóðlegum stofnunum, t.d. með því að gera regluverk óskilvirkt; hryðjuverk*

20 Understanding Hybrid Warfare (publishing.service.gov.uk); „The international consensus on 'hybrid warfare' is clear: no one understands it, but everyone, including NATO and the European Union, agrees it is a problem."

21 Norraen_utanrikis_og_oryggismal_2020_net.pdf (stjornarradid.is)

eða hræðsluáróður; ógnir við borgaralega flugumferð, skipaflutninga, raforkuflutningskerfi og [valda] *sjóslys*[um].“[22]

Í skýrslu Björns Bjarnasonar er einnig farið yfir leiðir sem beita má til að efla varnir gegn *fjölþáttaógnum* og eru fjögur lykilhugtök nefnd sem huga beri að í því samhengi en þau eru; ástandsmat (e. Situational awareness), viðnámsþol (e. Resilience), fælingarmáttur (e. Deterrence) og gagnráðstafanir (e. Countermeasures). Þá eru lagðar til aðgerðir til úrbóta s.s. að Norðurlöndin þrói samnorrænt ástandsmat vegna fjölþáttaógna auk þess er hugtakið allsherjarvarnir (e. Total Defence) kynnt sem mikilvæg leið varðandi stefnu í varnarmálum þar sem hún tekur bæði til almenns og hernaðarlegs öryggis.

Á vettvangi Þjóðaröryggisráðs hefur verið lögð rík áhersla á fjölþáttaógnir og hefur ráðið fjallað um þær í skýrslum sínum auk þess að standa fyrir málþingi og opnum fundi þar sem helstu áskoranir voru reifaðar. Forsætisráðherra Íslands, Katrín Jakobsdóttir, flutti inngangsorð á málþinginu um *fjölþáttaógnir* sem fram fór þann 27. febrúar 2020 í Hátíðasal Háskóla Íslands. Í samantekt Þjóðaröryggisráðs um málþingið kallar forsætisráðherra m.a. eftir að hugtök á borð við *fjölþáttaógnir* og -hernað séu krufin auk þess sem hún bendir á nauðsyn þess að byggja upp getu hér á landi til að fást við *hættur á gráu svæði*:

> **„Til að bregðast við þessu [fjölþáttaógnum] verða ríkisstjórnir að vera tilbúnar að samþykkja lög um allt frá því að skima erlendar fjárfestingar og beita refsiaðgerðum við netárásum, til þess að takast á við það sem kalla mætti hættur á gráu svæði. Það er einnig nauðsynlegt að byggja upp getu til að bera kennsl á og skilja spillandi starfsemi á byrjunarstigi og vekja almenningsvitund um vandamálið. Á sama tíma þurfum við einnig að brjóta til mergjar hugtök eins og fjölþáttaógnir og -hernað, án þess að líta á þau sem nýjungar. Þegar á miðjum fyrsta áratug 21. aldar voru slík hugtök hluti af öryggis- og hernaðarkenningum og við getum jafnvel farið aftur til föður innilokunarstefnunnar (e. containment) í upphafi kalda stríðsins, Georgs Kennan, sem árið 1948 skrifaði um takmarkanir hugmyndarinnar um skýran mun á stríði og friði. Í stuttu máli hafa hervald og herafli ávallt gert sér grein fyrir tvíræðninni á milli hernaðarátaka og pólitísks hernaðar. Hægt er hervæða upplýsingar og þær hafa verið hervæddar í hugmyndafræðilegum átökum. Nú er það oft notað á normalíseruðu máli til að grafa undan samfélagslegu trausti. Enginn vafi leikur á að sambland friðsamlegs pólitísks**

22 Ibid. Í upprunalegri enskri útgáfu skýrslunnar stendur „causing maritime incidents.“

> undirróðurs annars vegar og ofbeldis og ófriðar hins vegar hefur breikkað svið þeirra ógna sem fólk skynjar. Á hinn bóginn ef skilgreining fjölþáttaógna felur í sér of marga þætti er hætta á hugtakið verði óljóst.“[23]

HUGTÖKIN FJÖLÞÁTTAHERNAÐUR OG FJÖLÞÁTTAÓGNIR

Líkt og forsætisráðherra vék að í inngangsorðum málþingsins um fjölþáttaógnir er það svo að enn er að finna ólíkar skilgreiningar og skilning á *fjölþáttaógnum* í ýmsu alþjóðlegu samstarfi, innan fræðasamfélagsins og í opinberri umræðu sem gerir notkun þess ómarkvissa. Hér á eftir verður leitast við að skýra hugtökin líkt og kallað var eftir á málþingi þjóðaröryggisráðs í febrúarmánuði 2020.

Elsta dæmi um hugtakið *fjölþáttahernað* (e. hybrid war) sem GRD er kunnugt um er í bók Thomas R. Mockaitis; „British counterinsurgency in the post-imperial era“ frá árinu 1995. Í öðrum kafla bókarinnar er fjallað um fjölþáttahernað sem Indónesar háðu gegn Bretum m.a. á eynni Borneó í Indónesíu á sjöunda áratug síðustu aldar.[24]

Árið 2005 fjölluðu James N. Mattis hershöfðingi [síðar varnarmálaráðherra Bandaríkjanna] og Frank G. Hoffmann um hugtakið *fjölþáttahernað* (e. Hybrid War) og lýstu eiginleikum þess í stórum dráttum í stuttri grein í *Proceedings*, mánaðarriti u.s. Naval Institute, sú umfjöllun varð til þess að hugtakið náði töluverðri útbreiðslu.[25]

Tveimur árum síðar eða í desembermánuði 2007 skilgreindi Frank G. Hoffmann *fjölþáttastríð* í ritgerð sinni *Conflict in the 21st Century: The Rise of Hybrid Wars* fyrir Potomac stofnunina í Arlington, Virginíu.[26] Hann byggir þar m.a. á kenningum um fjórðu-kynslóðar hernað (e. Fourth-Generation Warfare), marglaga hernað (e. Compound War) og óheftan hernað (e. Unrestricted War) og setur fram eftirfarandi skilgreiningu:

> „Hybrid wars can be waged by states or political groups, and incorporate a range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder.“

23 Samtal um þjóðaröryggi: Fjölþáttaógnir (stjornarradid.is)
24 Höf. Mockaitis, Thomas R. Heiti British counterinsurgency in the post-imperial era. Útg: Manchester University Press, 1995
25 Future Warfare: The Rise of Hybrid Wars | Proceedings - November 2005 Vol. 131/11/1,233 (usni.org)
26 https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Sem þýða mætti á eftirfarandi hátt:

> **Ríki eða pólitískir hópar geta háð fjölþáttahernað, og nýtt fjölda mismunandi hernaðaraðferða þ.m.t. hefðbundna hernaðargetu, óhefðbundnar aðgerðir og liðsskipan, hryðjuverk þ.m.t. vægðarlaust ofbeldi og nauðung, og glæpi sem valda glundroða.**

Ljóst er af ritgerð Hoffmann að hugtaki hans er einkum ætlað að gagnast bandarískum stjórnvöldum og yfirstjórn heraflans við skipulag varnarmála Bandaríkjanna á 21. öldinni. Um er ræða „vígvallarhugtak" (sem ber að skilja í samhengi stríðsátaka) sem tekur bæði mið af hernaðarsögunni og jafnframt hinum miklu samfélags- og tæknibreytingum sem orðið hafa á þessari öld.[27] Hoffmann bendir á mikilvægi þess að stjórnvöld geti brugðist við fjölþáttaógnum á samhæfðan hátt, þrói og setji fram sviðsmyndir sem skori á hólm viðteknar hugmyndir um hernað um leið og öryggi mikilvægra innviða samfélagsins sé betur tryggt gegn skaða af mannavöldum.

Ýmsir hafa bent á varðandi skilgreiningu Hoffmann á fjölþáttahernaði og -ógnum að mörg dæmi um slíkan hernað og ógnir megi finna í sögunni a.m.k. frá dögum Pelópsskagastríðanna og því sé í raun ekki um nýmæli að ræða.[28] Hér þykir rétt að taka fram Hoffmann gerir ekki tilkall þess í ritgerð sinni að hafa fundið upp óhefðbundinn hernað. Hann segir beinlínis að í mörgum stríðum hafi slíkum aðferðum verið beitt (e. many wars have had regular and irregular components). Það sem virðist heldur vaka fyrir Hoffmann er að festa hendur á hvernig stríð 21. aldarinnar verði háð með orð prússneska hershöfðingjans Karl von Clausewitz (1780–1831) í huga um „að hver tími hafi sína eigin tegund af stríði, sín eigin takmarkandi skilyrði og fordóma."[29]

Í hugmynd Hoffmann felst sú hugsun, sem varla verður á móti mælt, að samtenging og samvirkni hinna mismunandi sviða nútímasamfélags sé með allt öðrum hætti og miklum mun meiri en í fábrotnari samfélögum fyrri tíma og þess vegna sé á vorum dögum t.d. hægt að hafa bein og afdrifarík áhrif á gang

27 Ibid. sjá m.a. bls. 43 „The rise of hybrid Warfare does not represent the defeat or the replacement of "the old-style warfare" or conventional warfare by the new. But it does present a complicating factor for defense planning in the 21st century. "Og bls. 11 „..., this does not eliminate the utility of the timeless Clausewitz or some 15 centuries of recorded military history before Westphalia. Quite the contrary, the Prussian theorist recognized that every age has its own conception of war. "

28 Murray, Williamson, and Peter R. Mansoor (eds). 2012. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge University Press: Cambridge.
Sjá t.d. bls. 3 „Despite its prominence as the latest buzz word in Washington, hybrid warfare is not new. Its historical pedigree goes back at least as far as the Peloponnesian War in the fifth century BC."(usni.org)

29 VomKriege-a4.pdf (clausewitz-gesellschaft.de) 3. hluti, kafli 8, bls. 357: „wie jede Zeit ihre eigenen Kriege, ihre eigenen beschränkenden Bedingungen, ihre eigene Befangenheit hatte."

mála á vígvellinum með árásum á mannvirki í órafjarlægð sem ekki var unnt með sama hætti í stríðum fyrri tíma.

Í grein í Armed Forces Journal þann 1. október árið 2009 fjallar Frank G. Hoffmann enn um skilgreiningu á fjölþáttaógnum, bregst við gagnrýni og fjallar lítillega um tilraunir annarra fræðimanna til að skilgreina fjölþáttógnir sem hann segir ekki nýjar af nálinni (e. „hybrid threats are not novel"). Í greininni skýrir Hoffmann hugsmíð (e. construct) sína um *fjölþáttaógnir* frekar og segir:

> **„Ég skilgreini fjölþáttaógn sem: hvern þann andstæðing sem samtímis aðlagar og samþættir hefðbundin vopn, óhefðbundnar aðferðir, hryðjuverk og glæpi á vígvellinum í því skyni að ná fram pólitískum markmiðum sínum."[30]**

Séu þær upplýsingar sem berast frá vígvöllum Úkraínu af árásarstríði Rússa bornar saman við skilgreiningar Hoffmann má ljóst vera að þar er um fjölþáttastríð að ræða.

NATO — FJÖLÞÁTTAÓGNIR

NATO fjallaði fyrst um fjölþáttaógnir árið 2010 í hernaðarstefnu bandalagsins. Þar var *fjölþáttaógnum* lýst sem þeim „ógnum sem stafar af óvinum sem ráða yfir getu til að beita samtímis hefðbundnum og óhefðbundnum aðferðum eftir aðstæðum hverju sinni í því skyni að ná fram markmiðum sínum."[31]

Rökstuðning fræðimanna fyrir því að slíkar aðgerðir teljist fremur til hernaðar en glæpa þ.e. hvenær aðgerðir fara yfir þröskuld stríðsyfirlýsingar og falli þess vegna undir alþjóðarétt um hernaðarátök er m.a. að finna í fjórða kafla Tallinn-handbókarinnar um alþjóðarétt og tölvuhernað sem unnin var að frumkvæði NATO í Öndvegissetri bandalagsins um netvarnir.[32]

Í samræmi við þann skilning á eðli *fjölþáttaógna* varaði Jens Stoltenberg, framkvæmdastjóri NATO, Rússa við að ráðast gegn mikilvægum innviðum NATO-ríkja í kjölfar umfangsmikilla skemmdarverka á gasleiðslum Nord Stream í Eystrasalti þann 26. september 2022. Jafnframt hét Stoltenberg því að NATO myndi efla varnir mikilvægra innviða bandalagsríkjanna.[33]

30 Armed Forces Journal – Hybrid vs. compound war : „I define a hybrid threat as: Any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battle space to obtain their political objectives."

31 „Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives." Sjá NATO Capstone Concept: http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

32 Sjá NATO Cooperative Cyber Defence Center of Excellence: https://issuu.com/nato_ccd_coe/docs/tallinnmanual

33 NATO warns Moscow against attacking allies' critical infrastructure | Reuters

Á HEIMASÍÐU NATO ERU VIÐBRÖGÐ BANDALAGSINS GEGN FJÖLÞÁTTAÓGNUM SETT FRAM Í SJÖ LIÐUM[34]

1. Ríki það sem fjölþáttaógn eða -árás beinist gegn ber meginábyrgð á gagnráðstöfunum. NATO ríkin hafa styrkt viðnámsþol sitt þ.m.t. gegn fjölþáttaógnum, og hafa aukið getu sína til að skilja þær fjölþáttaógnir sem steðja að bandalaginu í heild sinni.

