History of the Russian Intelligence Services and Cyberwarfare

By Will Thomas
Equinix Threat Analysis Center (ETAC)
SANS FOR589 Co-Author
Curated Intelligence Co-Founder
Bournemouth 2600 Organizer

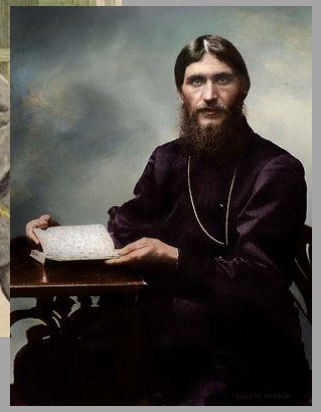
Talk Contents

- History of the Russian Intelligence Services
- Current Russian Intelligence Services
- Russian Private Sector Organizations
- Advanced Persistent Threat Groups
- Major Russian Cyber Espionage Operations
- Russian Organized Cybercrime and the State
- Russian Cyberwarfare in Ukraine
- Major Operational Failures
- Where do we go from here?

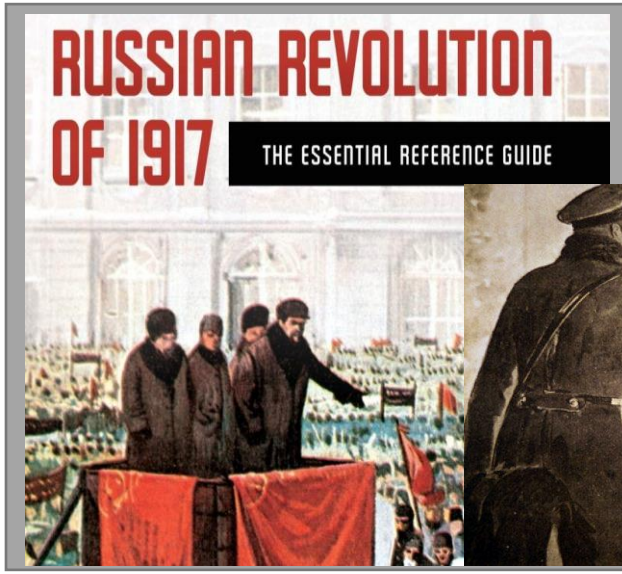
Russia. Am I right?

History of the Russian Intelligence Services

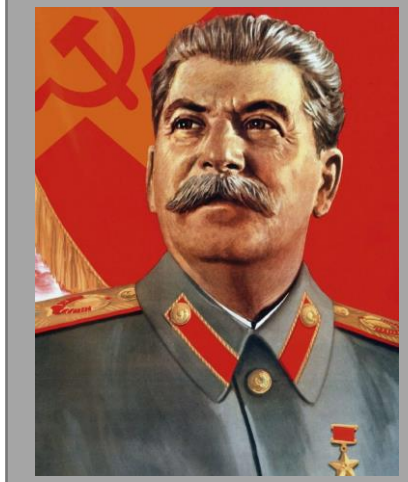
The Tsar's Ohkrana (1881)



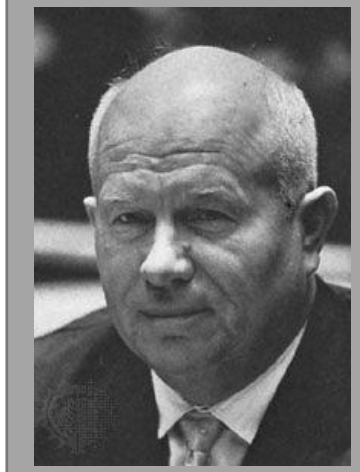
Rasputin



Lenin's Cheka (1917)



Stalin's NKVD (1934)



Khrushchev's KGB (1954)

Fall of the Soviet Union in 1991 (Swan Lake played on all Russian TVs)

History of the Russian Intelligence Services

Continued – post USSR Soviet Union

Yeltsin

Putin

General Gerasimov & Gerasimov Doctrine

President of the Russian Federation

Foreign Intelligence Service (SVR)

Federal Security Service (FSB)

Armed Forces of the Russian Federation

Main Directorate of the General Staff of the Armed Forces (GRU)

