CERT·IS

Netógnir á óvissutímum

Ský 29.10.2025

Net- og upplýsingaöryggi á tímum ófriðar

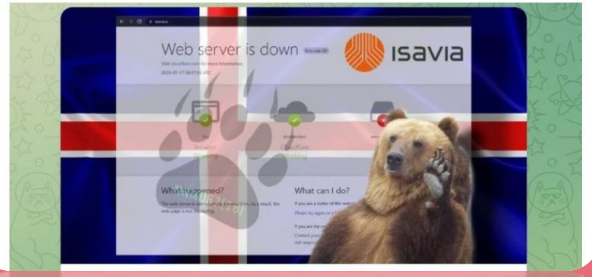
Aðalsteinn Jónsson

Vefur Alþingis liggur niðri: „Málið er í athugun“

Atli Ísleifsson skrifar 16. maí 2023 09:36

Sami hópur segist hafa tekið niður vefsíðu Isavia

Kjartan Kjartansson skrifar 17. maí 2023 11:30



CERT-IS
@cert_iceland · Follow

Árásarhópar eru að gera tilraunir til að nýta rafræn skilríki til að komast inn á viðkvæm svæði. Ekki staðfesta rafræn skilríki nema vera viss um að þú hafir beðið um það.

Ekki staðfesta rafræna auðkenningabeiðnir sem þú kannast ekki við.

11:56 AM · May 16, 2023

91 Reply Copy link

Read more on Twitter

Verið að fremja árásir á íslenska vefi

Verið er að fremja árásir á íslenska vefi að sögn aðstoðaryfirlögregluþjóns hjá greiningardeild ríkislögreglustjóra. Embættið telur sig hafa hugmynd um hvaðan árásirnar koma en ekkert hefur fengist staðfest.

INNLENT 16.5.2023 10:19

Tölvuþrjótarnir kalla Vesturlönd nasista

Samúel Karl Ólason og Máni Snær Þorláksson skrifa 16. maí 2023 12:27

Þessi mynd fylgdi yfirlýsingu tölvurjótahópsins um netárásina á Íslandi.

Netárás gerð á Dalvíkurbyggð

Bjarki Sigurðsson skrifar 15. maí 2023 11:09

Líklegt að árásirnar haldi áfram

Óvissustig Almannavarna var virkjað í dag vegna netárása Rússa í tengslum við fund Evrópuráðsins. Sérfræðingur í netöryggi segir Íslendinga mega eiga von á fleiri árásum og að almenningur þurfi einnig að hafa varan á.

INNLENT 16.5.2023 19:01

Helstu árásaraðilar

	Einyrkjar/Hacktivistar	Skipulagðir hópar	Ógnaraðilar á vegum þjóríkis
Markmið	Tækifærissinnuð	Fjárhagsávinningur	Aukin völd
Geta	• Misgóð þekking • Takmörkuð geta • Lítið fjármagn	• Þekking á UT • Takmarkað fjármagn	• Mikil þekking á UT • Vel fjármagnaðir

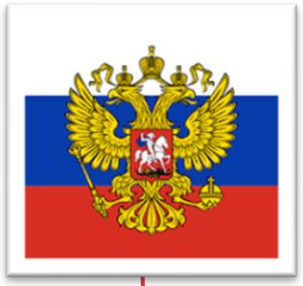
„Stóru Fjögur“

Kína

Rússland

Norður Kórea

Íran



"CIA"

"FBI"

GRU

APT28 – Fancy Bear

Sandworm (Voodoo Bear)

SVR

APT29 – Cozy Bear

FSB

Center 16

Center 18

NOTPETYA ÁRÁS - 2017

Sandworm (GRU) - ~$10 Milljarða tjón

FEB-MAR 2017

M.E.Doc brotist inn í - Sandworm kemur sér fyrir

APR-MAÍ 2017

Bakdyrum komið fyrir í uppfærslu

27. JÚNÍ 2017 - 10:30

ÁRÁS HEFST - Skrúbb óværa

27. JÚNÍ - SÍÐAR SAMA DAG

ALÞJÓÐLEG ÚTBREIÐSLA

Maersk, Merck, FedEx

2018 - NIÐURSTAÐA

Eignaður Rússlandi (Sandworm/GRU)