2. NATO er reiðubúið að veita hverju aðildarríki aðstoð gegn fjölþáttaógnum sem þáttur í sameiginlegum vörnum. Bandalagið hefur þróað strategíu um hvert hlutverk þess er í vörnum gegn fjölþáttahernaði og liðveislu gegn slíkum ógnum.

3. Frá árinu 2016 hefur það verið yfirlýst stefna bandalagsins að fjölþáttaaðgerðir gegn einu eða fleiri bandalagsríkjum gætu leitt til þess að fimmta grein Atlantshafssáttmálans yrði virkjuð.

4. Í júlímánuði 2018 samþykktu leiðtogar NATO ríkjanna að koma á fót sérstökum stuðningsteymum gegn fjölþáttaógnum sem, að fenginni beiðni um aðstoð, veita bandalagsríkjunum sérsniðna markvissa hjálp við undirbúning og viðbrögð gegn fjölþátta aðgerðum.

5. NATO vinnur að því að styrkja samhæfingu við samstarfsaðila þ.m.t. Evrópusambandið í því skyni að vinna gegn fjölþáttaógnum.

6. Sameiginleg upplýsinga- og öryggisþjónusta NATO hefur á að skipa greiningardeild fjölþáttaógna sem vinnur að því að bæta ástandsmat (e. situational awareness).

7. Bandalagið vinnur með virkum hætti gegn falsfréttum og áróðri – ekki með meiri áróðri heldur með staðreyndum – á netinu, á ljósvakanum og í prentuðu máli.

34 „NATO - Topic: NATO's response to hybrid threats

Fjölþáttaógnir eru samkvæmt skilgreiningu NATO aðferðir fallnar til að gera greinarmun á stríði og friði óskýrari. **Þannig fela fjölþáttaógnir í sér að tengdar eru saman (samhæfðar) beinar hernaðarlegar ógnir og aðgerðir á borð við undirróðursherferðir, efnahagsþvinganir, netárásir og beitingu óhefðbundinna herflokka/málaliða sem formlega falla ekki undir herafla árásarríkisins.**[35] NATO hefur mótað stefnu til að verjast fjölþáttahernaði og jafnframt lýst því yfir að það sé reiðubúið að verja bandalagið og öll aðildarríki þess gegn hverri ógn hvort heldur hefðbundinni eða fjölþátta.

Á vettvangi NATO kemur fram að „fjölþátta-aðferðir við hernað"[36] á borð við áróður, blekkingar, skemmdarverk og annars konar aðferðir sem ekki eru hernaðarlegar í eðli sínu hafi löngum verið nýttar til að raska stöðugleika í óvinaríkjum. **Það nýja við þær aðferðir sem greina hafi mátt á síðustu árum felist í hraða, umfangi og ákafa sem komi til vegna örra tæknibreytinga og hnattvæddra samtenginga.**

Líkt og rakið var að framan telja sérfræðingar NATO að fjölþáttaógnir hafi lengi verið til staðar í krafti vel þekktra aðferða í gegnum söguna. Breytingin felist í möguleikum tæknibreytinga og samtengingum ríkja til að magna áhrif aðgerða. Jafnframt sé það skilgreiningaratriði um *fjölþáttaógnir* og nýjung í senn, að bandalagið kunni að standa frammi fyrir þaulskipulagðri getu óvinaríkja til að ná fram langtíma pólitískum markmiðum gagnstætt tilviljanakenndri rás atburða.

Öndvegissetur NATO um netvarnir, CCDCOE, var stofnað að frumkvæði Eistlands ásamt sex öðrum þjóðum — Þýskalandi, Ítalíu, Lettlandi, Litháen, Slóvakíu og Spáni — þann 14. maí 2008. Öndvegissetrið skipuleggur á ári hverju eina stærstu netvarnaæfingu heims, Locked Shields, sem líkir eftir stórri netárás. Æfingin snýr að því að verja upplýsingatækni- og herkerfi ásamt mikilvæga innviði. Sömuleiðis eru netöryggissérfræðingar og stjórnendur æfðir í strategískri ákvarðanatöku, fjölmiðlasamskiptum og gætt að því að ákvarðanir og upplýsingamiðlun fari að lögum.

35 NATO - Topic: NATO's response to hybrid threats Heimasíða NATO, sótt 30. des. 2022. „Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies.
The speed, scale and intensity of hybrid threats have increased in recent years. Being prepared to prevent, counter and respond to hybrid attacks, whether by state or non-state actors, is a top priority for NATO."

36 Ibid. „Hybrid methods of warfare– such as propaganda, deception, sabotage and other non-military tactics – have long been used to destabilise adversaries. What is new about attacks seen in recent years is their speed, scale and intensity, facilitated by rapid technological change and global interconnectivity."

Eitt af þekktustu rannsóknarverkefnum sem CCDCOE hefur staðið að er hin svokallaða Tallinn handbók (e. Tallinn Manual 2.0) sem er umfangsmesta greiningin á því hvernig gildandi alþjóðalög eiga við um netheima. Tallinn-handbókin er grundvallarrit á þessu sviði um heim allan. Netnjósnir eins og þeim er lýst í Tallinn-handbókinni og á vettvangi NATO eru af þeim toga að þar er um að ræða athæfi ríkja er varða alþjóðarétt. Í fyrstu útgáfu handbókarinnar 2013 var sjónum beint að netnjósnum af þeirri stærðargráðu að hernaður var að lögum talinn réttmætur sem svar við árásinni. Í seinni útgáfu Tallinn-handbókarinnar (2017) hefur netnjósnum ríkja undir þeim þröskuldi verið bætt við. Þriðja útgáfa, Tallin 3.0, er í undirbúningi.[37, 38, 39]

EVRÓPUSAMBANDIÐ (ESB) — FJÖLÞÁTTAÓGNIR

Á vettvangi ESB hefur á undanförnum árum verið unnið mikið starf varðandi fjölþáttaógnir. Hugtakið kemur fyrst fram á vettvangi ESB sumarið 2015 þegar Ráðið fjallaði um endurnýjun stefnu varðandi innra öryggi ESB. Eystrasaltsríkin og Pólland mæltu sérstaklega með innleiðingu hugtaksins, tillagan hlaut einhverja gagnrýni vegna tengingar hugtaksins við hernað. Á árunum 2016 og 2017 undir forsæti Hollands, Slóvakíu og Möltu skerpti Ráðið enn á mikilvægi *fjölþáttaógna* í stefnumótun sinni og færði þær framarlega á lista áskorana fyrir Varnarmálastofnun Evrópu (e. European Defence Agency).[40, 41]

Þrátt fyrir að aðgerðir gegn fjölþáttaógnum séu fyrst og fremst á ábyrgðarsviði hvers bandalagsríkis þá hefur ESB tekist á hendur að stuðla að og auka samvinnu á milli ríkja bandalagsins í baráttunni gegn þessari vá. Sömuleiðis hefur ESB unnið að stefnumótun og stuðlað að miðlun bestu starfsháttа á milli aðildarríkja.

Viðbrögð ESB við fjölþáttaógnum hvíla að meginatriðum til á grunni tveggja orðsendinga framkvæmdastjórnar ESB (e. European Commission) annars vegar frá árinu 2016 til Evrópuþingsins og Ráðsins um sameiginlega umgjörð um aðgerðir gegn *fjölþáttaógnum*. Um er að ræða aðgerðamiðaða

37 CCDCOE
38 The Tallinn Manual (ccdcoe.org)
39 TÁ eftirfarandi slóð má nálgast rafræna útgáfu af handbókinni: Tallinn manual 20 international law applicable cyber operations 2nd edition | Humanitarian law | Cambridge University Press
40 https://data.consilium.europa.eu/doc/document/ST-9798-2015-INIT/de/pdf
41 https://data.consilium.europa.eu/doc/document/ST-12396-2015-INIT/de/pdf sjá bls. 22: „Der Europäischen Verteidigungsagentur kommt dabei eine unterstützende Rolle zu. In Bereichen wie hybride Bedrohungen, maritime Sicherheit, Kriseneinsätze und Cybersicherheit sind eine verstärkte Zusammenarbeit mit Partnerorganisationen, insbesondere den VN, der OSZE, der NATO und der Afrikanischen Union, eine größere Komplementarität und der gegenseitige Informationsaustausch von zentraler Bedeutung."

orðsendingu sem hverfist um tiltekin viðbrögð og aðgerðir. Hins vegar orðsending frá árinu 2018 til Evrópuþingsins, Leiðtogaráðsins og Ráðsins varðandi eflingu viðnámsþols og getu til að sporna gegn fjölþáttaógnum. Orðsendingin er fremur stefnumiðuð í eðli og beinist að langtíma uppbyggingu viðnámsþols og getu gegn *fjölþáttaógnum*.[42, 43]

Í báðum fyrrgreindum orðsendingum er hugtakið *fjölþáttaógnir* skilgreint vítt. Í hinu fyrra segir að skilgreiningar á *fjölþáttaógnum* séu mismunandi og þurfi að vera sveigjanlegar til að bregðast við breytilegu eðli og þróun fjölþáttaógna. Enn fremur að hugtakið miði að því að ná yfir mismunandi þvingunar- og undirróðursstarfsemi, hefðbundnar og óhefðbundnar aðferðir (þ.e. diplómatískar, hernaðarlegar, efnahagslegar, tæknilegar), sem hægt er að nota á samræmdan hátt af ríkjum eða öðrum aðilum til að ná tilteknum markmiðum undir viðmiðunarmörkum þess sem telst til formlegrar stríðsyfirlýsingar.[44]

Í síðari orðsendingunni segir að fjölþáttaherferðir séu marghliða, samþætti þvingunar- og undirróðursaðgerðir, nýti bæði hefðbundin og óhefðbundin verkfæri og aðferðir (diplómatískar, hernaðarlegar, efnahagslegar, tæknilegar) til að grafa undan andstæðingnum. Þær séu hannaðar svo að erfitt sé að bera kennsl á þær og finna þann sem ber endalega ábyrgð, og getur verið hrint af stað af þjóðríkjum eða gerendum sem ekki teljast til þjóðríkja (e. Non-State Actors).[45]

Þrátt fyrir viðamikið starf innan ESB varðandi fjölþáttaógnir virðist enn skorta á sameiginlegan skilning á hugtakinu. Má í því samhengi nefna skýrslu sem unnin var að beiðni Sérstakrar nefndar Evrópuþingsins um erlenda íhlutun í lýðræðislegum stjórnarháttum innan ESB, þ.m.t. upplýsingaóreiðu (e. European Parliament's Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation).

42 Joint Communication To The European Parliament And The Council Joint Framework on countering hybrid threats sjá: EUR-Lex – 52016JC0018 – EN – EUR-Lex (europa.eu)

43 Joint Communication To The European Parliament, The European Council And The Council; Increasing resilience and bolstering capabilities to address hybrid threats sjá: EUR-Lex – 52018JC0016 – EN – EUR-Lex (europa.eu)

44 EUR-Lex – 52016JC0018 – EN – EUR-Lex (europa.eu): „While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare."

45 EUR-Lex - 52018JC0016 - EN - EUR-Lex (europa.eu) : „Hybrid campaigns are multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic, and technological) to destabilise the adversary. They are designed to be difficult to detect or attribute, and can be used by both state and non-state actors."

Skýrslan ber heitið Bestu starfshættir varðandi allsherjarvarnir samfélagsins gegn fjölþáttaógnum (e. Best Practices in the whole-of-society approach in countering hybrid threats) og er frá maí 2021.[46] Þar segir m.a. í samantekt á bls. v: „*Sérstakt vandamál við notkun á hugtökum er varða fjölþáttaógnir innan ESB er að ekki tekst að greina á milli mismunandi tegunda fjölþáttaógna og gerir þar með stefnumótendum erfitt fyrir að afmarka stofnanaábyrgð og móta markvissari gagnaðgerðir.*"[47]

Í skýrslunni Landslag fjölþáttaógna – hugmyndafræðilegt líkan (e. The Landscape of Hybrid Threats – a Conceptual Model) frá árinu 2021 sem unnin var sem samstarfsverkefni Sameiginlegu rannsóknarmiðstöðvar framkvæmdastjórnar ESB (e. Joint Research Center (JRC), European Commission's science and knowledge service) og Evrópska öndvegissetursins um aðgerðir gegn fjölþáttaógnum (e. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)) segir á bls. 9:

„*Hugtakið fjölþáttaógnir hefur í auknum mæli verið rætt innan fræða- og háskólasamfélagsins. Nýleg leit að hugtökunum fjölþáttaógnir og fjölþáttastríð í Google Scholar skilaði u.þ.b. 9.990 niðurstöðum, þar af voru flestar – eða um 6.970 – birtar frá 2014 (Babbage 2019).*[48] *Þetta er til marks um að hugtakið fjölþáttaógnir er komið til að vera. En þetta þýðir ekki að hugtakið hafi verið viðurkennt að fullu og merking þess skilin.*"[49]

Í marsmánuði 2022 samþykkti ESB svokallaðan *strategískan áttavita* (e. The Strategic Compass) sem ætlað er að veita sameiginlegt mat á því herfræðilega umhverfi sem ESB býr við og þeim ógnum og áskorunum sem Evrópusambandið stendur frammi fyrir. Í skjalinu eru settar fram skýrt mótaðar tillögur, um aðgerðir og framkvæmd þeirra ásamt nákvæmum tímasetningum um innleiðingu, sem ætlað er að gera ESB kleift að bregðast við á afgerandi hátt í hættuástandi og tryggja öryggi bandalagsríkjanna og vernda þegna þeirra.[50]

46 Best Practices in the whole-of-society approach in countering hybrid threats (europa.eu)

47 Ibid. „A particular problem with the EU's use of hybrid threat terminology is the way it fails to distinguish between different forms of hybrid threats, thereby making it difficult for policymakers to delineate institutional responsibilities and formulate more targeted countermeasures."

