Sharing is caring

In a more insecure world

6 April 2022

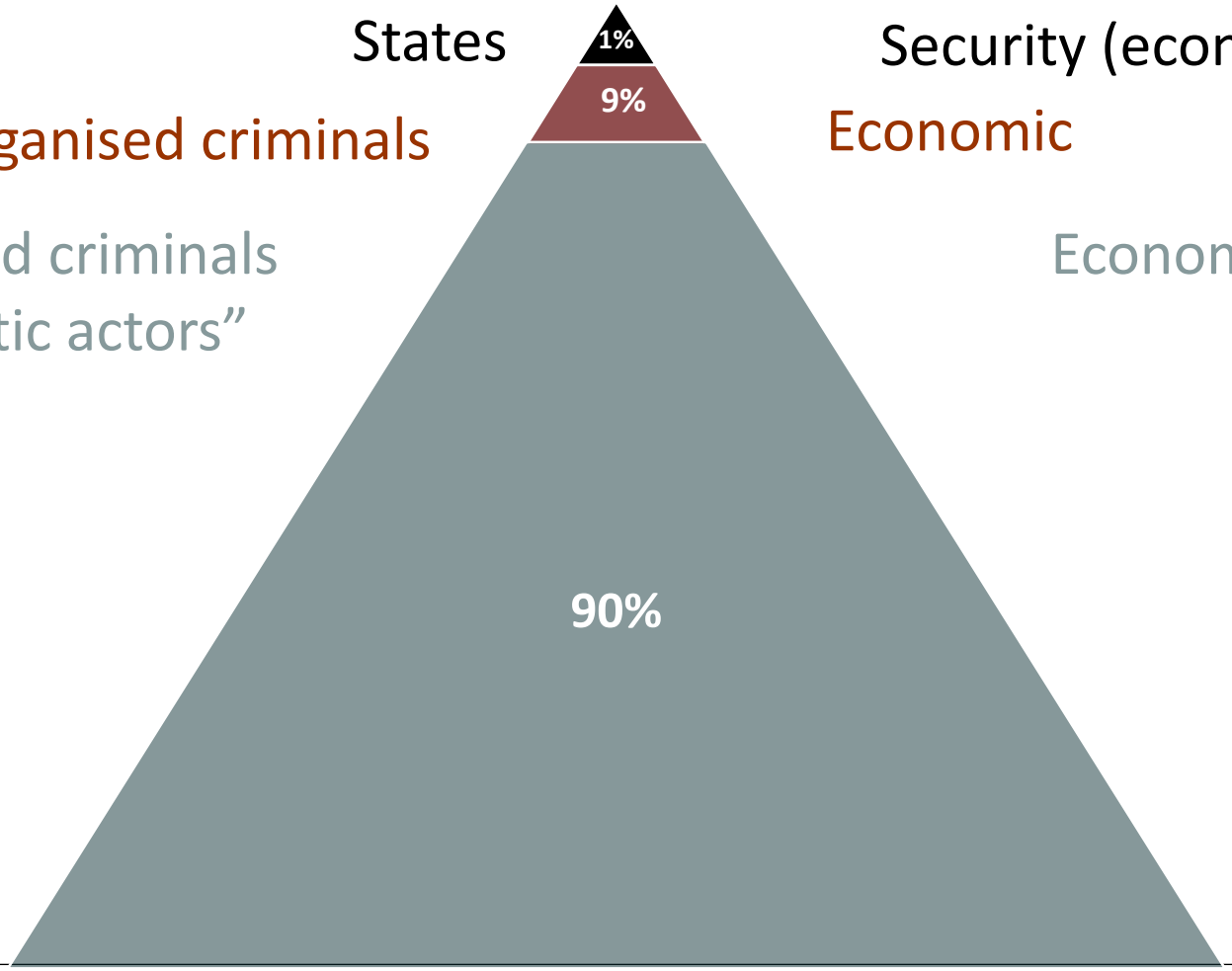
SRS

Agenda

- Status
- Threat actors
- Challenge
- Cooperation
- What inspired us?
- Lessons Learned
- Future

SRS

Threat actors



States

Security (economy)

Organised criminals

Economic

Non-organised criminals
”oppurtunistic actors”

Economic

SRS

Generic attack cycle for state actors

1. Strategic effects
2. ID objects that can give relevant effects (years)
3. Mapping of vulnerabilities in technology, plants and people (years-months)
4. Preparations, tests and evaluations (months)
5. Access created (months – days)
6. Attack supported by information operation or in support of information operation

Chinese reconnaissance – Critical infrastructure

- Oil and gas pipeline companies 2011-2013 (210720)

JOINT
CYBERSECURITY
ADVISORY

TLP:WHITE

Product ID: AA21-201A

July 20, 2021

Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013

SUMMARY

Note: CISA released technical information, including indicators of compromise (IOCs), provided in this advisory in 2012 to affected organizations and stakeholders.

This advisory uses the MITRE ATT&CK® framework, version 9. See the ATT&CK for Enterprise framework for all referenced threat actor tactics and techniques.

This Joint Cybersecurity Advisory—coauthored by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI)—provides information on a spearphishing and intrusion campaign conducted by state-sponsored Chinese actors that occurred from December 2011 to 2013, targeting U.S. oil and natural gas (ONG) pipeline companies.

CISA and the FBI provided incident response and remediation support to a number of victims of this activity. Overall the U.S. Government identified and tracked 23 U.S. natural gas pipeline operators targeted from 2011 to 2013 in this spearphishing and intrusion campaign. Of the known targeted entities, 13 were confirmed compromises, 3 were near misses, and 8 had an unknown depth of intrusion.

The U.S. Government has attributed this activity to Chinese state-sponsored actors. CISA and the FBI assess that these actors were specifically targeting U.S. pipeline infrastructure for the purpose of holding U.S. pipeline infrastructure at risk. Additionally, CISA and the FBI assess that this activity was ultimately intended to help China develop cyberattack capabilities against U.S. pipelines to physically damage pipelines or disrupt pipeline operations.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