Dýrasta netárás sögunnar

SOLARWINDS ÁRÁS - 2019-2021

APT29 (SVR/Cozy Bear) - 9 mánuðir óuppgötvuð

SEPT-OKT 2019

APT29 byrjar að skoða SolarWinds

OKT 2019 - FEB 2020

SUNBURST spillikóði þróaður - Fáguð bakdyr

MARS 2020

SÝKT UPPFÆRSLA SEND ÚT

~18,000 viðskiptavinir fá sýkta uppfærslu

MAÍ-DES 2020 (9 MÁNUÐIR)

NJÓSNIR

~100 skotmörk fyrir hnitmiðaðar árásir - vinna á vinnutíma

8-13. DESEMBER 2020

UPPGÖTVUN & OPINBERUN

FireEye uppgötvar - 9 ríkisstofnanir, Microsoft +

2021 - NIÐURSTAÐA

Árás er eignuð Rússlandi (APT29/SVR)

Ein fáguðasta birgðarkeðjuárás sem sést hefur

Taktískar breytingar

Netárásir í fyrirrúmi

Margir bjuggust við að innrás Rússlands inn í Úkraínu myndi fylgja ógrynni af netárásum sem myndi lita innrásina mikið

Netárásir fyrir og eftir innrás

Fjöldi netárása gerðist nokkrum dögum fyrir, klukkutímum fyrir og eftir að innrásin átti sér stað, hefur líklega ekki gefið Rússum það hernaðarlega forskot sem búist var við

Forgangur á njósnir og taktískari árásir

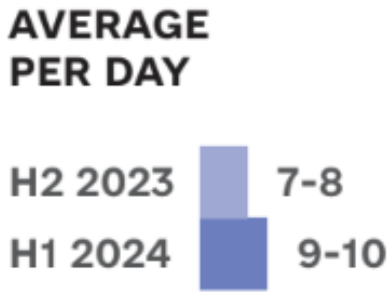
Síðan um mitt 2023 var augljós taktísk breyting þegar Rússar fóru að einbeita sér meira að njósnum

Mikið púður lagt í að komast inn í síma andstæðinganna

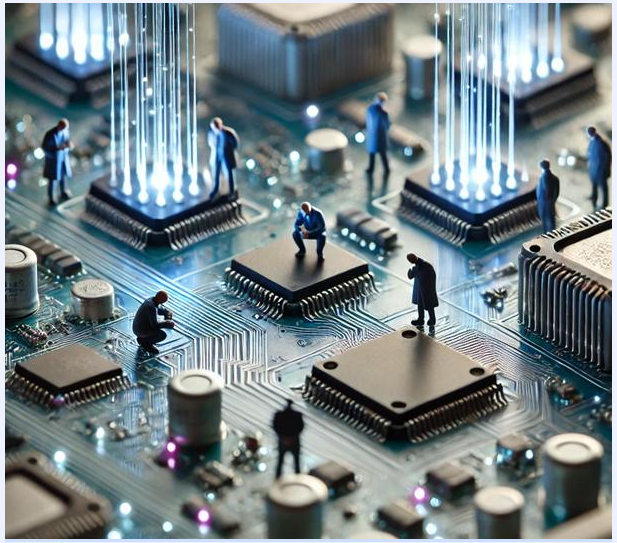
Augljóst að farsímar eru áleitnir hernaðarlega mikilvægir í dag

9-10 árásir á dag

Incidents by Severity Level	H2'2023	H1'2024	Change
Critical	31	3	-90%
High	156	45	-71%
Medium	1264	1670	32%
Low	12	21	75%
Total	**1463**	**1739**	**19%**