48 *Tilvitnun í Babbage, Ross. 2019. "Stealing a March: Chinese Hybrid Warfare in the Indo-Pacific: Issues and Options for Allied Defense Planners Volume II: Case Studies." Center for Strategic and Budgetary Assessments II: 1–51. https://csbaonline.org/uploads/documents/Ste aling_a_March_Annex_Final.pdf%0A25.

49 JRC Publications Repository - The landscape of Hybrid Threats: A Conceptual Model (Public Version) (europa.eu)

50 strategic_compass_en3_web.pdf (europa.eu)

Í *Strategíska áttavitanum* er að finna nýjustu skilgreiningu ESB á *fjölþátta-ógnum*: „*Fjölþáttaógnir hafa áhrif á og nýta veikleika í því skyni að valda skaða undir þröskuldi beinna stríðsaðgerða. Þær samþætta þvingunar- og undirróðursaðgerðir, hefðbundnar sem óhefðbundar aðferðir, notaðar á samhæfðan hátt þvert á fjölda sviða.*“

Jafnframt segir að einræðisstjórnir reyni í auknum mæli að grafa undan sameiginlegum lýðræðislegum gildum ESB og stuðli í eigin þágu að aukinni skautun innan Evrópu og noti til þess mismunandi tegundir fjölþáttaaðgerða (e. Hybrid activities) á borð við upplýsingamisnotkun, stafrænar árásir, efnahagsþvinganir, ólögmæta fólksflutninga o.fl.[51]

Í *Strategíska áttavita* ESB lýsa aðildarríkin vilja til að koma á laggirnar svokallaðri Verkfærakistu ESB gegn fjölþáttaógnum (e. EU Hybrid Toolbox) þar sem finna mætti tiltækar mótvægisaðgerðir sem snúa að forvörnum, samvinnu, uppbyggingu stöðugleika, hamlandi aðgerðum og stuðningsaðgerðum. Markmiðið með Verkfærakistunni er í fyrsta lagi að bera kennsl á flóknar og marghliða fjölþáttaherferðir og í öðru lagi að samhæfa sérsniðnar og þverlægar gagnaðgerðir.

Segja má að viðhorf ESB til *fjölþáttaógna* hafi þróast frá víðum skilningi hugtaksins þar sem reynt var að forðast tengingar við hernað yfir í nauðsyn þess að tryggja að hægt sé að greina og bregðast við *fjölþáttaógnum* með afgerandi hætti í æ öflugra samstarfi við NATO. Helst það í hendur við þá vaxandi ógn sem stafar að Evrópu og raunar Vesturlöndum öllum frá Rússlandi og öðrum einræðisríkjum sem með markvissum hætti vinna gegn grunngerð vestrænna lýðræðisríkja.

ESB OG NATO – SAMSTARF GEGN FJÖLÞÁTTAÓGNUM

Samskiptum NATO og ESB var komið í fastan farveg í upphafi aldarinnar, og byggði á skrefum sem stigin höfðu verið á tíunda áratug síðustu aldar til að auka varnargetu Evrópu með samstarfi NATO og Vestur-Evrópusambandsins.[52]

51 https://www.eeas.europa.eu/sites/default/files/documents/2022-03-28-countering-Hybrid-Threats_NewLayout.pdf : „Hybrid threats influence and exploit vulnerabilities to incur damage below the threshold of overt aggression. They are a mixture of coercive and subversive activities, conventional and unconventional methods, used in a coordinated manner across multiple domains.“

52 Understanding EU-NATO cooperation (europa.eu)

Árið 2023 gerðist Finnland aðildarríki NATO og eru 22 ríki hvoru tveggja aðildarríki að NATO og ESB.[53]

Meðal helstu áfanga í samstarfi NATO og ESB má nefna yfirlýsingu NATO og ESB um Evrópska öryggis- og varnarmálastefnu árið 2002 (e. NATO-EU Declaration on a European Security and Defence Policy (ESDP)) sem tryggði aðgang ESB að skipulagsgetu NATO vegna hernaðaraðgerða ESB. Árið 2003 lagði „Berlín plús" fyrirkomulagið grunninn að því að NATO gæti veitt ESB stuðning í hernaðaraðgerðum þrátt fyrir að NATO sem heild væri ekki virkjað.

Á leiðtogafundinum í Lissabon árið 2010 undirstrikuðu bandalagsríkin vilja til að efla strategíska samvinnu NATO og ESB sem svo var staðfest í Öryggisstefnu Atlantshafsbandalagsins 2010 (e. NATO Strategic Concept 2010). Í öryggisstefnunni er þeim áskorunum sem bandalagið stendur frammi fyrir á sviði öryggismála lýst ásamt því sem gerð er grein fyrir þeim pólitísku og hernaðarlegu verkefnum sem NATO mun sinna til að bregðast við þeim.

Í júlímánuði 2016 birtu NATO og ESB sameiginlega yfirlýsingu sem ætlað var að styrkja strategíska samvinnu í ljósi sameiginlegra áskorana m.a. að vinna gegn fjölþáttaógnum, efla stafrænt öryggi, auka viðnámsþol, upplýsingaskipti og samvinnu.[54] Í framhaldi aukins samstarfs NATO og ESB var grunnur lagður að Evrópska öndvegissetrinu um aðgerðir gegn *fjölþáttaógnum* (e. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)) sem styður aðildarríki til að efla getu sína, viðnámsþrótt og viðbúnað í baráttunni gegn fjölþáttaógnum.[55, 56, 57] Hybrid CoE var formlega stofnað 11. apríl 2017. Aðild er opin öllum NATO og ESB ríkjum. Fjöldi þátttökuríkja er 33 og árlegar tekjur Öndvegissetursins nema 3.6 milljónum evra árið 2023.[58, 59]

Haustið 2017 héldu ESB og NATO í fyrsta skipti samhliða og samstiga æfingar gegn *fjölþáttaógnum* (ESB hélt PACE17 æfinguna og NATO hélt æfinguna CMX17) þar sem viðbrögð og samvirkni gegn hugsanlegum áhrifum

53 NATO ríkin eru 31 : Albanía, Bandaríkin, Belgía, Bretland, Búlgaría, Danmörk, Eistland, Finnland, Frakkland, Grikkland, Holland, Ísland, Ítalía, Kanada, Króatía, Lettland, Litháen, Lúxemborg, Norður-Makedónía, Noregur, Portúgal, Pólland, Rúmenía, Slóvakía, Slóvenía, Spánn, Svartfjallaland, Tékkland, Tyrkland, Ungverjaland, Þýskaland.
ESB löndin eru 27: Austurríki, Belgía, Búlgaría, Danmörk, Eistland, Finnland, Frakkland, Grikkland, Holland, Írland, Ítalía, Króatía, Kýpur, Lettland, Litháen, Lúxemborg, Malta, Portúgal, Pólland, Rúmenía, Slóvakía, Slóvenía, Spánn, Svíþjóð, Tékkland, Ungverjaland, Þýskaland.

54 NATO - Official text: Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization , 08-Jul.-2016

55 What is Hybrid CoE? - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats

56 Security Compass (europa.eu)

57 Common set of proposals for the implementation of the Joint Declaration.pdf (hybridcoe.fi)

58 Hybrid CoE final Mou 110417

59 About us - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats

fjölþáttaógna voru könnuð og æfð. Sérstök áhersla var á miðlun strategískra upplýsinga (e. strategic communication), árið 2018 var önnur og flóknari æfing haldin, *Hybrid Exercise Multilayer 18*, þar sem fleiri viðbragðsaðilar innan sameiginlegu öryggis og varnarstefnunnar (e. Common Security and Defence Policy, CSDP) bættust í hópinn, þar voru m.a. viðbrögð við miklum straumi flóttamanna æfð. Á æfingum sem þessum leika margar skipulagsheildir NATO og ESB stóran þátt m.a: Fjölþáttaógnadeild ESB (e. EU Hybrid Fusion Cell), sem staðsett er innan miðstöðvar upplýsingasöfnunar (e. Intelligence Situation Centre, INTCEN) utanríkisþjónustu ESB (e. European External Action Service, EEAS) í Brussel en þar eiga öryggis- og leyniþjónustur aðildarríkja ESB fulltrúa, Starfshópur utanríkisþjónustu ESB um strategísk samskipti í austri (e. East Stratcom Task Force, ESTF); sem fæst m.a. við falsfréttir og áróður Rússa, Öndvegissetur NATO um strategísk samskipti staðsett í Ríga í Lettlandi (e. NATO Strategic Communications Centre of Excellence , NATO StratCom COE); sem hefur m.a. með höndum að afbyggja rússneskan áróður og koma á framfæri sjónarmiðum NATO og Vesturlanda, Greiningardeild fjölþáttaógna (e. Hybrid Analysis Branch) sem er innan Sameiginlegrar upplýsinga- og öryggisdeildar NATO (e. Joint Intelligence and Security Division, JISD). Núverandi staða er sú að upplýsingamiðstöðvar NATO og ESB (e. Intelligence Centres) vinna náið saman við gerð greiningar- og áhættumatsskýrslna varðandi fjölþáttaógnir.[60, 61, 62, 63, 64, 65, 66, 67, 68]

Þann 10. júlí 2018, birtu NATO og ESB sameiginlega yfirlýsingu um enn frekara samstarf varðandi hreyfanlegan herafla, baráttu gegn hryðjuverkum og aðgerðir til að efla viðnámsþol samfélagsins gegn ógnum sem stafa af gjöreyðingarvopnum svokölluðum CBRN ógnum (efnavopn, lífefnavopn, geislavirk vopn og kjarnorkuvopn). Jafnframt er tekið fram í yfirlýsingunni að hin margháttaða öryggisógn sem steðjar að bandalagsríkjum NATO og ESB úr austri og suðri geri að verkum að óhjákvæmilegt sé að dýpka og efla

60 FAQ: Joint Framework on countering hybrid threats (europa.eu)
61 EU launches exercise to test crisis management mechanisms in response to cyber and hybrid threats | EEAS Website (europa.eu)
62 FAQ: Joint Framework on countering hybrid threats (europa.eu)
63 https://ccdcoe.org/incyder-articles/eu-policy-on-fighting-hybrid-threats/
64 StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia (stratcomcoe.org)
65 2021 StratCom activity report - Strategic Communication Task Forces and Information Analysis Division | EEAS Website (europa.eu)
66 E-9-2022-001011-ASW_EN.pdf (europa.eu)
67 https://www.europarl.europa.eu/doceo/document//E-8-2017-005865-ASW_EN.html
68 NATO - IMS - Joint Intelligence and Security (JIS) Division

samstarfið enn frekar og þar með talið á sviði fjölþátta- og stafrænna ógna (e. „*including in responding to hybrid and cyber threats*“).[69]

Árið 2019 setti Ráðið á laggirnar sérstakan vinnuhóp gegn fjölþáttaógnum (e. Horizontal Working Group on Resilience and Countering Hybrid Threats, ERCHT). Hlutverk hans er að samþætta aðgerðir ESB gegn fjölþáttaógnum þvert á stofnanir og skipulagsheildir ESB. Vinnuhópurinn starfar innan ramma Strategíska áttavita ESB og hefur lagt áherslu á að fjölþáttaógnum sé mætt með samhæfðum viðbrögðum borgaralegra öryggisstofnana og herafla.[70]

Á leiðtogafundi NATO í Madrid í júní 2022 var ný öryggisstefna NATO samþykkt (NATO Strategic Concept 2022). Í henni kemur fram varðandi *fjölþáttaógnir*; að þær vegi að öryggi bandalagsríkjanna (grein 7), að mesta ógn við öryggi bandalagsríkjanna stafi frá Rússlandi og rússnesk stjórnvöld beiti m.a. fjölþáttaaðferðum til að ógna NATO ríkjum (grein 8) og að Kína leitist við skaða bandalagsríkin með fjölþáttaaðgerðum (grein 13).[71]

Í 27. grein öryggisstefnunnar 2022 segir um viðbrögð NATO gegn fjölþáttaógnum:

> **„Við munum fjárfesta í hæfni til að búa okkur undir, hindra og verjast pólitískum, efnahagslegum, orkutengdum, upplýsingatengdum þvingunum og annarskonar fjölþátta aðgerðum ríkja og sjálfstæðra aðila. Fjölþátta aðgerðir gegn bandalagsríkjum gætu jafngilt vopnaðri árás og því leitt til þess að Norður-Atlantshafsráðið virkjaði 5. gr. Norður-Atlantshafssáttmálans. Við munum áfram styðja samstarfsríki okkar til að bregðast við fjölþátta áskorunum og leitast við að hámarka samlegðaráhrif með öðrum viðeigandi aðilum, eins og Evrópusambandinu.“**[72, 73]

Í greininni er beinlínis gert ráð fyrir að fjölþáttaaðgerðir geti farið yfir þröskuld stríðsaðgerða og jafngilt beinni árás á bandalagsríki NATO og felst mikill fælingarmáttur í svo skýrri yfirlýsingu.