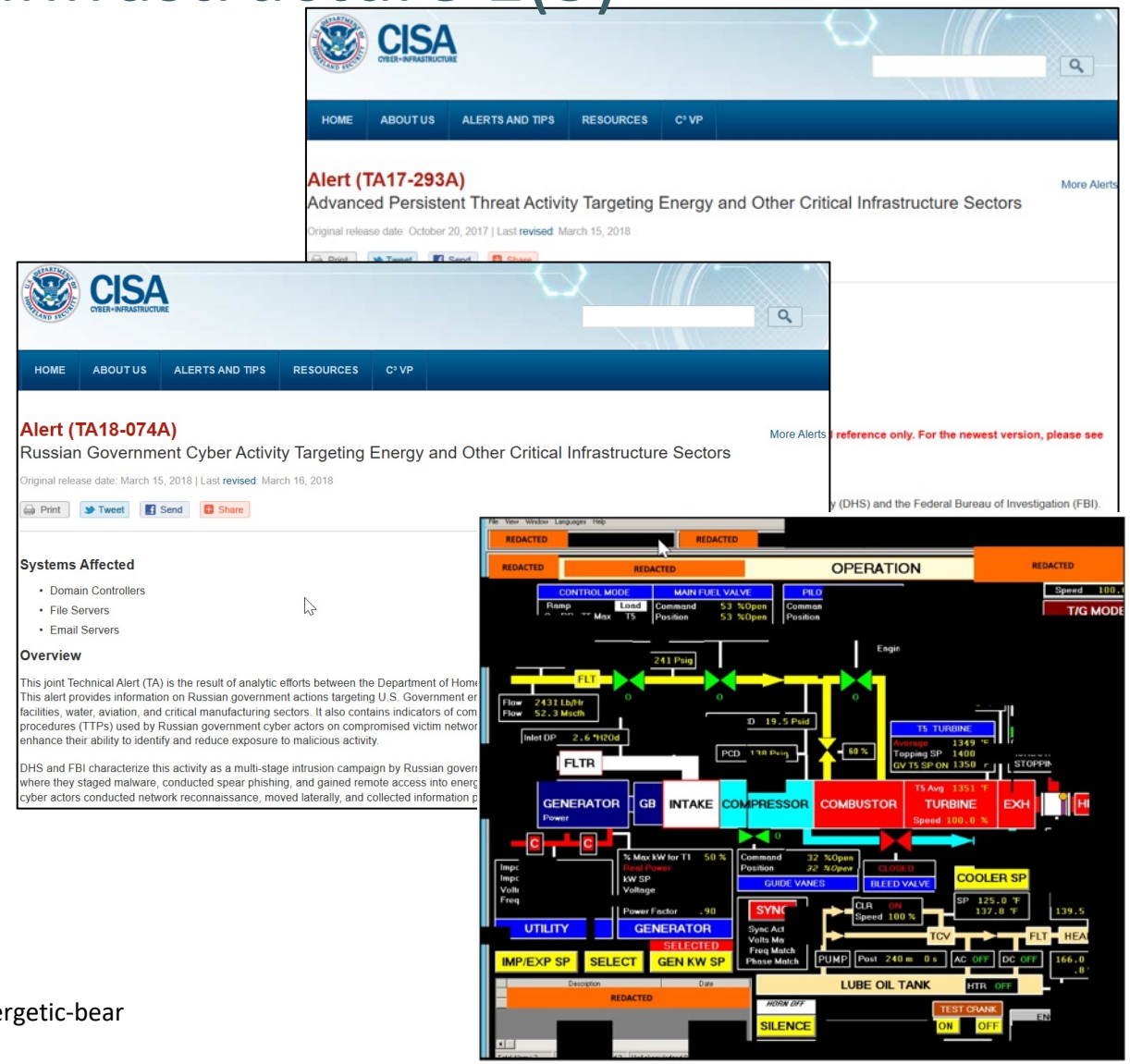
TLP:WHITE

https://us-cert.cisa.gov/sites/default/files/publications/AA21-201A_Chinese_Gas_Pipeline_Intrusion_Campaign_2011_to_2013%20(1).pdf

SRS

Russian - reconnaissance Critical infrastructure 1(3)

- Dragonfly/Energetic Bear 2011-
  - Symantec found them 140630
  - Symantec report 171020
  - DHS, FBI Warning threat energy, water 171020
  - DHS, FBI Warning Russian threat 180315



https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear

https://www.us-cert.gov/ncas/alerts

Russian - reconnaisance Critical infrastructure 2(3)

NCSC, DHS, FBI 180416

Targets:

- Government and private-sector organizations
- Critical infrastructure providers
- Internet service providers (ISPs)

- Lesson: “world events influence risk”

https://www.us-cert.gov/ncas/alerts

Russian - reconnaissance Critical infrastructure 3(3)

- DHS, FBI, NSA 220111
  - Mitigating Russian state sponsored attacks to US Critical infrastructure

https://www.us-cert.gov/ncas/alerts

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA22-011A

January 11, 2022

Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

SUMMARY

This joint Cybersecurity Advisory (CSA)—authored by the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA)—is part of our continuing cybersecurity mission to warn organizations of cyber threats and help the cybersecurity community reduce the risk presented by these threats. This CSA provides an overview of Russian state-sponsored cyber operations; commonly observed tactics, techniques, and procedures (TTPs); detection actions; incident response guidance; and mitigations. This overview is intended to help the cybersecurity community reduce the risk presented by these threats.

CISA, the FBI, and NSA encourage the cybersecurity community—especially critical infrastructure network defenders—to adopt a heightened state of awareness and to conduct proactive threat hunting, as outlined in the Detection section. Additionally, CISA, the FBI, and NSA strongly urge network defenders to implement the recommendations listed below and detailed in the Mitigations section. These mitigations will help organizations improve their functional resilience by reducing the risk of compromise or severe business degradation.

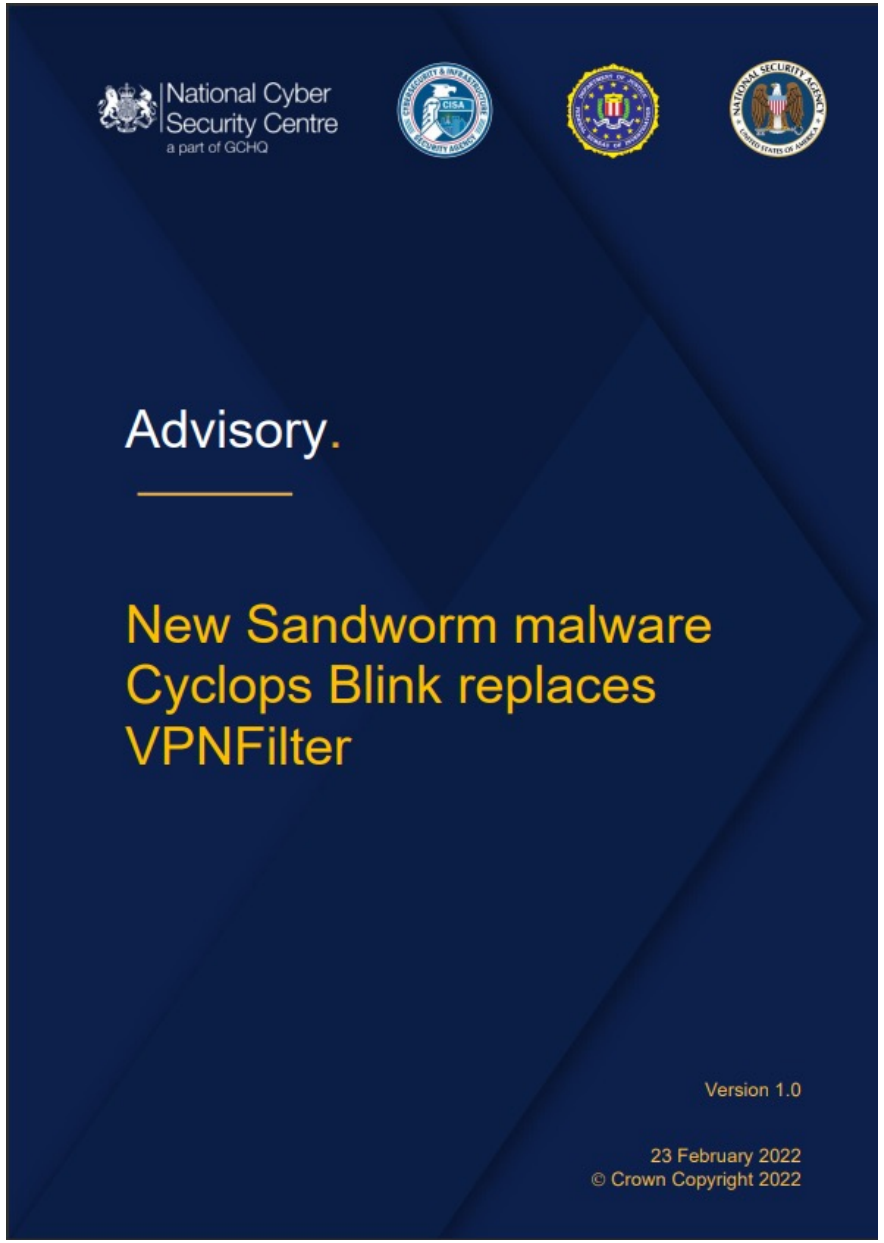
Actions critical infrastructure organizations should implement to immediately strengthen their cyber posture.