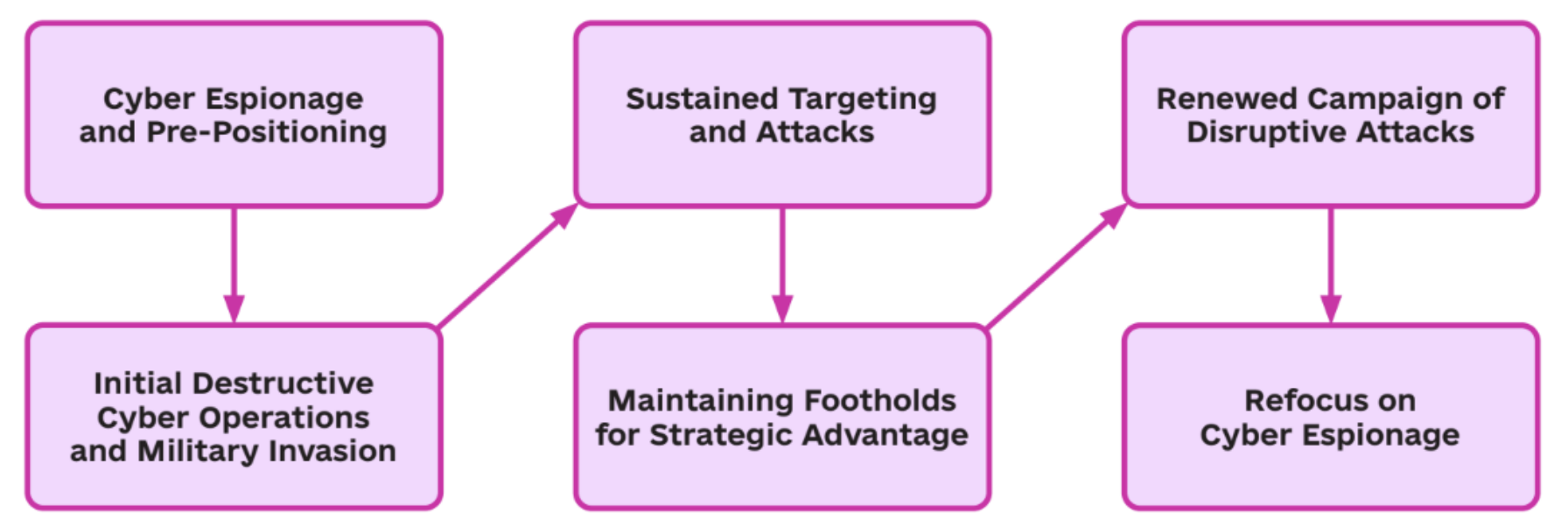
Netárásir



- Erfitt að tímasetja
- Heppnaðist hún?
- Dreifðist hún of víða
- Of mikill tími

	🇷🇺 Rússland	🇨🇳 Kína
Njósnir	🟢 Mikil áhersla	🟢 Megináhersla
Þjófnaður á hugverkum	🟣 Tækifærissinnað	🟢 Mikil áhersla
Áhrifaaðgerðir (e. Influence operations)	🟢 Mikil geta – upplýsingaóreiða	🟣 Vaxandi geta
Truflun og skemmdarverk	🟢 Algengt (Úkraína, orkuinnviðir)	🟣 Sjaldan (áhersla á Taívan)
Efnahagslegur ávinningur	🟣 Takmarkað	🟣 Takmarkað
Undirbúningur fyrir átök	🟢 Beinist að kerfum NATO og Úkraínu	🟢 Staðsetning í vestrænum netkerfum
Hefnd / fælingarmáttur	🟢 Algeng viðbrögð við refsiaðgerðum	🟣 Yfirleitt diplómatískar aðgerðir