69 NATO - Official text: Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 10-Jul.-2018

70 https://www.consilium.europa.eu/de/council-eu/preparatory-bodies/horizontal-working-party-on-enhancing-resilience-and-countering-hybrid-threats/

71 https://www.nato.int/strategic-concept/

72 „We will invest in our ability to prepare for, deter, and defend against the coercive use of political, economic, energy, information and other hybrid tactics by states and non state actors. Hybrid operations against Allies could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty. We will continue to support our partners to counter hybrid challenges and seek to maximise synergies with other relevant actors, such as the European Union.“ Sjá https://www.nato.int/strategic-concept/

73 Þessi þýðing er fengin af vefsíðu Varðbergs, samtaka um vestræna samvinnu og alþjóðamál, vardberg.is, en samtökin birtu heildarþýðingu á NATO Strategic Concept á vefsíðu sinni á Þorláksmessu 2022. Varðberg þýðir enska hugtakið NATO Strategic Concept sem grunnstefna NATO og gefur það góða mynd af tilgangi og mikilvægi stefnunnar. Í þessari skýrslu er hugtakið þýtt sem öryggisstefna NATO í þeim skilningi að þar sé lýst þeim áskorunum sem NATO stendur frammi fyrir á sviði öryggismála og geri jafnframt grein fyrir þeim pólitísku og hernaðarlegu verkefnum sem NATO mun sinna til að bregðast við þeim. Grunnstefna NATO - Varðberg birtir textann á íslensku. | Varðberg, samtök um vestræna samvinnu og alþjóðamál (vardberg.is)

43. grein öryggisstefnu NATO 2022 er um samstarf NATO og ESB og nauðsyn þess að efla það enn frekar. Vikið er að nauðsyn þess að grípa til sameiginlegra gagnaðgerða varðandi stafrænar ógnir (e. cyber) sem og fjölþáttaógnir. Þarna er skýrt að orði kveðið um mikilvægi samstarfs NATO og ESB á sviði öryggis- og varnarmála.

Í janúarmánuði 2023 birtu NATO og ESB þriðju sameiginlegu yfirlýsinguna um aukna samvinnu.[74, 75] Við það tækifæri flutti Ursula von der Leyen forseti framkvæmdastjórnar ESB ræðu og sagði hún mest aðsteðjandi ógnir og áskoranir ESB og NATO tengjast Rússlandi og Kína og ljóst væri að byggja þyrfti upp viðnámsþol gegn þeim. Von der Leyen sagði að með yfirlýsingunni myndi samstarf NATO og ESB færast upp á nýtt stig og nefndi hún fjögur svið þar sem samstarfið myndi dýpka og aukast. Fyrst nefndi von der Leyen svið fjölþáttaógna, stafrænna ógna og ógna af völdum hryðjuverkastarfsemi, tók hún fram að varðandi þessar ógnir væri þegar til staðar náið samstarf en það yrði breikkað og dýpkað. Í annan stað nefndi Leyen nauðsyn þess að auka samstarf á sviði nýtækni og skerðandi tækni (e. emerging and disruptive technologies). Þriðja sviðið var loftslagsváin og fjórða og síðasta sviðið sem Leyen nefndi var uppbygging viðnámsþols og þá bæði hvað varðar samfélagsgerð sem og nauðsynlega innviði.[76]

Hér að framan voru í stuttu máli rakin viðbrögð og sívaxandi samvinna ESB og NATO í baráttunni gegn *fjölþáttaógnum*. Segja má að í viðbrögðum ESB og NATO við *fjölþáttaógnum* kristallist það samspil innra og ytra öryggis sem Lissabon sáttmálinn (e. Lisbon Treaty) gerði ráð fyrir.[77] Í aðgerðum og viðbrögðum gegn fjölþáttaógnum, hryðjuverkum og stafrænum ógnum hafa NATO og ESB samþætt hernaðarlega og borgaralega sérþekkingu m.ö.o. herir, öryggisþjónustur og löggæslustofnanir aðildarríkjanna hafa stækkað snertifleti sína og aukið gagnkvæma miðlun upplýsinga. Enda eru ógnir þessar með þeim hætti að þær krefjast heildstæðrar nálgunar á sviði öryggismála.

74 NATO - Official text: Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 10-Jan.-2023

75 Joint Declaration on EU-NATO Cooperation, 10 January 2023 - Consilium (europa.eu)

76 Statement by the President: EU-NATO Cooperation (europa.eu)

77 https://www.iss.europa.eu/sites/default/files/EUISSFiles/op89_The_internal-external_security_nexus_0.pdf

FJÖLÞÁTTAHERNAÐUR

Ólögmæt innrás Rússahers í Úkraínu og tortímingarstríðið í kjölfar hennar hefur með óyggjandi hætti sýnt hversu brýnt og aðkallandi verkefni það er að byggja upp getu til að bera kennsl á *fjölþáttaógnir* svo unnt sé að verjast þeim með gagnaðgerðum á upphafsstigum. Sömuleiðis er afar mikilvægt að efla viðnámsþol og fælingarmátt samfélagsins gegn *fjölþáttaógnum*. Ein forsenda þess er að sameiginlegur skilningur ríki um merkingu hugtaksins og hverjar afleiðingar og áhrif slíkra ógna kunni að verða.

Ógn verður ekki til án getu og ásetnings. Greinilegt er að með örri tækniþróun á ýmsum sviðum s.s. gervigreindar, djúpfölsunar og drónatækni hefur geta til að hrinda *fjölþáttaaðgerðum* í framkvæmd aukist til muna. Hvað ásetning varðar þá er stigvaxandi spenna á milli Rússlands og Vesturlanda til þess fallin að byggja undir eindreginn ásetning rússneskra stjórnvalda um að beita hverjum þeim aðgerðum og aðferðum sem tiltækar eru í því skyni að þvinga fram sigur á vígvöllum Úkraínu. Rússnesk stjórnvöld búa enn fremur yfir mikilli getu til að framkvæma *fjölþáttaaðgerðir*. Þá verður ekki undanskilinn sá möguleiki að rússnesk stjórnvöld beiti *fjölþáttaaðgerðum* gegn þeim ríkjum sem styðja stjórnvöld í Úkraínu. Raunar hafa þegar komið upp atvik sem flokka má undir *fjölþáttaaðgerðir* á Vesturlöndum þar sem grunur leikur á að gerendur gangi erinda rússneskra stjórnvalda og fjallað verður um í næstu köflum.

Eðli *fjölþáttaógna* er margvíslegt en margar þeirra eiga það sameiginlegt að beinast gegn almenningi, allsherjarreglu og stofnunum ríkisins og jafnframt að erfitt er að bera kennsl á þær og verjast þeim. Því er það svo að málaflokkur *fjölþáttaógna* er yfirleitt einnig á borði stofnana og skipulagsheilda er sinna málum á sviði þjóðaröryggis og löggæslu.

Af þeim skilgreiningum sem fjallað var um í fyrri köflum á hugtakinu *fjölþáttaógnir* má ráða að megin aðgreiningin lýtur að því hvort hefðbundin hernaðargeta sé áskilin eður ei. Ekki verður annað séð en að tilraunir til að útvíkka hugtakið og draga úr þætti hefðbundins hernaðar hafi vikið fyrir þeim skilningi að hefðbundin hernaðargeta árásaraðilans sé forsenda þess að *fjölþáttaógn* teljist trúverðug m.ö.o. að ef hefðbundin hernaðargeta er ekki til staðar sé ekki um fjölþáttaógn að ræða. Hefur árásarstríð Rússa í Úkraínu sýnt fram á réttmæti þessarar túlkunar. Jafnframt má líta til þess að ESB hefur

lagt áherslu á að tryggja að til staðar sé geta til gagnaðgerða þ.m.t. hefðbundin hernaðargeta. Niðurstaðan er því sú að *fjölþáttaógnir* séu tvíþættar þ.e. annars vegar hefðbundinn hernaður og hins vegar óhefðbundinn sem beitt sé í samspili undir þröskuldi beinna hernaðaraðgerða. Gegn samsettri ógn hefðbundins og óhefðbundins hernaðar getur verið erfitt að verjast þar sem um mismunandi og jafnvel breytilega samsetningu aðferða getur verið að ræða í hvert sinn sem árás er gerð.

Varðandi hinn hefðbundna hernað gilda ýmsar reglur og alþjóðasamningar en um hinn óhefðbundna engar. Ýmis siðferðisleg viðmið sem að einhverju leyti hafa mótað framgöngu herja í nútímahernaði, (að því gefnu að hægt sé að ræða hernað og siðferði yfirhöfuð þ.e. að siðferði og stríð séu ekki óásættanlegar andstæður) og miðast m.a. að því að gera þjáningar almennra borgara bærilegri. Slík siðferðisviðmið er ekki að finna í *fjölþáttastríði*. Þvert á móti beinast sumar aðgerðir fjölþáttastríðs sérstaklega gegn almenningi.

Í klassískum kenningum um *réttlátt stríð* (e. Just War), sem rekja má allt aftur til evrópsku miðaldakirkjunnar, er ein mikilvægasta reglan sú að óheimilt er að miða að því að drepa óbreytta borgara eða vinna verk sem hafa í för með sér mikið fall óbreyttra borgara, þótt ekki sé það tilgangur þeirra.[78]

Árásir Rússa gegn mikilvægum innviðum Úkraínu, víðsfjarri vígvellinum, svo sem sprengjuárásir, tölvu- og nethernaður sem og sprengjuárásir á íbúðahverfi, eru skýr dæmi um algert vægðarleysi rússneskra stjórnvalda gagnvart almenningi Úkraínu og eru í trássi við alþjóðalög.

Aðrar *fjölþáttaaðferðir* sem Rússar beita í Úkraínu eru síst skárri eins og beiting málaliðahópa. Er þar m.a. að nefna hinn illræmda Wagner-hóp sem staðið hefur fyrir ólýsanlegum ódæðum á vígvellinum og er nú að stórum hluta skipaður rússneskum refsiföngum. Ástæða þess að rússnesk stjórnvöld beita slíkum aðferðum er m.a. sú að með þeim hætti hyggjast þau afneita beinni ábyrgð sem er einn lykilþáttur í fjölþáttaaðgerðum.

Aðrar aðgerðir Rússa svo sem stórfelldur og kerfisbundinn stuldur menningarverðmæta, brottnám barna, kerfisbundnar nauðganir, pyntingar og

78 Er fælingarstefnan mönnum bjóðandi? Höfundur Eyjólfur Kjalar Emilsson (1953). Tímarit Skírnir 162. árgangur 1988. Vor, bls. 83-99. Grein sótt af Tímarit.is þann 14. desember 2022 klukkan 09:43 á vefslóðinni https://timarit.is/gegnir/000517999

aftökur og aðrir stórfelldir ofbeldisglæpir falla einnig undir skilgreiningu Hoffmann á *fjölþáttahernaði*.

Síðast en ekki síst gerir *fjölþáttahernaður* þjóðum erfiðara fyrir að fara eftir einni meginreglu réttláts stríðs sem er sú að ekki megi beita meira ofbeldi en nauðsynlegt er til að leiðrétta rangindin (e. principle of proportionality), m.ö.o. að gagnaðgerðir verða að vera í réttu hlutfalli við árásina og ekki umfram það afl sem þarf til að ná lokamarkmiði.[79] Slíkt er erfitt ef ekki er til staðar skýrt skilgreindur gerandi sem ber ábyrgð á rangindunum.

ÍSLAND – FJÖLÞÁTTAÓGNIR

Vestrænir leiðtogar hafa lýst áhrifum innrásar Rússa í Úkraínu sem tímahvörfum í evrópskri sögu og að þessi áratugur muni ráða úrslitum um hvernig meginreglur alþjóðasamskipta þróast; hvort lýðræðisleg og frjálslynd gildi haldi velli eða hvort einræði og stjórnlyndi vaxi úr hófi fram.[80, 81]

Íslenska þjóðin hefur frá upphafi skipað sér á bekk með vestrænum lýðræðisþjóðum enda eiga smáþjóðir allt sitt undir því að sjálfstæði þeirra, sjálfsákvörðunar- og fullveldisréttur sé að fullu virt. Sá einarði stuðningur sem íslensk stjórnvöld hafa sýnt Úkraínu er til marks um þessa afstöðu.

Ísland hefur tekið virkan þátt í aðgerðum NATO til að styrkja varnargetu Úkraínu m.a. með fjárframlögum, aðstoð við flutning búnaðar, sjúkragögnum, raforkubúnaði, þjálfun við sprengjuleit, vetrarfatnaði og móttöku flóttafólks. Sömuleiðis tekur Ísland þátt í þvingunaðgerðum alþjóðasamfélagsins gegn Rússum vegna hernaðar þeirra í Úkraínu.[82, 83, 84]

Afdráttarlaus stuðningur íslenskra stjórnvalda við Úkraínu hefur haft neikvæðar afleiðingar á samskipti Íslands og Rússlands. Rússnesk stjórnvöld hafa skilgreint Ísland sem óvinveitt ríki og talsmenn þeirra gagnrýnt íslensk stjórnvöld og málflutning íslenskra ráðamanna.