- Patch all systems. Prioritize patching known exploited vulnerabilities.
- Implement multi-factor authentication.
- Use antivirus software.
- Develop internal contact lists and surge support.

Russian – pre-positioning

- DHS, FBI, NSA targeting SOHO-routers 220223
  - GRU's Main Centre for Special Technologies GTsST
    - The BlackEnergy disruption of Ukrainian electricity in 2015
    - Industroyer in 2016
    - Ukraines Ministry of Finance 2016
    - NotPetya in 2017
    - Attacks against the Winter Olympics and Paralympics in 2018
    - A series of disruptive attacks against Georgia in 2019
  - Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM)
    - Triton malware Saudi Arabian oil refinery
    - US oil refineries

https://www.us-cert.gov/ncas/alerts



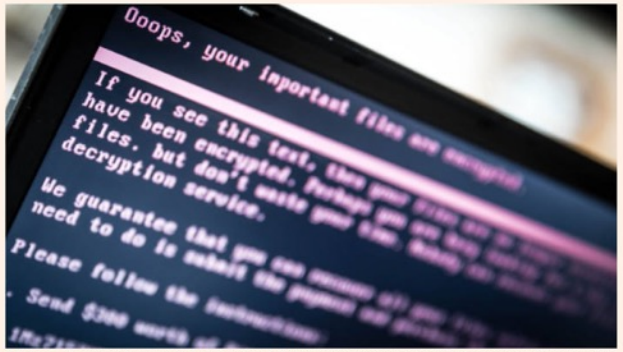
Cyberattacks on critical infrastructure

- Tv5 Monde 2015
- Ukraine 2015 - Electricity
- Ukraine 2016 - Financial
  - Ministry of Finance
  - State Treasury Service
  - Lost 3 TB data
  - Could not perform 150k transactions/day
- Ukraine 2016 – Electricity
- Notpetya 2017
- Saudiarabia 2017 – Gas
- Israel 2020 – Water
- USA 2020 – Gas pipelines
- USA 2020 – Colonial Oil pipeline

Cyber Security + Add to myFT

Mondelez sues Zurich in test for cyber hack insurance

Insurance group had refused to pay for NotPetya attack, invoking a war exclusion



Mondelez said it had been hit twice by NotPetya, with 1,700 of its servers and 24,000 laptops rendered 'permanently dysfunctional' © EPA

Oliver Ralph in London and Robert Armstrong in New York JANUARY 10, 2019 26

Mondelez, the US food company that owns the Oreo and Cadbury brands, is suing its insurance company, Zurich, for refusing to pay out on a $100m claim for damage caused by the NotPetya cyber attack.

Catalin Cimpanu
January 21, 2022
News Technology

Merck wins cyber-insurance lawsuit related to NotPetya attack

A New Jersey court has ruled in favor of Merck in a lawsuit the pharmaceutical company filed against its insurer, Ace American, which declined to cover the losses caused by the NotPetya ransomware attack.

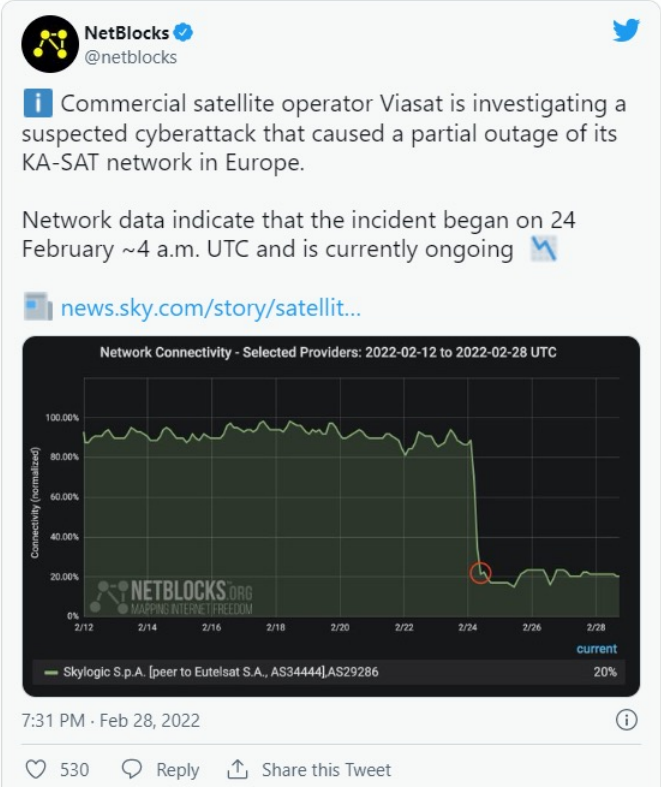
The NotPetya incident, which took place in June 2017 and impacted thousands of companies all over the world, destroyed data on more than 40,000 Merck computers and took the company months to recover.

Merck estimated the damage at $1.4 billion, a loss caused by production outage, costs to hire IT experts, and costs of buying new equipment to replace all affected systems.

At the time, the company had a $1.75 billion "all-risk" insurance policy, which included coverage for software-related data loss events.