Aukin áhersla á upplýsingaöflun

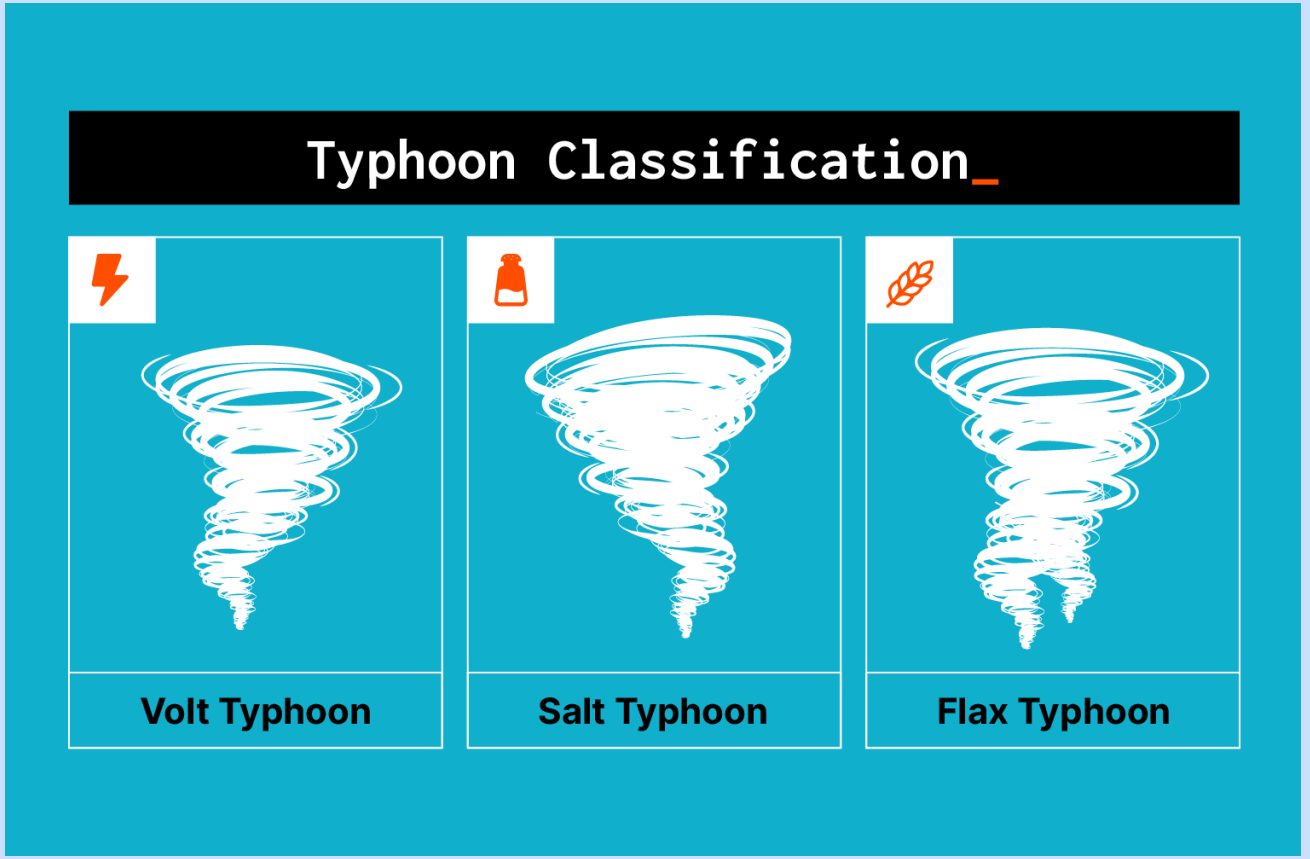


Kína

Notast við skúffufélög til að fela tengingar við ríkið

- Léttara að neita ábyrgð
- Þekktari fyrir njósnir

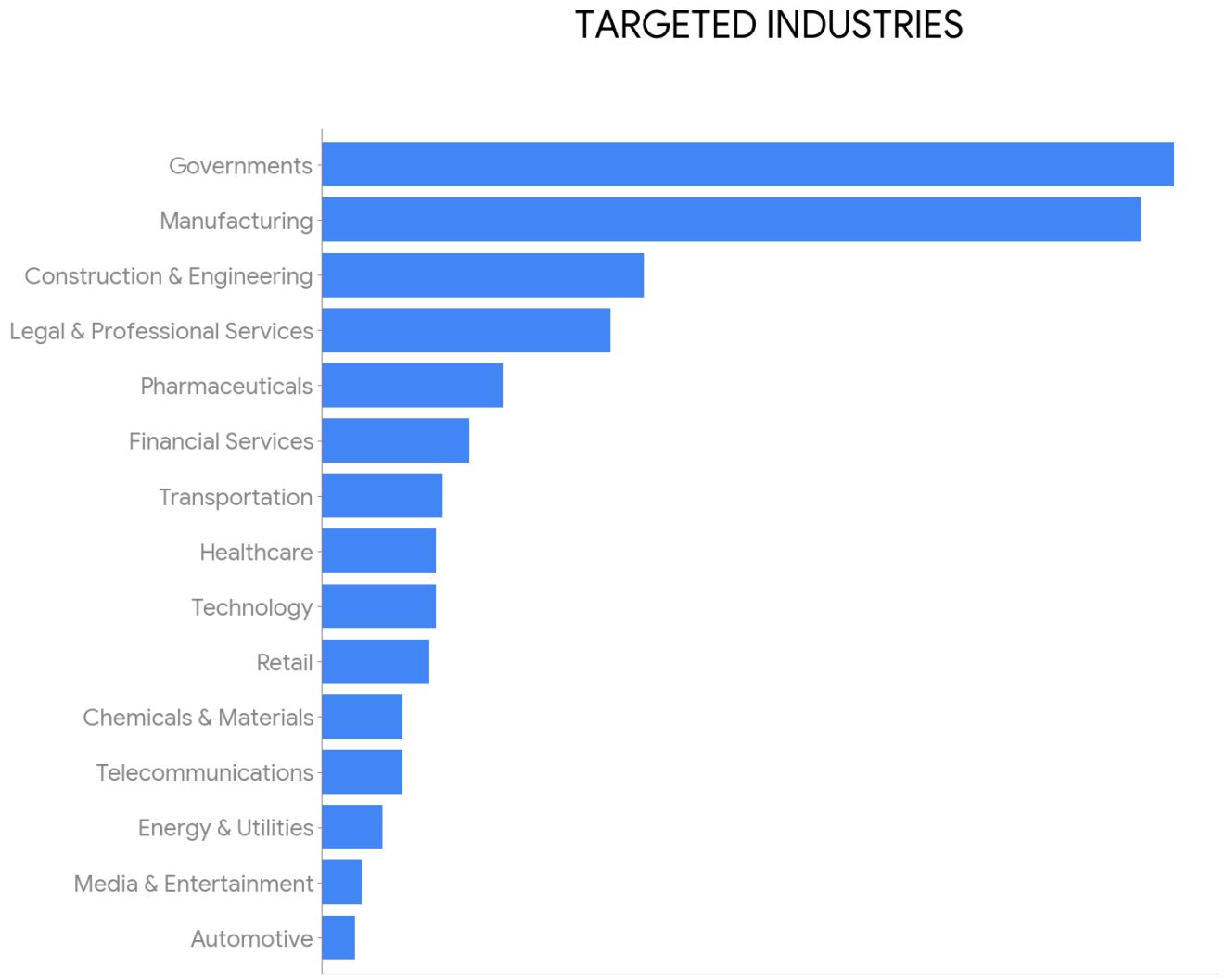
Kínverskir Ógnarhópar



CERT·IS

Helstu skotmörk

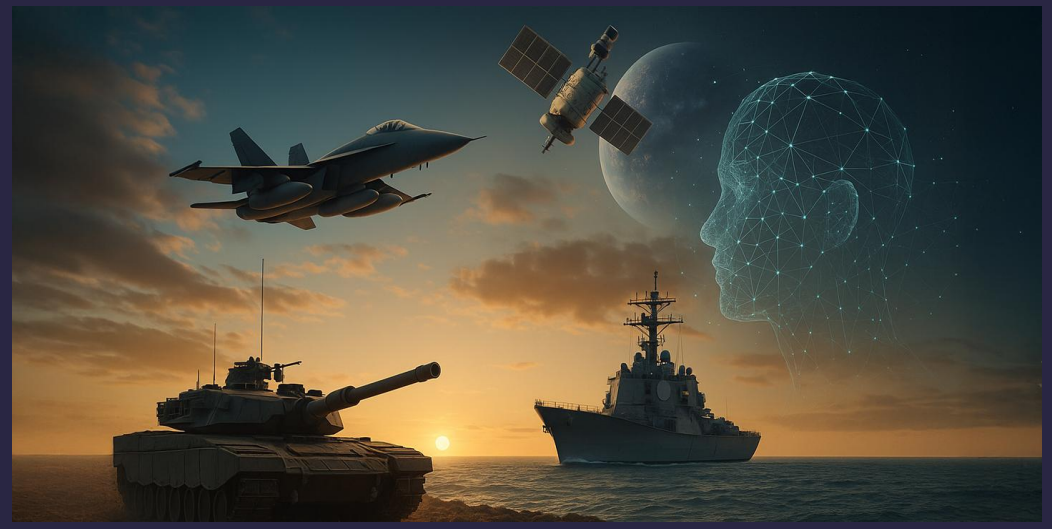
Q4 2024



*Gögn frá Mandiant

Eftirlýstir

https://www.fbi.gov/wanted/cyber/aquatic-panda-cyber-threat-actors



HEFÐBUNDIÐ ÖRYGGI