Í mati GRD varðandi fjölþáttaógnir frá 2019 segir: *„Að mati greiningardeildar ríkislögreglustjóra stafar Íslendingum ekki hernaðarógn af*

79 The Doctrine of Proportionality in a Time of War (core.ac.uk)
80 https://www.bundesregierung.de/breg-de/aktuelles/regierungserklaerung-von-bundeskanzler-olaf-scholz-am-27-februar-2022-2008356
81 https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/12/fact-sheet-the-biden-harris-administrations-national-security-strategy/
82 Government of Iceland | War in Ukraine - Iceland's response
83 https://www.stjornarradid.is/efst-a-baugi/frettir/stok-frett/2023/02/21/Raforkubunadur-af-ymsu-tagi-til-Ukrainu/
84 Stjórnarráðið | Þjálfun úkraínskra hermanna í sprengjuleit og sprengjueyðingu hafin (stjornarradid.is)

neinu ríki eða ríkjasambandi. Því fylgir að fjölþáttaógnir sem liður í viðleitni óvinaríkis til að vinna landsmönnum skaða eða tjón eru ekki til staðar nema að því leyti sem þátttaka Íslands í Atlantshafsbandalaginu og varnarsamstarf við Bandaríkjamenn gæti reynst óvinaríki tilefni til fjölþáttaárása. Af þessu leiðir að fjölþáttaógnir geta aðeins talist raunverulegar hvað Íslendinga varðar á spennu- eða átakatímum í samskiptum austurs og vesturs."

Fljótt skipast veður í lofti. Hinar umfangsmiklu breytingar í öryggis- og varnarmálum Evrópu sem orðið hafa með árásarstríði Rússa í Úkraínu gera að verkum að nauðsynlegt er að greina stöðu mála varðandi fjölþáttaógnir á Íslandi frá grunni.

Í öryggisstefnu NATO er Rússneska sambandsríkið talið mesta ógnin við öryggi bandalagsríkjanna og gert er ráð fyrir þeim möguleika að ráðist verði gegn fullveldi eða landamærahelgi þeirra. Í stefnunni eru m.a. tilgreindar fjölþáttaógnir sem bandalagsríkin skuldbinda sig að berjast gegn bæði með því að efla eigin viðnámsþrótt og fælingarmátt sem og í öryggissamstarfi við önnur NATO ríki þ.m.t. undirróður, ógnandi notkun herafla, upplýsingafölsun, ólögleg upplýsingaöflun, hugverkastuldur, veiking mikilvægra innviða og skerðing opinberrar þjónustu.[85]

ÓLÖGLEG UPPLÝSINGAÖFLUN

Ólögleg upplýsingaöflun er lögbrot sem heyrir undir lögbundið hlutverk GRD sem er m.a. að rannsaka og meta hættu og áhættu vegna brota er falla undir X. og XI. kafla almennra hegningarlaga nr. 19/1940, með síðari breytingum og veita ráðgjöf um viðbúnað sem hefur þýðingu fyrir hagsmuni ríkisins og þjóðhagslega mikilvæga starfsemi.[86]

Í X. kafla almennra hegningarlaga um landráð segir í 91. gr:

> **„Hver, sem kunngerir, skýrir frá eða lætur á annan hátt uppi við óviðkomandi menn leynilega samninga, ráðagerðir eða ályktanir ríkisins um málefni, sem heill þess eða réttindi gagnvart öðrum ríkjum eru undir komin, eða hafa mikilvæga fjárhagsþýðingu eða viðskipta fyrir íslensku þjóðina gagnvart útlöndum, skal sæta fangelsi allt að 16 árum.**

85 Sjá https://www.nato.int/strategic-concept/
86 404/2007 – Reglugerð um greiningardeild ríkislögreglustjóra. (island.is)

> **Sömu refsingu skal hver sá sæta, sem falsar, ónýtir eða kemur undan skjali eða öðrum munum, sem heill ríkisins eða réttindi gagnvart öðrum ríkjum eru undir komin.**
>
> **Sömu refsingu skal enn fremur hver sá sæta, sem falið hefur verið á hendur af íslenska ríkinu að semja eða gera út um eitthvað við annað ríki, ef hann ber fyrir borð hag íslenska ríkisins í þeim erindrekstri."**

Í 92. gr. segir:

> **„Hver, sem af ásetningi eða gáleysi kunngerir, lýsir eða skýrir óviðkomandi mönnum frá leynilegum hervarnarráðstöfunum, er íslenska ríkið hefur gert, skal sæta ... 1) fangelsi allt að 10 árum, eða sektum, ef brot er lítilræði eitt.**
>
> **Sömu refsingu skal hver sá sæta, sem af ásetningi eða gáleysi stofnar hlutleysisstöðu íslenska ríkisins í hættu, aðstoðar erlent ríki við skerðingu á hlutleysi þess, eða brýtur bann, sem ríkið hefur sett til verndar hlutleysi sínu."**

Og í 93. gr:

> **„Stuðli maður að því, að njósnir fyrir erlent ríki eða erlenda stjórnmálaflokka beinist að einhverju innan íslenska ríkisins eða geti beint eða óbeint farið þar fram, þá varðar það ... 1) fangelsi allt að 5 árum."**

Miklar viðsjár eru nú með NATO og Rússlandi. Vægðarlaus hernaður Rússa í Úkraínu í kjölfar ólöglegrar innrásar þeirra þann 24. febrúar 2022 hefur breytt grunnforsendum varðandi öryggis- og varnarmál á Vesturlöndum.[87]

Ólögleg upplýsingaöflun Rússa fer vaxandi innan Evrópu. Frá upphafi innrásarinnar í Úkraínu hefur mörg hundruð rússneskum sendiráðsmönnum verið brottvísað frá Vesturlöndum vegna gruns um njósnir eða tenginga við ólöglega upplýsingaöflun. Þessar brottvísanir hafa skert hefðbundna getu Rússa til njósnastarfsemi í viðkomandi löndum þó sendiráð þeirra séu enn virk í áróðursstríði Rússa vegna innrásarinnar í Úkraínu.[88]

Er það mat leyniþjónustustofnana á Norðurlöndum að ógn vegna aðgerða Rússa sem eru undir þröskuldi stríðs hafi aukist. Sömuleiðis að rússnesk stjórnvöld séu reiðubúin að taka meiri áhættu við ólöglega upplýsingaöflun þar sem hugsanlegur ávinningur sé álitinn meiri en skaðinn sem af getur hlotist.[89, 90]

Í Danmörku og Noregi er ólögleg upplýsingaöflun erlendra ríkja

87 290622-strategic-concept.pdf (nato.int)
88 Nearly 600 Russian diplomats expelled from Western countries since February 2022 - Russian Politics & Diplomacy - TASS
89 https://www.pst.no/globalassets/ntv/2023/ntv_2023_nor_web.pdf
90 https://www.reuters.com/world/europe/swedish-military-intelligence-says-threat-russia-has-increased-2023-02-20/

þ.m.t. rafræn/stafræn talin ógn við þjóðaröryggi og geti m.a. beinst gegn mikilvægum innviðum. Þann 6. október 2022 var tilkynnt um drónaflug yfir gaslindum Dana í Norðursjó. [91, 92]

Þann 13. apríl 2023 ráku norsk stjórnvöld 15 rússneska sendiráðsstarfsmenn úr landi í því skyni að draga úr njósnastarfsemi rússneskra stjórnvalda í Noregi.[86] Þá er svo komið að mikill meirihluti NATO – ríkja þar á meðal Finnland, Danmörk, Svíþjóð og Noregur hafa brottvísað miklum fjölda rússneskra sendiráðsmanna vegna gruns um ólöglega upplýsingaöflun.[93, 94, 95, 96, 97]

Rússar eru taldir beina ólöglegri upplýsingaöflun og stafrænum árásum gegn ríkjum sem styðja Úkraínu. Hópur netþrjóta sem tengjast Rússlandi eru taldir ábyrgir fyrir netárásum og tilraunum til ólöglegrar upplýsingaöflunar á Íslandi. Á árinu 2022 voru umfangsmiklar netárásir gerðar á vef lögreglunnar og tilraunir til að brjótast inn í tölvukerfi lögreglu og netaðgang starfsmanna.[92, 98, 99, 100, 101, 102, 103, 104, 105,106, 107]

Á vettvangi NATO er gengið út frá því að mjög miklar líkur séu á að rússnesk og kínversk stjórnvöld haldi uppi njósnum í aðildarríkjunum. Erlendar samstarfsstofnanir embættis ríkislögreglustjóra hafa upplýst að gera beri ráð fyrir að erlend ríki haldi uppi ólöglegum njósnum hér á landi.

Á árinu 2022 fjölgaði tilkynningum til GRD varðandi erlenda ríkisborgara sem hugsanlega tengjast ólöglegri upplýsingaöflun á Íslandi. Ýmsar breytingar á aðstöðu innan RLS hafa bætt til muna getu greiningardeildar ríkislögreglustjóra til að afla upplýsinga frá samstarfsþjóðum með skilvirkum hætti.

Með tilliti til njósna Rússa gagnvart aðildarríkjum NATO telst líklegt að rússnesk stjórnvöld skipi Íslandi ekki í forgangshóp ríkja sem þeir halda uppi

91 Denmark: drones reported near North Sea gas fields - Energynews.pro
92 Vurdering af spionagetruslen mod Danmark (pet.dk)
93 15 etterretningsoffiserer ved Russlands ambassade i Oslo erklæres uønsket i Norge - regjeringen.no
94 Finland expels two Russian diplomats | News | Yle Uutiset
95 Sweden joins European nations in expelling Russian diplomats | Reuters
96 Denmark expels 15 Russian diplomats; Moscow to retaliate | Reuters
97 Countries expel Russian diplomats in protest over Ukraine - U.S. Embassy & Consulates in Italy (usembassy.gov)
98 Curtailing Russia: Diplomatic Expulsions and the War in Ukraine (csis.org)
99 French government warns of increased risk of Russian espionage (lemonde.fr)
100 Russia is rebuilding its spy networks throughout Europe (lemonde.fr)
101 'Tip of the iceberg': rise in Russian spying activity alarms European capitals | Financial Times
102 Switzerland's Security 2022: The Federal Intelligence Service publishes its latest situation report (admin.ch)
103 Russia Increased Cyber Espionage Against Countries Supporting Ukraine, Microsoft Says - WSJ
104 In a Wary Arctic, Norway Starts to See Russian Spies Everywhere - The New York Times (nytimes.com)
105 NTV-2022 (pst.no)
106 vsd_uk.pdf (pet.dk)
107 Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression - Microsoft On the Issues

njósnum gegn. Þó verður að hafa í huga hernaðarlegt mikilvægi Íslands í Norður-Atlantshafi og hið mikla spennuástand vegna stríðsins í Úkraínu. Líklegt verður að telja að gefist tækifæri til að afla mikilvægra upplýsinga um afstöðu leiðtoga Evrópuríkja varðandi áframhaldandi stuðning við Úkraínu verði það reynt með lögmætum aðferðum eða eftir atvikum ólögmætum.

Ísland er aðildarríki NATO og verður sem slíkt að halda uppi sambærilegum varnarráðstöfunum varðandi upplýsingaöryggi og hin NATO ríkin. Afleiðingar þess að trúnaðarupplýsingar sem falla undir alþjóðlegar skuldbindingar Íslands komist í hendur óviðkomandi valda ekki einvörðungu hagsmunum Íslands tjóni heldur skaða þær einnig þær þjóðir sem íslenska ríkið á trúnaðarflokkuð upplýsingaskipti við. Á það við um alþjóðlegar skuldbindingar Íslands skv. reglugerð 959/2012. Afleiðingar er því ekki hægt að meta út frá hagsmunum Íslands eingöngu. Horfa verður til hagsmuna sem þau ríki eða bandalög geta orðið fyrir ef óviðkomandi fær aðgang að trúnaðarflokkuðum upplýsingum hér á landi.

Stundi erlend ríki njósnir á Íslandi í trássi við alþjóðalög er geta íslenskra stjórnvalda til að uppgötva eða koma í veg fyrir slíka starfsemi takmörkuð. Upplýsingar um einstaklinga og tengsl þeirra við leyniþjónustustofnanir liggja fyrir í einhverjum tilvikum þ.e. þegar slíkar upplýsingar berast frá erlendum samstarfsstofnunum embættis ríkislögreglustjóra.

Talið er líklegt að Rússar muni beita stafrænum njósnum í meira mæli og enn fremur er talið að Rússar séu reiðubúnir að notast við áhættusamari aðferðir við öflun upplýsinga og jafnvel að beita til þess ríkisborgurum annarra landa.

UNDIRRÓÐUR – UPPLÝSINGAFÖLSUN

Í x. kafla almennra hegningarlaga um landráð segir í 88. gr:

> **„Hver, sem opinberlega í ræðu eða riti mælir með því eða stuðlar að því, að erlent ríki byrji á fjandsamlegum tiltækjum við íslenska ríkið eða hlutist til um málefni þess, svo og hver sá, er veldur hættu á slíkri íhlutun með móðgunum, líkamsárásum, eignaspjöllum og öðrum athöfnum, sem líklegar eru til að valda slíkri hættu.“**

Í skýrslum frá norrænum leyniþjónustum segir að rússnesk stjórnvöld leitist við að hafa bein áhrif á stjórnmálamenn og -samtök og aðra þá sem koma að pólitískum ákvörðunum í samfélaginu í þeim tilgangi að halda að viðkomandi

rússneskum hagsmunum og afstöðu. Í því skyni að dylja þátt rússneskra stjórnvalda er gjarnan stuðst við milligöngumenn, aðila sem ekki er vitað að tengist beint rússneskum stjórnvöldum.