Ukraine – KA-SAT Modem wiper February 24

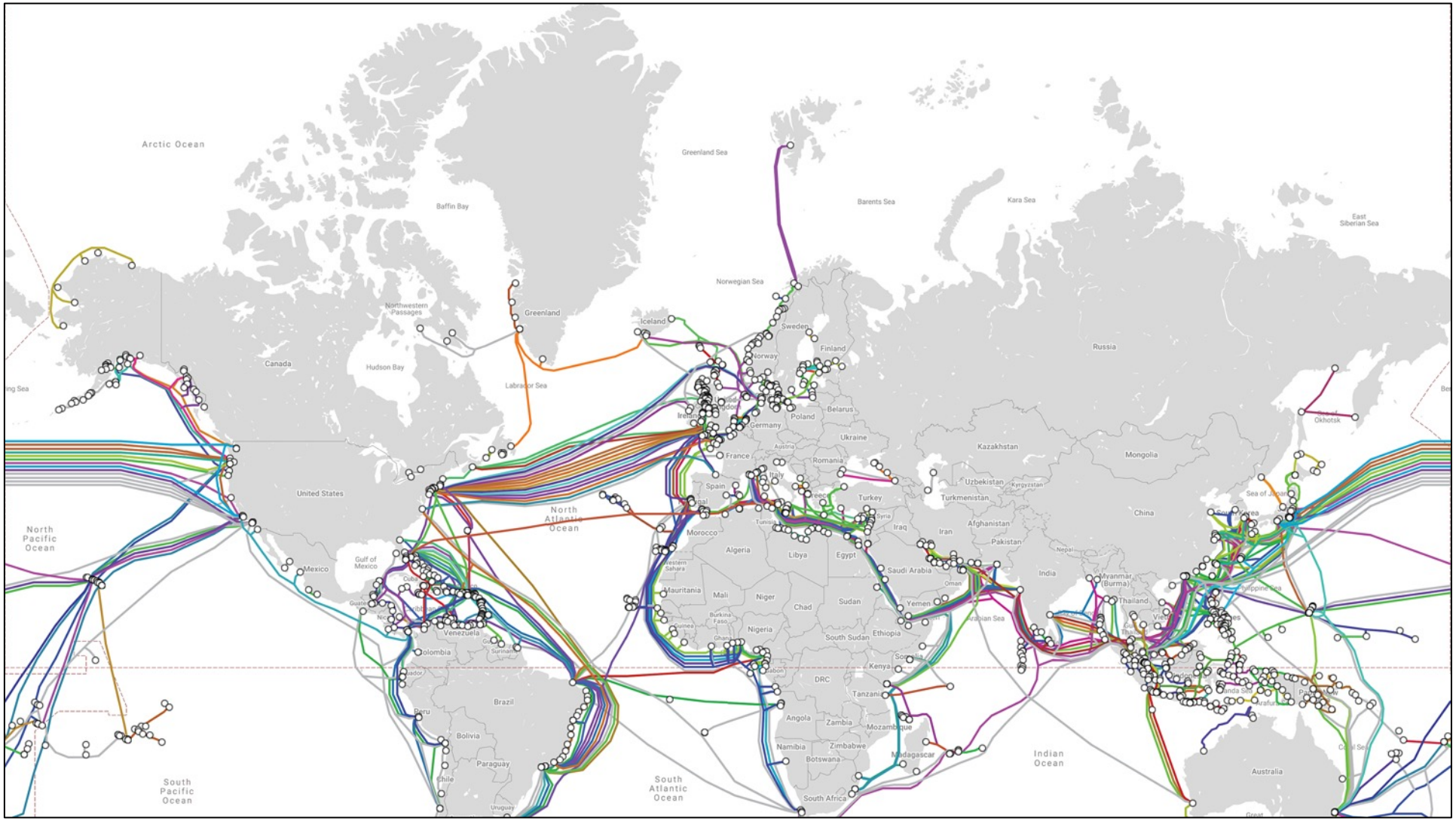
- “Modem Wiper” – wiped 30 000 modems
- 5 800 Wind turbines in Germany affected
- Cyberattack FBI and CISA joint advisory March 17



https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html and https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

SRS

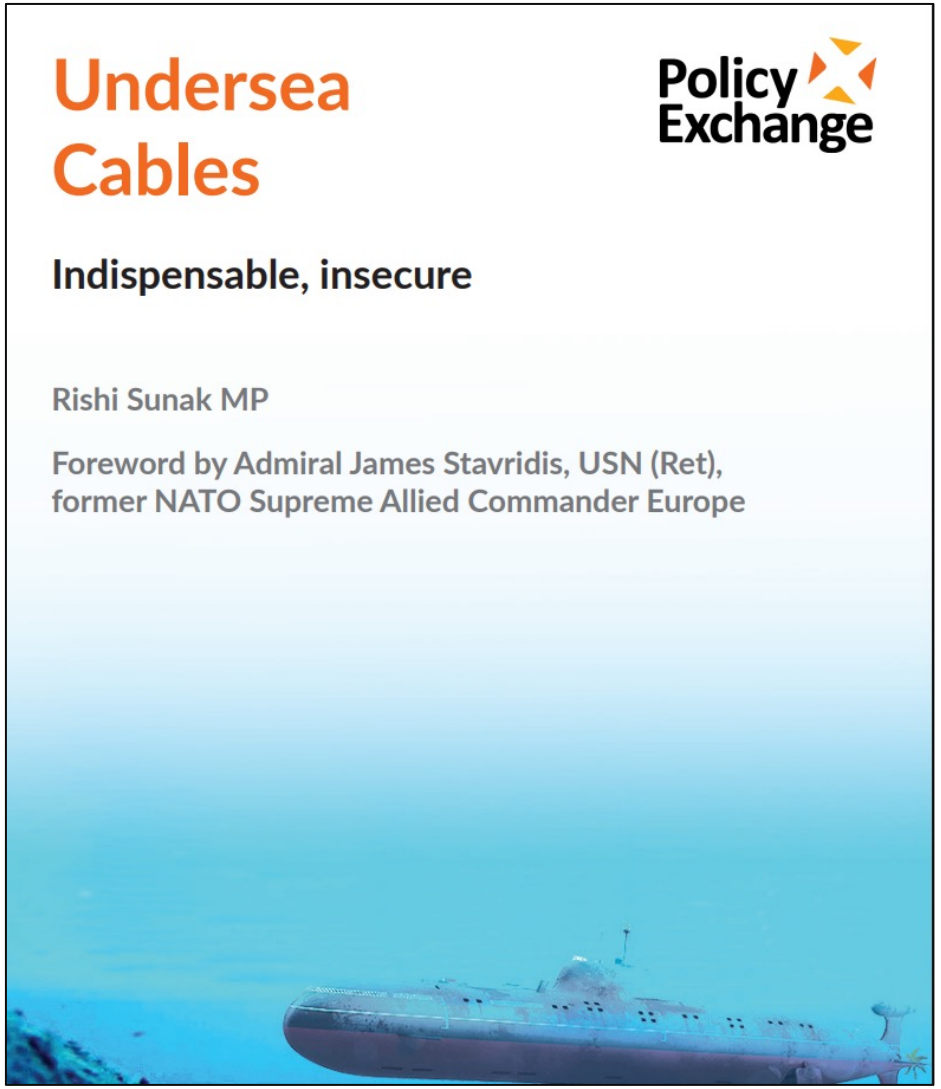
My real worry - Infrastructure



SRS

Submarine cables – our achilles heel?