- Lögregla
- Leyniþjónusta
- Landhelgisgæsla
- Herlið

NETÖRYGGI

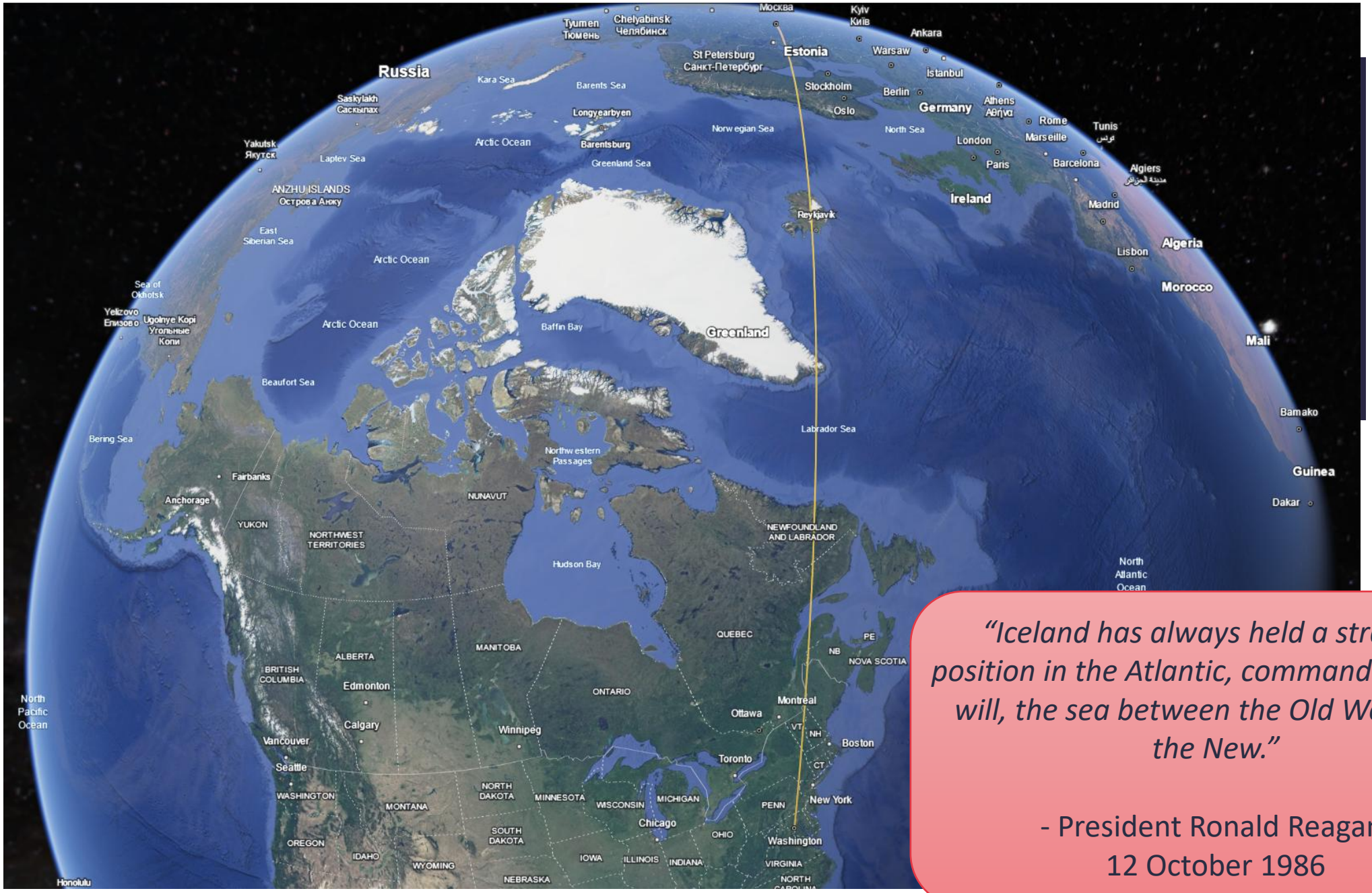
- Mikilvægir innviðir
- Fyrirtæki
- Einstaklingar

"Við erum öll netvarnir"

Cyber Coalition

Árleg NATO Netöryggisæfing

Markmið: Auka áfallaþol og viðbragðsgetu NATO við ógnarhópum



"Iceland has always held a strategic position in the Atlantic, commanding, if you will, the sea between the Old World and the New."

- President Ronald Reagan,
12 October 1986

CERT·IS

Takk fyrir

adalsteinn@cert.is

HLIÐARRÁSARÁRÁSIR (E. SIDE CHANNEL ATTACKS)

- 95% Nákvæmni
  - 93% í gegnum fjarfundarbúnað
- Þróaðir hljóðnemar gera árás enn skilvirkari

https://arxiv.org/pdf/2308.01074.pdf

Zero Click Njósnir

CVE-2025-43300 (CVSS 8.8) // Apple

-> Patched in iOS 18.6.2 (Aug. 20th)

CVE-2025-55177 (CVSS 5.4) // Whatsapp

-> 2.25.21.73 (patched July 28, 2025)

Chained together for zero-click spyware