Nú geta erlend stjórnvöld og hópar þeim hlynntir/á þeirra vegum nýtt tölvutækni og náð til gríðarlegs fjölda fólks og miðlað lygum, áróðri og tilbúningi. Með notkun sérhannaðra algóritma (e. algorithms) er unnt að miðla „fölskum fréttum", áróðri, lygum og undirróðri til milljóna manna t.a.m. í tilteknu landi eða á tilteknu svæði. Þetta er að sönnu mikil breyting og tækifærin til slíkrar miðlunar í raun óendanleg.

Vestrænt lýðræði byggir m.a. á mál-, fjölmiðla- og skoðanafrelsi og því er það svo að miðlun lyga, áróðurs og „falskra frétta" varðar ekki nauðsynlega við lög og jafnframt blasir við að sífellt erfiðara verður að greina uppruna slíkrar miðlunar. Nútímaleg miðlun upplýsinga þekkir engin landamæri.

Rússar hafa beitt undirróðri gegn Eystrasaltsríkjunum þremur til að standa vörð um hagsmuni rússneskra minnihluta þar, halda uppi ógnandi framferði m.a. hótunum um hernaðaraðgerðir og hafa staðið fyrir leynilegum ofbeldisaðgerðum.

Nálgun Rússa er sú að „upplýsingastríð" sé liður í skipulögðum hernaði sem háður er í nafni hugmyndafræði. Þættirnir eru því þrír: hernaður, skipulag, hugmyndafræði. Áróðri og fölskum fréttum sem eiga uppruna sinn í Rússlandi og víðar er oftar en ekki miðlað til Vesturlandabúa um samfélagsmiðla.

Starfandi eru í Rússlandi sérstakar deildir innan öryggis- og leyniþjónustustofnana sem fást einvörðungu við gerð falskra frásagna og sálfræðihernað. Má þar nefna leyniþjónustu hersins GRU sem hefur sett upp deild sem ber heitið sérstök þjónustumiðstöð númer 72 (eða eining 54777) sem sérstaklega er tileinkuð sálfræðihernaði, falsfréttum og áróðursherferðum erlendis og nýtir sér stofnanir, staðgengla auk gervimannareikninga (e. Sock puppet account) á netinu til að, eftir atvikum, koma á framfæri eða hrekja sérstakar frásagnir.

Rússneska utanríkisleyniþjónustan SVR sem er arftaki KGB starfrækir stjórnstöð, Framkvæmdaráð MS, sem tileinkuð er því sem nefnist „virkar aðgerðir" og fæst einkum við að magna upp og breiða út ákveðnar frásagnir.

Auk þessa stofnaði Sergei Shoigu varnarmálaráðherra séstakar upplýsingahersveitir hersins, VIO, einvörðungu í því skyni að koma á framfæri villandi upplýsingum og áróðri. Við þetta bætist starfsemi FSB sem auk

ritskoðunar innanlands virðist nú leggja aukna áherslu á að „fara höndum um" stafrænar upplýsingar erlendis, sérstaklega beinast böndin að Miðstöð fyrir Upplýsingaöryggi öðru nafni miðstöð 18 sem talin er fara fyrir aðgerðum FSB á samfélagsmiðlum.

Síðast en ekki síst ber að nefna hlut Yevgeny Prigozhin eiganda Wagner-málaliðahópsins sem fyrr var nefndur í sambandi við hryðjuverk, mannréttindabrot, stríðsglæpi og önnur stórfelld afbrot en hann rak umfangsmikla falsfréttastofnun Rannsóknarstofnun Internetsins (e. Internet Research Agency) sem meðal annars hefur verið beitt gegn lýðræðislegum ferlum á Vesturlöndum, gegn NATO og Úkraínu.[108, 109, 110, 111, 112, 113, 114]

Frá því að innrásin í Úkraínu hófst hafa Rússar með virkum hætti m.a. í gegnum sendráð sitt á Íslandi komið fram áróðri, fölskum upplýsingum og illa dulbúnum hótunum í fjölmiðlum og samfélagsmiðlum.

Umfangsmikill áróður rússneskra stjórnvalda hefur hlotið nokkurn hljómgrunn innan evrópu og ýmsir fréttamiðlar birt greinar og skoðanir þar sem tekið er undir málstað og falsfréttir sem ættaðar eru frá framangreindum stofnunum og nettröllaverksmiðjum.

ÓGNANDI BEITING HERAFLA

Rússar hafa á síðustu árum aukið hernaðarumsvif á norðurslóðum. Það ásamt því að Rússar hafa skilgreint Ísland sem óvinaríki setur ítrekaðar ögranir þeirra nálægt íslenskri loft- og landhelgi í nýtt og mun alvarlegra samhengi.[115]

Rússar hafa allt frá brotthvarfi bandaríska setuliðsins frá Íslandi sent langdrægar sprengjuflugvélar í leiðangra nærri íslensku loftrými sem loftrýmisgæsla NATO hefur þurft að bregðast við. Sömuleiðis hefur kafabátaumferð aukist og þannig kallað á fasta viðveru bandarískra P8 flugvéla í Keflavík til kafabátaeftirlits.

Nýmæli var hringsigling tundurspillisins Severomorsk umhverfis Ísland í ágústmánuði 2021 ásamt tveimur aðstoðarskipum dráttabátnum Pamir

108 How Russia's military intelligence agency became the covert muscle in Putin's duels with the West - The Washington Post
109 Sock puppet account - Wikipedia
110 Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections | U.S. Department of the Treasury
111 Russia sets up information warfare units - defence minister | Reuters
112 DisinfoDigest: Russian Intelligence Controlled Platforms, Chinese Sanctions Disinformation and More - DisinfoWatch
113 Updated Copy of Fronton_report (hubspotusercontent-na1.net)
114 Wagner chief admits to founding Russian troll farm sanctioned for meddling in US elections - CNN
115 Russian government approves list of unfriendly countries and territories - Russian Politics & Diplomacy - TASS

og olíubirgðaskipinu Sergei Osipov. Severomosk er ríflega 150 metra langt herskip, búið bæði flugskeytum og tundurskeytum. Herskipið hefur einnig tveimur þyrlum á að skipa sem m.a. eru ætlaðar í kafbátahernað auk þess er Severomosk búið tækjum til að trufla rafeindabúnað og -samskipti. Á Norður-Atlantshafi búa Rússar þannig yfir getu t.d. til að trufla samskipti og jafnvel staðsetningarbúnað skipa. Sá möguleiki er fyrir hendi að slík árás gæti haft áhrif á siglingar til og frá Íslandi og þannig valdið efnahagslegum skaða hið minnsta.

Ekki hefur enn fengið staðfest hver raunverulegur tilgangur þessarar hringsiglingar var en ekki verður undan því vikist að setja hana í samhengi við innrásina í Úkraínu hálfu ári síðar þ.e. að rússneski flotinn hafi verið að æfa einhvers konar sviðsmynd varðandi hernað í Evrópu. Reynist sú ályktun eiga við rök að styðjast má ljóst vera hverjar afleiðingar kunna að verða fari svo að átökin í Úkraínu magnist enn.[116, 117]

HRYÐJUVERK – SKEMMDARVERK

Hryðjuverk eða skemmdarverk sem veikja mikilvæga innviði og/eða skerða opinbera þjónustu þannig að stjórnskipun eða stjórnmálalegar, efnahagslegar eða þjóðfélagslegar undirstöður ríkis eða alþjóðastofnunar skaðist eru lögbrot sem falla undir lögbundið hlutverk GRD sem er m.a. að meta hættu og áhættu vegna brota er falla undir X. og XI. kafla almennra hegningarlaga nr. 19/1940, með síðari breytingum og veita ráðgjöf um viðbúnað sem hefur þýðingu fyrir hagsmuni ríkisins og þjóðhagslega mikilvæga starfsemi.[118]

Í XI. kafla almennra hegningarlaga um landráð segir í 100. gr. a:

> **„Fyrir hryðjuverk skal refsa með allt að ævilöngu fangelsi hverjum sem fremur eitt eða fleiri af eftirtöldum brotum í þeim tilgangi að valda almenningi verulegum ótta eða þvinga með ólögmætum hætti íslensk eða erlend stjórnvöld eða alþjóðastofnun til að gera eitthvað eða láta eitthvað ógert eða í því skyni að veikja eða skaða stjórnskipun eða stjórnmálalegar, efnahagslegar eða þjóðfélagslegar undirstöður ríkis eða alþjóðastofnunar:**

116 „In the past few years, Russia's military activities in the region that impact on neighbouring countries have markedly increased"; Russia in the Arctic. Development Plans, Military Potential, and Conflict Prevention (swp-berlin.org)

117 The Russian Arctic Threat: Consequences of the Ukraine War (csis.org)

118 Russian government approves list of unfriendly countries and territories - Russian Politics & Diplomacy - TASS

1. manndráp skv. 211. gr.,

2. líkamsárás skv. 218. gr.,

3. frelsissviptingu skv. 226. gr.,

4. raskar umferðaröryggi skv. 1. mgr. 168. gr., truflar rekstur almennra samgöngutækja o.fl. skv. 1. mgr. 176. gr. eða veldur stórfelldum eignaspjöllum skv. 2. mgr. 257. gr. og þessi brot eru framin á þann hátt að mannslífum sé stefnt í hættu eða valdið miklu fjárhagslegu tjóni,

5. flugrán skv. 2. mgr. 165. gr. eða veitist að mönnum sem staddir eru í flughöfn ætlaðri alþjóðlegri flugumferð skv. 3. mgr. 165. gr.,

6. brennu skv. 2. mgr. 164. gr., veldur sprengingu, útbreiðslu skaðlegra lofttegunda, vatnsflóði, skipreika, járnbrautar-, bifreiðar- eða loftfarsslysi eða öfórum annarra slíkra farar- eða flutningatækja skv. 1. mgr. 165. gr., veldur almennum skorti á drykkjarvatni eða setur skaðleg efni í vatnsból eða vatnsleiðslur skv. 1. mgr. 170. gr. eða lætur eitruð eða önnur hættuleg efni í muni, sem ætlaðir eru til sölu eða almennrar notkunar, skv. 1. mgr. 171. gr.“

Haustið 2022 voru unnin skemmdaverk innan Evrópu m.a. á mikilvægum innviðum sem tengjast orkuflutningum, samgöngum og samskiptum og sömuleiðis hefur orðið vart við drónaflug nálægt orkuinnviðum. Mörg ríki Evrópu hafa brugðist við með því að efla öryggisgæslu og varnargetu.

Þann 8. október var unnið skemmdarverk á lestakerfinu í Norður-Þýskalandi þegar mikilvægir kaplar voru skornir sundur á tveimur stöðum með þeim afleiðingum að lestarsamgöngur lágu niðri. Samgönguráðherra Þýsklands, Volker Wissing , sagði ljóst að um skipulegt illvirki hefði verið að ræða.[119] Þann 18. október voru neðansjávarkaplar nærri Hjaltlandseyjum rofnir sem orsakaði sambandsleysi og talsverða röskun.[120]

Þann 21. mars 2023 kynnti Jens Stoltenberg, framkvæmdastjóri NATO, ársskýrslu bandalagsins fyrir árið 2022. Þar er sérstök áhersla lögð á að efla varnir mikilvægra innviða bandalagsríkjanna og þar með talið samskiptakapla og orkuinnviða sem liggja neðansjávar. Stoltenberg kynnti stofnun sérstakrar Samhæfingarstofu neðansjávarinnviða (e. Undersea Infrastructure Coordination Cell) og sameiginlegan verkefnahóps NATO og ESB (e. Joint NATO-EU Task Force). [121]

119 Malicious and targeted' sabotage halts rail traffic in northern Germany | Reuters

120 Damaged cable leaves Shetland cut off from mainland - BBC News

121 NATO - News: NATO Secretary General launches his Annual Report for 2022 , 21-Mar.-2023

Stjórnvöld á Vesturlöndum hafa nú um árabil haft auknar áhyggjur af öryggi samskiptakapla og orkuinnviða sem liggja óvarðir neðansjávar. Mikil umfjöllun hefur verið um þessa vaxandi ógn og sum ríki Evrópu þegar brugðist við með því að auka verulega útgjöld til að tryggja öryggi neðansjávar samskipta- og orkukapla. Bresk stjórnvöld hafa tilkynnt um kaup á sérstökum fjölnota eftirlitsskipum sem eru ætluð eru til að tryggja betur öryggi neðansjávar-innviða. Frönsk stjórnvöld hafa aukið verulega fjármagn til að tryggja „sjávarbotnsvarnir".[122, 123, 124, 125, 126, 127, 128, 129, 130]

Rússnesk skip hafa undanfarin misseri ítrekað hagað ferðum sínum á þann veg að þau gætu sem hægast verið að kortleggja hvar neðansjávarkaplar liggja. Nú síðast í marsmánuði vöktu tvö rússnesk skip athygli írska hersins þar sem þau héldu sig nærri hinum nýja fjarskiptastreng, IRIS, sem tengir Ísland og Írland.[131, 132, 133]

Mögulegar aðgerðir á slíkum spennutímum gætu einnig varðað öryggi tengistöðva þar sem samskiptakaplar neðansjávar eru teknir á land. Þar kann vörnum og eftirliti að vera ábótavant enda teljast þetta borgaraleg mannvirki. Skemmdarverk á þessum búnaði á landi eru möguleiki og í sumum tilvikum gæti reynst einfaldara er fyrir óvinaríki að beita þeirri aðferð fremur en að rjúfa sæstrengi á hafi úti.