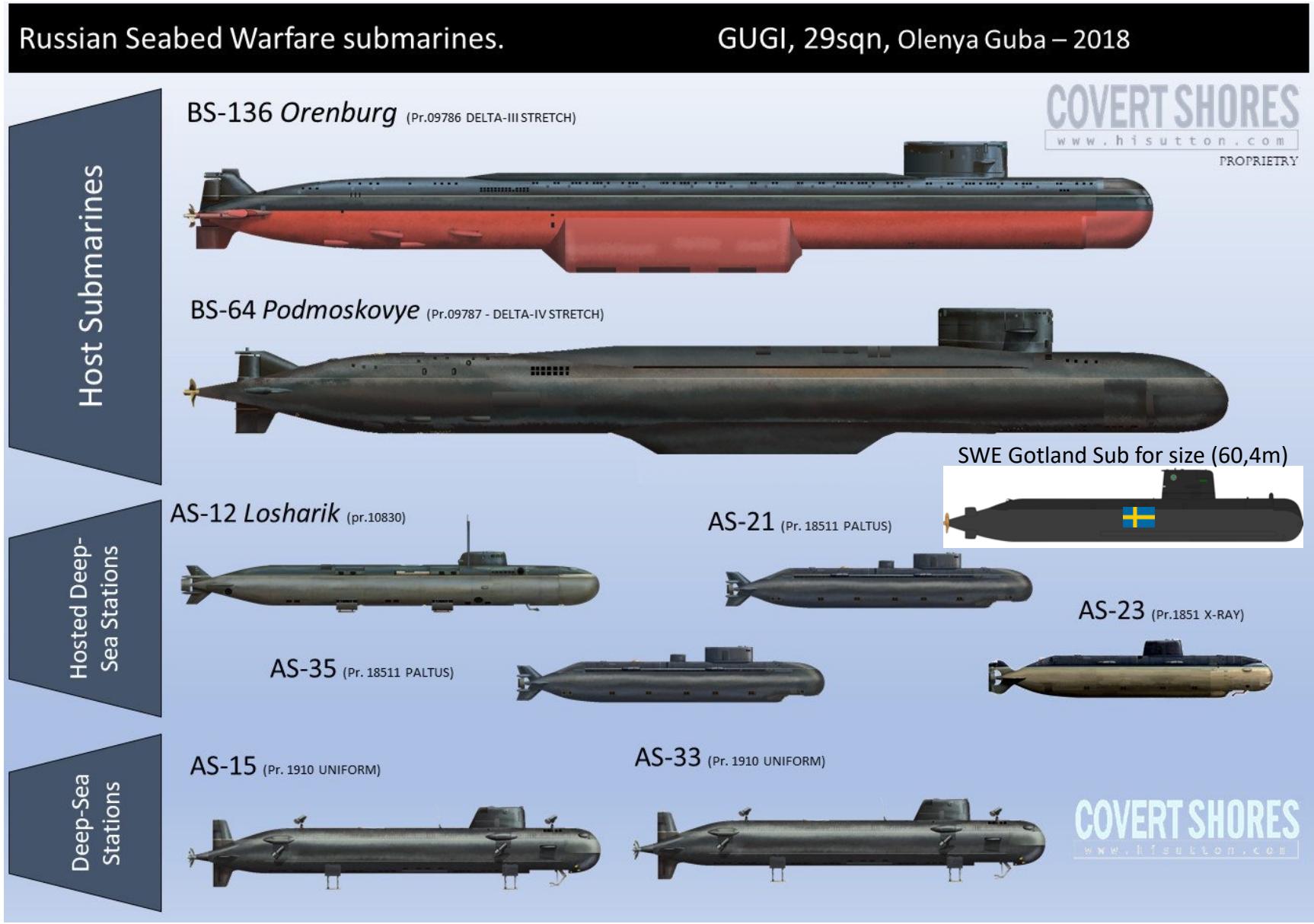
- Main Directorate of Deep-Sea Research (GUGI)
- 8 nuclear powered submarines
  - 2 ” Motherships”
  - 6 deep diving smaller submarines
- 2 Ships



https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf

GUGI Capacity to cut submarine cables

- Plausible deniability



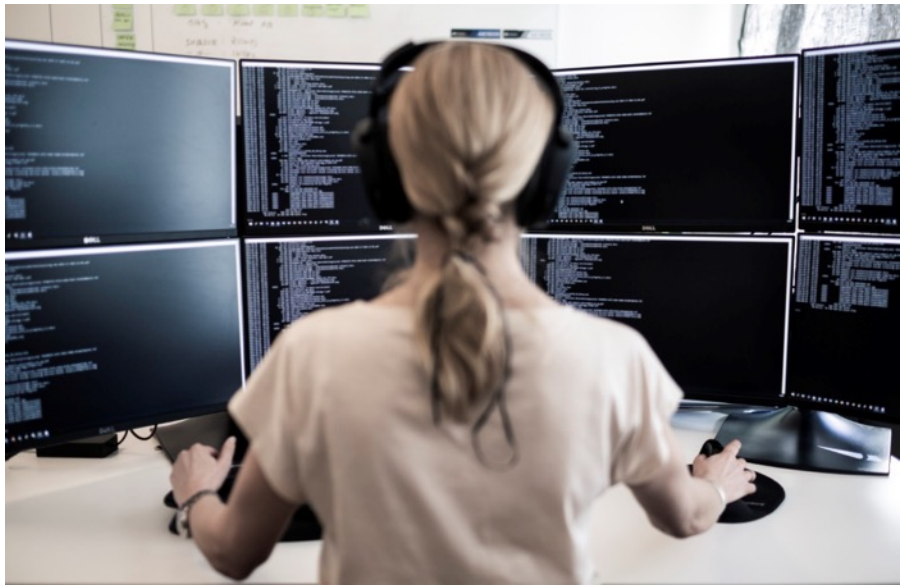
http://www.hisutton.com/Undersea_Cables.html

Organised crime are cooperating

Larger than Global drug trade and more profitable

- ”Business” with markets selling:
  - Ransomware-as-a service (RaaS)
  - Phishing-as-a service (PhaaS)
  - Infrastructure hosting
  - Exploit kits

- Effective “business models” for RaaS

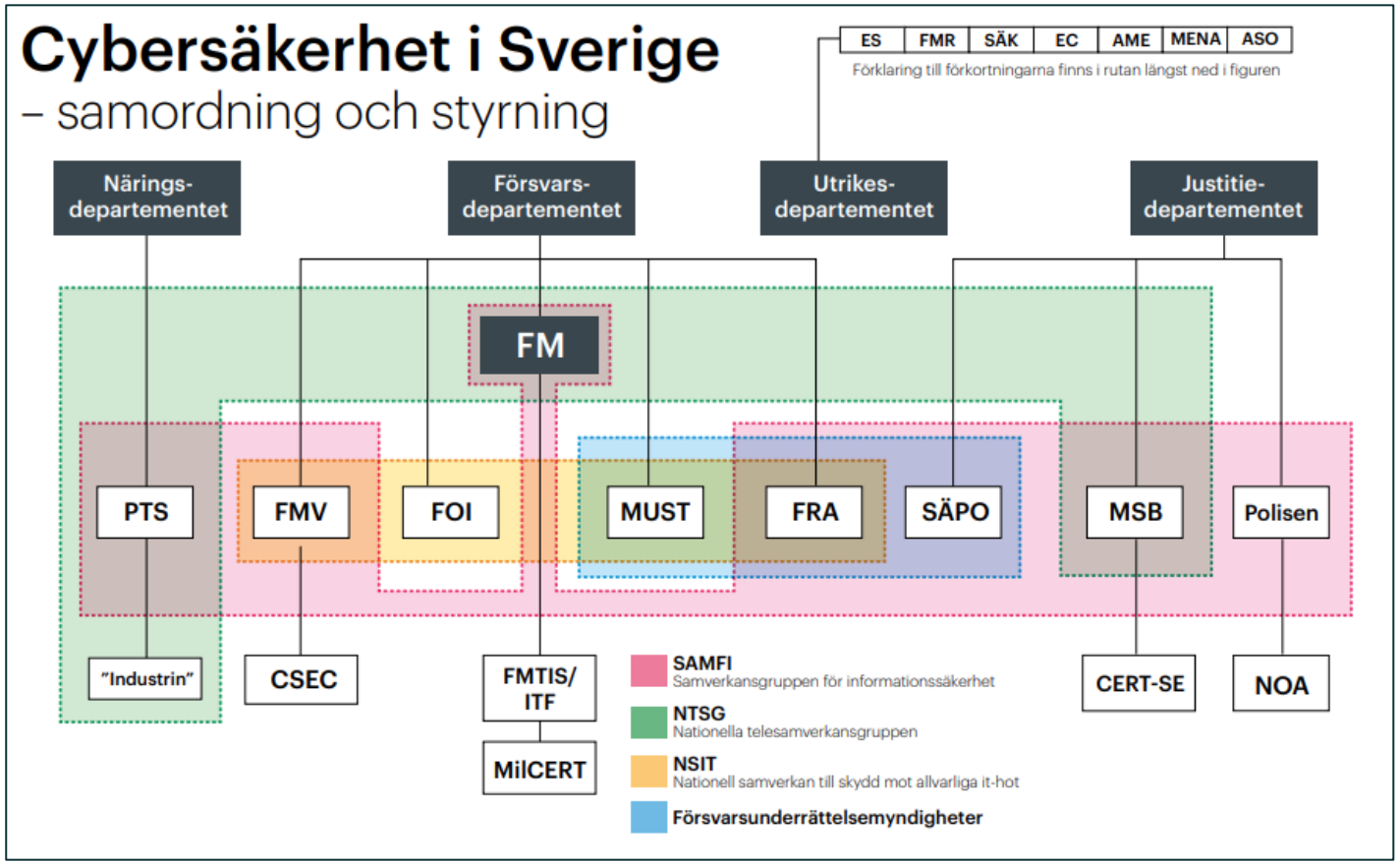


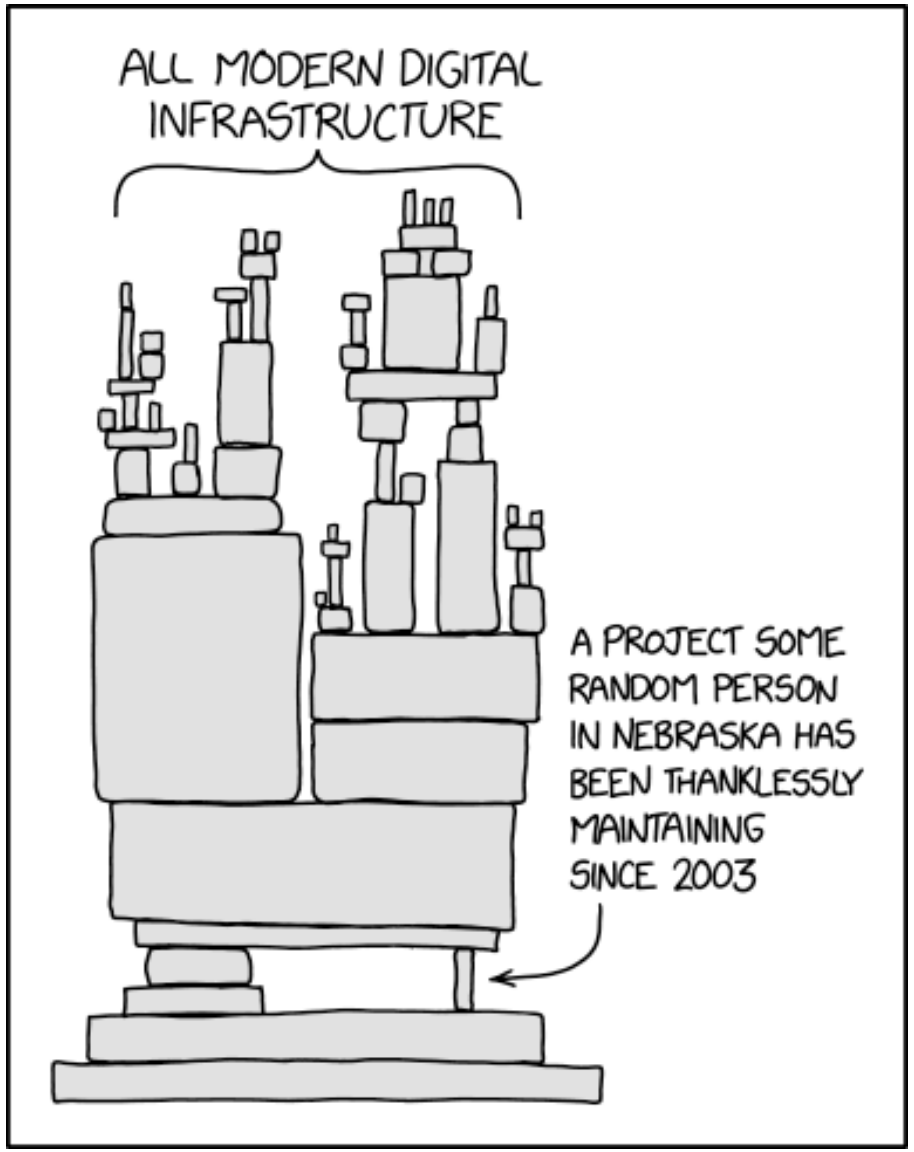
https://pdf.ic3.gov/2018_IC3Report.pdf

https://www.europol.europa.eu/sites/default/files/documents/report_do_criminals_dream_of_electric_sheep.pdf

SRS

Challenge – Cybersecurity in Sweden





https://www.iva.se/globalassets/projekt/201902-iva-digitalisering-slutrapport-l-uppslag.pdf
https://xkcd.com/2347/

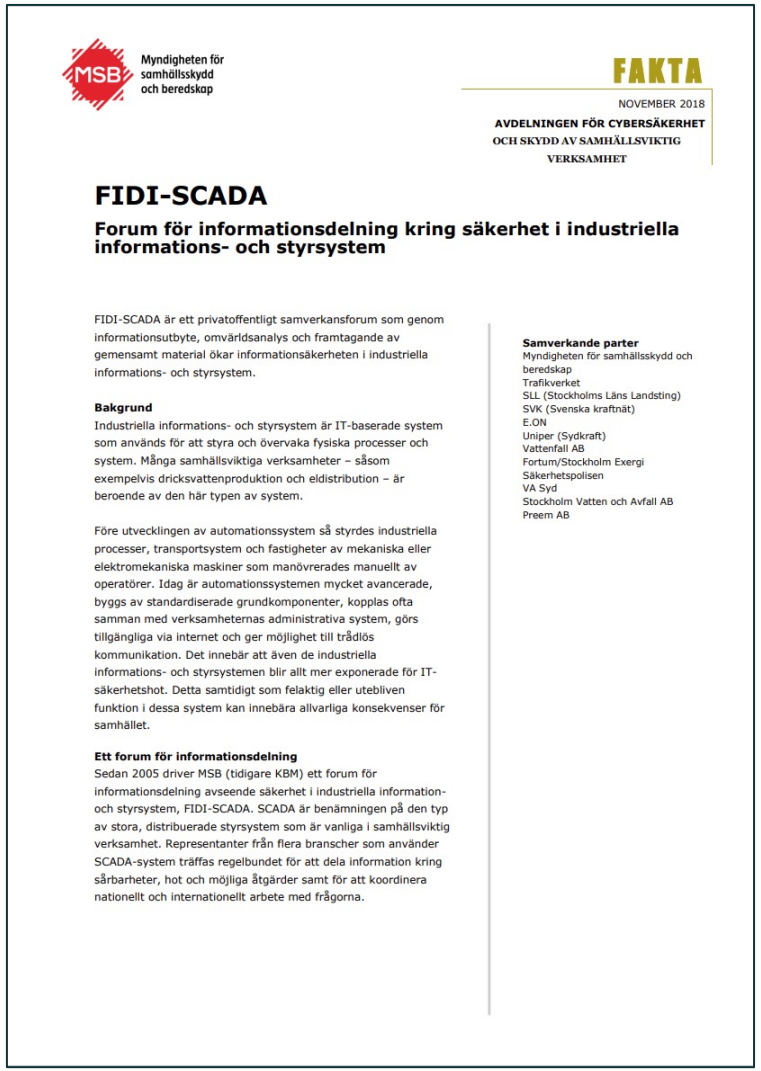
SRS

One solution – organize ISACS

Information Sharing and Analysis Centers (ISACS)