Tugum milljarða íslenskra króna hefur verið varið til uppbyggingar varnartengdra mannvirkja í Keflavík undanfarin ár vegna breyttrar stöðu á Norður-Atlantshafi. Enn frekari framkvæmdir varðandi rekstur, viðhald og endurbætur varnarmannvirkja á Íslandi og önnur uppbygging eru deiglunni á næstu árum. Ljóst er að tryggja þarf öryggi varnarmannvirkja NATO á Íslandi og lögregla gegnir þar lykilhlutverki.[134, 135]

Í nýlegri greiningarskýrslu (júní 2022) um mikilvæga neðansjávar samskiptainnviði ESB sem unnin var fyrir Evrópuþingið er á kerfisbundinn hátt

122 20220214_FRENCH SEABED STRATEGY.pdf (defense.gouv.fr)
123 The threat to Britain's undersea cables | The Spectator
124 France tightens subsea cable security amid growing fear of sabotage – POLITICO
125 Admiral Sir Tony Radakin warns of Russian threat at sea (thetimes.co.uk)
126 Sabotage or Accident: Was Russia or a fishing trawler responsible for Shetland Island cable cut? – Technology Blog (comsoc.org)
127 Putin knows that undersea cables are the west's Achilles heel | Financial Times (ft.com)
128 France to dive deeper for undersea security after Nord Stream attacks | Reuters
129 Protecting seabed infrastructure – UK Multi-Role Ocean Surveillance Ship to be in service by 2023 | Navy Lookout
130 Concern over underwater cables with Russian ships off Irish coast (breakingnews.ie)
131 Russia Cripples NATO's Undersea Communications | Warsaw Institute
132 Russians may have been mapping cables off Ireland since 2014, expert claims (irishexaminer.com)
133 Herinn vill milljarða fjárfestingu (mbl.is)
134 0689.pdf (althingi.is)
135 Unseen and underhand: Putin's hidden hybrid war is trying to break Europe's heart | Simon Tisdall | The Guardian

farið yfir núverandi öryggisógnir, uppruna þeirra sem og hugsanlega ógnvalda. Skýrslan byggir á traustum sérfræðigrunni og gerir m.a. úttekt á núverandi viðbúnaðar- og viðbragðskerfi innan aðildarríkja ESB. Einnig eru settar fram ráðleggingar um hvernig megi bæta viðnámsþol og öryggi neðansjávar samskiptakapla.[136]

NATO hefur lýst því yfir að bandalagið hafi mótað stefnu til að verjast fjölþáttahernaði og að það sé reiðubúið að verja bandalagið og öll aðildarríki þess gegn hverri ógn, hvort heldur hefðbundinni eða fjölþátta. Þannig veitir NATO-aðildin Íslendingum vörn gagnvart slíkum ógnum og styður við þá getu sem fyrir er í landinu.[137, 138]

NET- OG TÖLVUÁRÁSIR

Frá innrás Rússa í Úkraínu hefur tíðni netárása á NATO ríki margfaldast. Ísland hefur ekki verið undanþegið þeirri þróun. Reyndar er það svo að net- og tölvuárásir eru vaxandi áhyggjuefni fyrir stjórnvöld, fyrirtæki og einstaklinga m.a. vegna þess hversu hratt tæknin þróast og hve auðvelt getur verið að nýta hana til ólögmætrar og skaðlegrar starfsemi.

CERT-IS er netöryggissveit íslenskra stjórnvalda með áherslu á mikilvæga innviði. Árið 2020 voru tilkynnt 266 netárásir hjá CERT IS og samkvæmt CERT IS hefur atvikum fjölgað jafnt og þétt og fóru þau yfir 700 á árinu 2022.

136 Security threats to undersea communications cables and infrastructure – consequences for the EU (europa.eu)
137 NATO warns Moscow against attacking allies' critical infrastructure | Reuters
138 Germany, Norway seek NATO-led hub for key undersea structures (france24.com)

MEÐAL ALVARLEGRA NET- OG TÖLVUÁRÁSA Á ÍSLANDI ÁRIÐ 2022 ÞAR SEM SPILLIFORRITUM VAR BEITT MÁ NEFNA

JANÚAR	Gagnaleki hjá Strætó
FEBRÚAR	Ó. Johnson & Kaaber spilliforrit lamar innar starf
MAÍ	Neyðarlínan tilkynnir að fjögur hundruð þúsund netárásir á einum sólarhring
JÚLÍ	Þjónustukerfi Lyfjastofnunar gert óstarfhæft
JÚLÍ	Gagnaleki hjá Reykjavíkurborg
ÁGÚST	Netárás á Fréttablaðið í framhaldi af gagnrýni frá rússneska sendiráðinu í tengslum við fréttaflutning.
SEPTEMBER	Spilliforrit truflar starfsemi Tækniskólans

Árið 2022 voru sömuleiðis gerðar umfangsmiklar tilraunir til að brjótast í tölvukerfi lögreglu af rússneskum tölvuþrjótum að talið er, bæði á logreglan.is og á netaðganga starfsmanna.

Í nýrri skýrslu frá 16 febrúar 2023 sem ber heitið „Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape" frá net- og tölvuöryggisfyrirtæki Google, Mandiant, Google Trust & Safety ásamt Áhættugreiningarhópi Google (e. Google Threat Assessment Group, TAG) eru stafrænar árásir Rússa í kjölfar innrásarinnar í Úkraínu greindar. Niðurstöðurnar sýna svo ekki verður um villst að Rússar hafa lagt mikla áherslu á skerða mikilvæga net- og tölvuvirkni innan Úkraínu en sömuleiðis er staðfest að stafrænar árásir Rússa á NATO ríki árið 2022 hafi aukist um 300% frá árinu 2020.[139]

139 google_fog_of_war_research_report.pdf

ÞRJÁR MEGINNIÐURSTÖÐUR SKÝRSLUNNAR FOG OF WAR

1. Ógnvaldar studdir af rússneskum stjórnvöldum hafa hrint af stað margþátta net- og tölvuárásum í því skyni að öðlast herfræðilega yfirburði í stríðinu í Úkraínu með árásum sem beinast m.a. gegn úkraínsku ríkisstjórninni og mikilvægum innviðum landsins. Sömuleiðis hefur orðið veruleg aukning í vefveiðum sem beinast gegn NATO-ríkjum og aukning í stafrænum aðgerðum (e. Cyber operations) sem miða að því að styðja fjölmörg markmið rússneskra stjórnvalda; ógnvaldar brjótast inn á netsvæði og leka þaðan upplýsingum til að styrkja narratívu rússneskra stjórnvalda.

2. Stjórnvöld í Moskvu hafa nýtt sér alla þá möguleika sem í boði eru til að móta skoðun almennings á stríðsátökunum með áróðurs- og upplýsingaherferðum, allt frá ríkisstyrktum fjölmiðlum niður í leynilega vefvanga og vefreikninga. Markmið þessara áróðurs- og upplýsingaherferða eru einkum af þrennum toga; í fyrsta lagi að grafa undan ríkisstjórn Úkraínu, í annan stað að brjóta niður stuðning við Úkraínu á alþjóðavettvangi og hið þriðja er að halda uppi stuðningi við stríðið innan Rússlands.

3. Breytingar hafa orðið innan austur-evrópskra netbrotahópa sem að öllum líkindum munu hafa langvarandi breytingar á stafræna brotastarfsemi á heimsvísu svo og á samhæfingu og samvinnu netbrotahópa.

Leyniþjónusta rússneska hersins, GRU, er talin standa fyrir stórum hluta þess net- og tölvuhernaðar sem stöðugt beinist gegn Úkraínu og NATO-ríkjunum. Hópar sem tengdir eru GRU sýna vel hversu mismunandi svið stafrænna aðgerða (e. cyber activity) geta skarast. Þannig fer fram á vegum GRU upplýsingaöflun, skerðandi netárásir og stuðningur við áróðurs- og upplýsingaherferðir. GRU hóparnir sem skýrslan nefnir eru annars vegar Frozenbarents (öðru nafni Sandworm, Voodoo Bear og Iridium) og hins vegar Frozenlake (öðru nafni APT28, SOFACY, Fancy Bear, Strontium og Sednit). Þessir hópar láta til sín taka við auðkennanám/-stuld (e. Credential phising), dreifingu spilliforrita og áróðurs- og

upplýsingaherferða en talið er að GRU nálgist og samhæfi aðgerðir sínar við hópa aðgerðasinnaðra hakkara (e. Hacktivists) í því skyni að móta narratívuna og upplýsingaumhverfið í hag rússneskra stjórnvalda.

Í skýrslunni er rakið hvernig þriðji hópurinn Coldriver (öðru nafni Gossamer Bear, Callisto Group, Seaborgium og TA446) einbeitir sér að árásum á NATO ríki, í marsmánuði 2022 réðist hópurinn t.d. gegn Öndvegissetri NATO og herjum margra NATO ríkja.

Höfundar áðurnefndrar skýrslu „Fog of War" leggja mat á framtíðarhorfur varðandi stafrænar árásir Rússa og meta með mikilli vissu (e. High confidence) að rússnesk stjórnvöld muni styðja ógnvalda til áframhaldandi netárása gegn Úkraínu og NATO ríkjum í því skyni að ná rússneskum hernaðarmarkmiðum.

Þeir meta einnig með mikilli vissu (e. High confidence) að stjórnvöld í Moskvu muni auka umfang og afl stafrænna árása til að bregðast við þróun á vígvellinum sem gæti talist hagfelld Úkraínu (t.d. nýjar erlendar skuldbindingar um að veita pólitískan eða hernaðarlegan stuðning o.s.frv.). Þessar net- og tölvurásir muni fyrst í stað beinast gegn Úkraínu en í auknum mæli taka einnig til NATO ríkja.

Höfundarnir meta með hóflegu trausti (e. Moderate confidence) að Rússland haldi áfram að auka bæði hraða og umfang upplýsingaaðgerða sinna til ná þeim markmiðum sem lýst er hér að ofan, sérstaklega varðandi lykilákvarðanir eins og alþjóðlegs fjármögnun, hernaðaraðstoð, þjóðaratkvæðagreiðslur innanlands og fleira. Höfundar segja óljósara hvort þessar stafrænu aðgerðir Rússa muni ná tilætluðum árangri, eða hvort þær muni skila sér í harðnandi andstöðu gegn yfirgangi Rússa.[140]

Í Danmörku hefur frá árinu 2012 verið starfrækt sérstök Miðstöð Stafrænna Varna (e. Centre For Cyber Security) sem hefur það verk með höndum að ráðleggja stjórnvöldum jafnt sem einkafyrirtækjum, sem styðja við starfsemi mikilvægra innviða, um hvernig skuli fyrirbyggja, verjast og bregðast við stafrænum árásum. Í kjölfar hernaðar Rússa í Úkraínu hefur miðstöðin gefið út tug skýrslna er varða stafrænt öryggi í Danmörku og þá auknu hættu sem talin er á net- og tölvuárásum af hálfu rússneskra stjórnvalda eða aðgerðasinna sem styðja rússnesk stjórnvöld.[141]

140 google_fog_of_war_research_report.pdf **141** Threat assessments (cfcs.dk)

Þann 14. mars 2023 birti Miðstöð Stafrænna Varna (MSV) áhættumatsskýrslu vegna stafrænna aðgerðasinna (e. Cyberactivist). Þar er ógn vegna aðgerðasinna metin í fjórða og næsthæsta þrepi (e. High). Matið er byggt á upplýsingum um mikla virkni hakkarahópa sem styðja rússneskan málstað og vegna getu og ásetnings þeirra til að ráðast gegn dönskum skotmörkum. Hækkunin merkir að til skamms tíma er talið líklegt að dönsk fyrirtæki og opinber yfirvöld verði fórnarlömb stafrænna aðgerðasinna.[142]

Í ágúst 2022 birti MSV áhættumat sitt vegna stafrænna ógna á landsvísu (e. The cyber threat against Denmark 2022). Ógn af netnjósnum og er í efsta þrepi fimm af fimm eða Mjög mikil (e. Very high). MSV segir þrálátar netnjósnir og ólögmæta öflun upplýsinga með stafrænum hætti beinast gegn aðilum sem tengjast danska utanríkis- og varnarmálaráðuneytinu en einnig öðrum stjórnvöldum og einkafyrirtækjum í mikilvægum geirum.[143]

MSV metur sömuleiðis ógnina af netglæpum í hæsta þrepi sem Mjög mikla. Lausnargjaldsárásir (e. Ransomware attacks) eru mesta og alvarlegasta netglæpaógn sem Danmörk stendur frammi fyrir að mati MSV. Er það mat MSV að skipuleg tölvu- og netbrotasamtök einkennist mjög af samvinnu, verkaskiptingu og sérhæfingu, sem eigi sinn þátt í að viðhalda mjög háu hættustigi vegna net- og tölvuglæpa.[144]

Þann 16. mars 2023 birti MSV áhættumat sitt um stafrænar ógnir sem beinast gegn Grænlandi. Er það mat MSV að Mjög mikil (e. Very high) hætta sé á að Grænland verði fyrir stafrænum njósnum (netnjósnum) ekki síst er það vegna legu landsins á Norðurheimskautinu og telja skýrsluhöfundar að slíkar upplýsingar, fengnar með ólögmætum hætti, kunni að verða notaðar gegn hagsmunum Grænlendinga. Sömuleiðis telur MSV mjög mikla hættu á að Grænland verði fyrir árásum stafrænna afbrotamanna. Sérstaklega eru lausnargjaldsárásir taldar hættulegar og að þær geti jafnvel skaðað mikilvæga virkni samfélagsins. [145]

Að framansögðu má ljóst vera að net- og tölvuárásir Rússa og millilíða þeirra beinast ekki einvörðungu gegn milljónaþjóðum Evrópu heldur eru

142 threat-assessment---cyber-activism-against-denmark-2023.pdf (cfcs.dk)
143 cfcs-the-cyber-threat-against-denmark-2022-mar23.pdf
144 cfcs-the-cyber-threat-against-denmark-2022-mar23.pdf
145 the-cyber-threat-against-greenland-.pdf (cfcs.dk)

fámennar þjóðir á norðurhjara veraldar einnig í skotlínu þeirra. Ísland hefur þegar orðið fyrir barðinu á alvarlegum árásum sem sumar hið minnsta hafa verið raktar til rússneskra ógnvalda eða aðgerðasinna þeim hliðhollum. Mjög líklegt er talið að stafrænn hernaður Rússlands gegn NATO ríkjum muni aukast eftir því sem átökin í austri magnast.