- Sweden - Forum informationsdelning - FIDI
  - FIDI drift
  - FIDI Finans
  - FIDI Scada
  - FIDI Telekom
  - FIDI Hälso- och sjukvård

- Focusing on ”key” business verticals
- Will miss some new service providers



Myndigheten för samhällsskydd och beredskap

FAKTA

NOVEMBER 2018

AVDELNINGEN FÖR CYBERSÄKERHET OCH SKYDD AV SAMHÄLLSVIKTIG VERKSAMHET

FIDI-SCADA

Forum för informationsdelning kring säkerhet i industriella informations- och styrsystem

FIDI-SCADA är ett privatoffentligt samverkansforum som genom informationsutbyte, omvärldsanalys och framtagande av gemensamt material ökar informationsäkerheten i industriella informations- och styrsystem.

Bakgrund

Industriella informations- och styrsystem är IT-baserade system som används för att styra och övervaka fysiska processer och system. Många samhällsviktiga verksamheter – såsom exempelvis dricksvattenproduktion och eldistribution – är beroende av den här typen av system.

Före utvecklingen av automationssystem så styrdes industriella processer, transportsystem och fastigheter av mekaniska eller elektromekaniska maskiner som manövrerades manuellt av operatörer. Idag är automationssystemen mycket avancerade, byggs av standardiserade grundkomponenter, kopplas ofta samman med verksamheternas administrativa system, görs tillgängliga via internet och ger möjlighet till trådlös kommunikation. Det innebär att även de industriella informations- och styrsystemen blir allt mer exponerade för IT-säkerhetshot. Detta samtidigt som felaktig eller utebliven funktion i dessa system kan innebära allvarliga konsekvenser för samhället.

Ett forum för informationsdelning

Sedan 2005 driver MSB (tidigare KBM) ett forum för informationsdelning avseende säkerhet i industriella information- och styrsystem, FIDI-SCADA. SCADA är benämningen på den typ av stora, distribuerade styrsystem som är vanliga i samhällsviktig verksamhet. Representanter från flera branscher som använder SCADA-system träffas regelbundet för att dela information kring sårbarheter, hot och möjliga åtgärder samt för att koordinera nationellt och internationellt arbete med frågorna.

Samverkande parter

Myndigheten för samhällsskydd och beredskap
Trafikverket
SLL (Stockholms Läns Landsting)
SVK (Svenska kraftnät)
E.ON
Uniper (Sydkraft)
Vattenfall AB
Fortum/Stockholm Exergi
Säkerhetspolisen
VA Syd
Stockholm Vatten och Avfall AB
Preem AB

SRS

One solution – increase sharing of information

IOC's and Tactics, Techniques, and Procedures (TTP) - MITRE ATT&CK

JOINT
CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA22-083A

March 24, 2022

Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector

Executive Summary

This joint Cybersecurity Advisory (CSA)—coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE)—provides information on multiple intrusion campaigns conducted by state-sponsored Russian cyber actors from 2011 to 2018 and targeted U.S. and international Energy Sector organizations. CISA, the FBI, and DOE responded to these campaigns with appropriate action in and around the time that they occurred. CISA, the FBI, and DOE are sharing this information in order to highlight historical tactics, techniques, and procedures (TTPs) used by adversaries to target U.S. and international Energy Sector organizations.

Actions to Take Today to Protect Energy Sector Networks:

- Implement and ensure robust network segmentation between IT and ICS networks.
- Enforce MFA to authenticate to a system.
- Manage the creation of, modification of, use of—and permissions associated with—privileged accounts.

On March 24, 2022, the U.S. Department of Justice unsealed indictments of three Russian Federal Security Service (FSB) officers and a Russian Federation Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM) employee for their involvement in the following intrusion campaigns against U.S. and international oil refineries, nuclear facilities, and energy companies.[1]

- **Global Energy Sector Intrusion Campaign, 2011 to 2018:** the FSB conducted a multi-stage campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data.

All organizations should report incidents and anomalous activity to CISA 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov

APPENDIX A: CAMPAIGN AND MALWARE TACTICS, TECHNIQUES, AND PROCEDURES

Global Energy Sector Campaign: Havex Malware

Table 1 maps Havex's capabilities to the ATT&CK for Enterprise framework, and table 2 maps Havex's capabilities to the ATT&CK for ICS framework. Table 1 also provides associated mitigations. For additional mitigations, refer to the Mitigations section of this advisory.

Table 1: Enterprise Domain Tactics and Techniques for Havex [2]