LOKAORÐ

Ógnir fjölþáttahernaðar gegn Íslandi myndu, eðli málsins samkvæmt, beinast gegn borgaralegum stofnunum og mikilvægum innviðum. Í því efni geta varnir þjóðarinnar verið ófullnægjandi á einhverjum sviðum og veikleikar því talsverðir. Netárásir, njósnir og skemmdarverk væru þær birtingarmyndir fjölþáttaógna sem líklegastar eru að óvinveitt ríki myndi beita gegn Íslandi. Vitað er að stjórnvöld í Rússlandi hafa nýtt skipulagða glæpahópa og sérfróða aðila til njósna, skemmdarverka, tölvu- og netárása og undirróðursstarfsemi af ýmsu tagi.

Komi til þess að Rússar telji af einhverjum sökum ástæðu til að ráðast gegn Íslandi með fjölþáttahernaði kynnu fyrstu merki um þau áform að birtast í tilraunum til að veikja samfélagið og auka í því úlfúð til lengri tíma. Fyrstu stig slíkra aðgerða gætu falist í undirróðursherferðum t.a.m. gegn tilteknum stjórnmálaflokkum, stjórnmálamönnum og stofnunum. Jafnframt kynnu Rússar að freista þess að dýpka átakalínur á borð við NATO-aðild og þátttöku Íslendinga í Evrópusamvinnu sem Rússum er í mun að veikja líkt og komið hefur í ljós í stuðningi þeirra við flokka og samtök á meginlandinu sem andvígir eru þessu samstarfi.

Einkennandi fyrir netárásir gegn vestrænum ríkjum er viðleitni til að brjótast inn í tölvukerfi stofnana og ráðuneyta í því skyni að komast yfir upplýsingar sem þjónað geta tilgangi í langtímabaráttu austurs og vesturs. Frá sjónarhóli gerandans er mikilvægast við fjölþáttaaðgerðir að auðveldlega megi neita aðild og aðkoma verði ekki sönnuð með óyggjandi hætti.[146]

146 Sjá: https://globalsecurityreview.com/plausible-deniability-russias-hybrid-war-ukraine/ og upplýsingar frá Norsku alþjóðamálastofnuninni: https://www.nupi.no/en/Events/2018/The-threats-from-Hybrid-Warfare-Challenges-and-countermeasures-in-liberal-democracies

Í þessu samhengi þykir rétt að halda til skila að á Vesturlöndum gætir mikillar tortryggni í garð kínverskra tæknifyrirtækja meðal annars vegna þess að í kínverskri löggjöf er gert ráð fyrir að þarlend stjórnvöld geti krafist aðstoðar við upplýsingaöflun frá kínverskum stofnunum, fyrirtækjum og einstaklingum. Þannig gæti allur sá tækja- og hugbúnaður frá Kína sem almenningur og stjórnvöld á Íslandi kaupa og nýta á ári hverju verið til þess fallinn að draga úr stafrænu öryggi og þá sérstaklega ef hann tengist viðkvæmum upplýsingum stjórnvalda eða mikilvægum innviðum.[147, 148]

Fjölþáttahernaður gegn Íslandi á hættu- eða átakatímum gæti haft mikil áhrif. Einsýnt er að efla verður viðbúnað, fælingarmátt og viðnámsþrótt íslensks samfélags auk alþjóðlegrar samvinnu til þess að fyrirbyggja og/eða draga sem mest úr þeim skaða sem slíkar fjölþáttaárásir kunna að valda.

Umfangsmikil netárás á mikilvægustu innviði Íslendinga (t.d. raforku- og/eða fjarskiptakerfi) væri hernaðaraðgerð sem hugsanlega myndi fela í sér tilefni til að virkja 5. grein Atlantshafssáttmálans, stofnskrár NATO. Í því efni er einnig vert að hafa í huga birgðalínur og þá staðreynd að gangverk íslenskra innviða byggir á erlendri framleiðslu; hér undir geta fallið raforkuframleiðsla, lyfjainnflutningur, olía, áburður og umbúðir (t.a.m. vegna matvæladreifingar). Rof á birgðaflutningum, vísvitandi „tölvu-sýkingar" framleiðenda í snjalltækjum og stjórnbúnaði innviða gætu einnig verið aðferðir til að koma höggi á Íslendinga.

Sömuleiðis gæti allur sá tækja- og hugbúnaður frá Kína sem almenningur og stjórnvöld á Íslandi kaupa og nýta á ári hverju verið til þess fallinn að draga úr stafrænu öryggi og þá sérstaklega ef hann tengist viðkvæmum upplýsingum stjórnvalda eða mikilvægum innviðum.

Forsenda Íslendinga sem herlausrar þjóðar í baráttunni gegn fjölþáttaógnum og -hernaði er aðildin að NATO, varnarsamstarfið við Bandaríkin og aukið samstarf við Norðurlöndin á sviði varnar- og öryggismála. Í ljósi yfirlýsinga NATO um varnir gegn fjölþáttaógnum, skuldbindinga Bandaríkjamanna og þeirra fjármuna sem Íslendingar sjálfir verja á hverju ári til að uppfylla skuldbindingar þessa samstarfs sem snýr m.a. að því að efla

147 China's intelligence law and the country's future intelligence competitions - Canada.ca

148 Is China's Huawei a Threat to U.S. National Security? | Council on Foreign Relations (cfr.org)

viðnámsþrótt verður ekki séð að betri tryggingar fáist gegn fjölþáttaógnum nema ógnin þyki svo mikil að grundvallarbreytinga sé þörf á herlausu, opnu og lýðræðislegu samfélagi. Að þessu sögðu þá mótast viðbrögð og viðbúnaður af ógnarmati stjórnvalda hverju sinni, mati þeirra á mikilvægi þess samstarfs og skuldbindinga sem efnt hefur verið til vegna fjölþáttaógna og vilja íslenskra stjórnvalda til að efla enn frekar varnir gegn slíkum ógnum, einkum netárásum, skemmdarverkum, njósnum og undirróðri.

VIÐAUKI

MÖSKVAGREINING FYRIR FJÖLÓGNIR

LYKILÞÆTTIR *(e. key factors)*	FÆLINGARMÁTTUR *(e. Deterrence)*	VIÐNÁMSÞOL *(e. Resilience)*
SKILGREININGAR *(e. definitions)*	Koma í veg fyrir að andstæðingar beiti fjölþáttaógnum með því að byggja upp gagnráðstafanir og trúverðuga getu til gagnárása *(e. Prevent adversaries from undertaking hybrid threats by establishing countermeasures and credible retaliation capabilities)*	Geta samfélags, ríkisstjórnar og stofnana til að þola, veita viðnám gegn, endurreisa virkni vegna og laga sig að fjölþáttaógnum/árásum *(e. The ability of societies, governments, and organizations to withstand, respond to, recover from, and adapt to hybrid threats)* Efla varnir og viðnámsþol mikilvægra innviða og kerfa gegn stafrænum árásum og skemmdarverkum *(e. Strengthening critical infrastructure and systems against cyber-attacks and sabotage)*
GAGNRÁÐSTAFANIR *(e. Countermeasures)*	Setja skýrar marklínur og áþreifanlega afleiðingar fyrir brot gegn þeim *(e. Establishing clear red lines and consequences for transgressions)* Þróa sterkar og snarpar stafrænar varnir *(e. Develop strong and responsive cyber defences)* Bæta strategísk upplýsingaskipti í því skyni að afhjúpa og sporna gegn falsfréttum og upplýsingaóreiðu *(e. Enhance strategic communications to expose and counter fake news and disinformation)*	Efla viðnámsþol samfélagsins með aukinni áherslu á fjölmiðlalæsi, gagnsæi og almennri vitundarvakningu um fjölþáttaógnir *(e. Enhance societal resilience through media literacy, transparency, and public awareness campaigns regarding hybrid threats)* Stuðla að auknu efnahagslegu þolgæði með fjölbreyttum aðfangakeðjum. Auka sjálfbærni og draga úr hæði ríkisins á einstökum vörum/ vörutegundum/nauðsynjum/íhlutum frá einum birgja eða ákveðnu ríki *(e. Promote economic resilience by diversifying supply chains, increasing sustainability and reducing dependencies regarding products/types of product/ necessities/components from a single supplier or certain state)*
ÁSKORANIR *(e. Challenges)*	Rekjanleiki: að rekja uppruna fjölþáttaógna getur reynst erfitt og gert erfiðara viðfangs að hefja gagnárásir *(e. Attribution: to identify the source of hybrid threats can be difficult which could complicate retaliation efforts)* Að tryggja að gagnráðstafanir og fælingar-aðgerðir leiði ekki til stigmögnunar átaka *(e. To ensure that deterrence measures do not lead to conflict escalation)*	Að tryggja að fullnægjandi fjármagni sé úthlutað til að byggja upp viðnámsþol *(e. To ensure adequate resources are allocated to resilience-building initiatives)* Að viðhalda árvekni vegna breytilegs eðlis og áhrifa fjölþáttaógna *(e. To maintain vigilance regarding evolving hybrid threats and their impact)*

ÁSTANDSMAT *(e. Situational awareness)*	ALÞJÓÐLEG SAMVINNA *(e. International cooperation)*
Geta til að finna, staðsetja og skilja fjölþáttaógnir í rauntíma og sjá fyrir hvar þeirra er að vænta *(e. The capacity to perceive, locate and understand hybrid threats in real-time and to anticipate their occurrence)*	Fjölþáttaógnir virða ekki landamæri og krefjast samræmdra alþjóðlegra viðbragða *(e. Hybrid threats transcend national boundaries, necessitating a coordinated international response)*
Setja lagaramma um, og þróa getu varðandi, upplýsingaöflun í því skyni að bera kennsl á og greina fjölþáttaógnir *(e. Set legal framework regarding, and develop, intelligence capabilities to detect and analyse hybrid threats)*	Koma á marghliða samstarfi í því skyni að auðvelda miðlun upplýsinga, sameiginlegar aðgerðir, og auka getu *(e. Establishing multilateral cooperation to facilitate information sharing, joint operations, and capacity building)*
Miðla upplýsingum, verklagsreglum og bestu starfsháttum milli ríkisstjórna, stofnana og einkageirans *(e. Share information and best practices among governments, organizations, and the private sector)*	Þáttaka í alþjóðasamstarfi til að ákveða viðmið og reglur um ábyrga hegðun ríkja í hinum stafræna heimi og á öðrum sviðum er varða fjölþáttaógnir *(e. Engage in international efforts to establish norms and rules for responsible state behaviour in cyberspace and other domains concerning hybrid threats)*
Fjárfestingar í tækni sem eykur vöktunar og greiningargetu *(e. Invest in technologies that enhance monitoring and analytical capabilities)*	Stuðla að samstarfi hins opinbera og einkaaðila til að nýta sérþekkingu og fjármagn frá ýmsum geirum *(e. Promote public-private partnerships to leverage expertise and resources from various sectors)*
Að tryggja að tafarlaust sé brugðist við upplýsingum varðandi fjölþáttaógnir og þeim miðlað *(e. To ensure information on hybrid threats is promptly disseminated and acted upon)*	Að efla gagnkvæmt traust og samvinnu á milli ólíkra aðila *(e. To foster mutual trust and collaboration among diverse actors)*
Að tryggja að jafnvægi ríki varðandi miðlun upplýsinga og öryggis- og persónuverndarsjónarmiða *(e. To balance the need for information sharing with concerns for privacy and security)*	Að tryggja skilvirka samhæfingu á milli mismunandi aðgerða og hagsmunaaðila *(e. To ensure effective coordination among different initiatives and stakeholders)*

FJÖLÞÁTTAÓGNIR