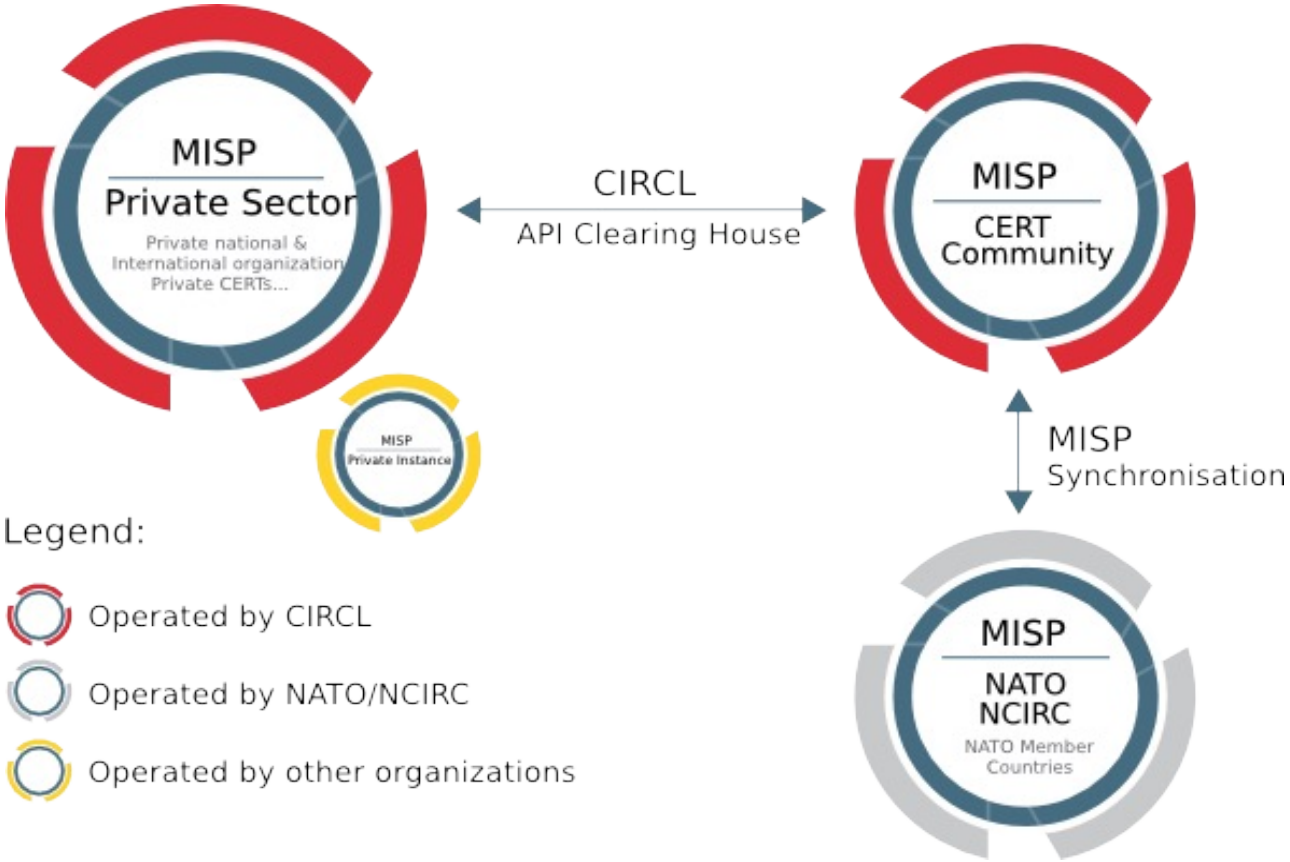
Tactic	Technique	Use	Detection/Mitigations
Persistence [TA0003]	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547.001]	Havex adds Registry Run keys to achieve persistence.	**Monitor**: monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Monitor the start folder for additions or changes. Tools such as `Sysinternals Autoruns` may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders. Suspicious program execution as startup programs may show up as outlier processes that have not been seen before when compared against historical data.
Privilege Escalation [TA0004]	Process Injection [T1055] **Note**: this technique also applies to Tactic:	Havex injects itself into `explorer.exe`.	**Behavior Prevention on End Point:** use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, Application Programming Interface (API) call, etc., behavior.

SRS

Security and Defense Industry Association

SOFF
Säkerhets- och försvarsföretagen

- Cyberdefence group has started info sharing:
  - Physical meetings
  - MISP ”Malware Information Sharing Platform”
  - Signal group



https://soff.se/en/about-soff/

SRS

Who inspired us to start sharing

- Computer Incident Response Center Luxembourg (CIRCL)

- Cyber Security Sharing and Analytics (CSSA)

- Computer Incident Response Center for Civil Society (CiviCERT)

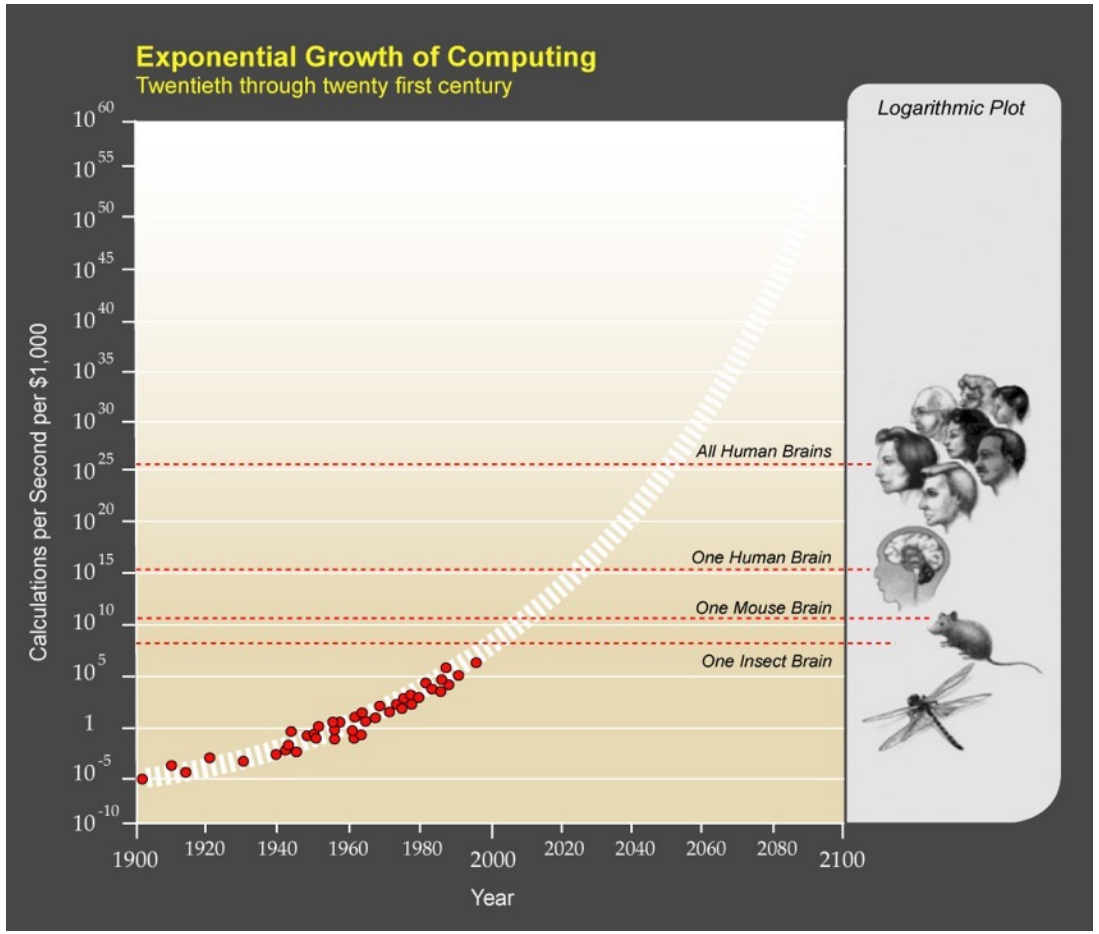
Lessons learned

- **”We are all in this together”**
- **Trust is important**
- **Members see a value in sharing**
- **Non competitive – we need to give and recieve help**
- **We need to increase methods and tools for sharing threat and vulnerability information**
- **We need a cultural change – especially for government agencies**

Future

Future

- **More threat actors**
- **More vulnerable system - “Time to market” shortens design and test cycle**
- **Escalating complexity - (thanks: @halvarflake)**
  - **Anomaly of cheap complexity**
  - **Interdependence of systems**
  - **Decoupling of ownership and control**
- **Technological change is accelerating**
  - **Quantum computers**
  - **AI – machine/deep learning**



Sources:
Thomas Dullien / Halvar Flake https://thomasdullien.github.io/about/
https://rule11.tech/papers/2018-complexitysecuritysec-dullien.pdf and
https://docs.google.com/presentation/d/14iFim2m0jmPhQKQFOPoqvVKykz8EVgmV1q_8dsapZ68/edit#slide=id.g59d850d457_0_594

https://singularityhub.com/2016/03/22/technology-feels-like-its-accelerating-because-it-actually-is/

SRS

Questions

SRS

PO Box 244 | SE-101 24 Stockholm, Sweden | www.srsgroup.se