Spetsnaz GRU

Russian Private Sector Organizations

- **Cybersecurity**

GROUP IB

POSITIVE TECHNOLOGIES

Dr.WEB®
Anti-virus

- **Social Media**

- **Media**

RT

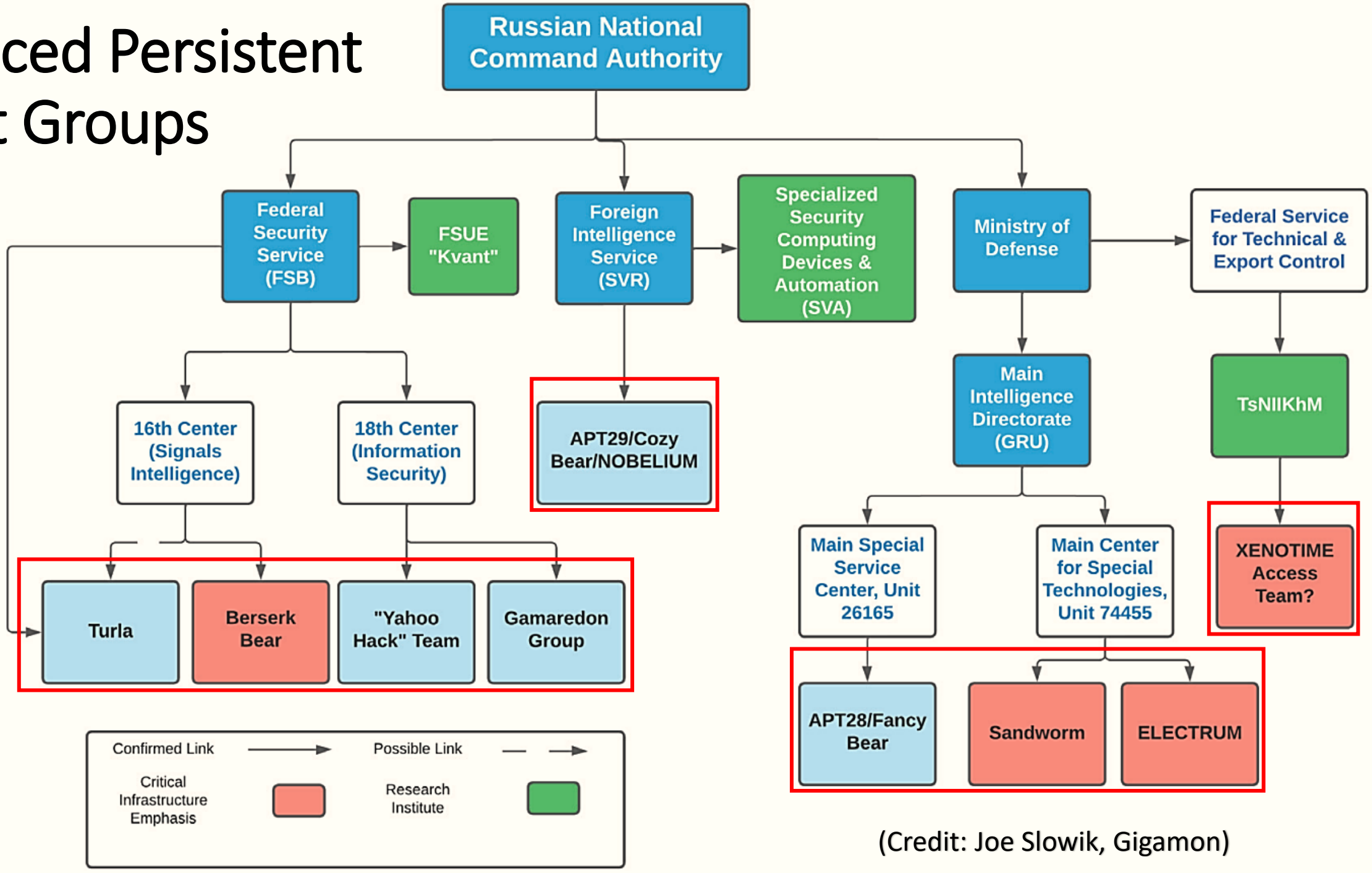
TASS

- **Telecommunications**

VimpelCom

Rostelecom

Advanced Persistent Threat Groups



(Credit: Joe Slowik, Gigamon)

Major Russian Cyber Espionage Operations

2015
TV5 Monde
(GRU)

2016
DNC Hack
(GRU & SVR)

2016
ShadowBrokerz
(FSB)

2017
Olympics
Destroyer
(GRU)

2018
Skripal
Poisonings
(GRU)

2019
Turla hacked
Iranian APT
(FSB)

2013
Yahoo Hack
(FSB)

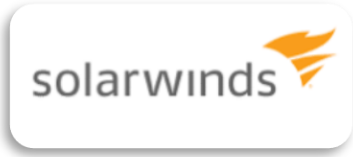
2015/16
Ukraine
Power Cuts
(GRU)

2016
WADA Hack
(GRU)

2017
NotPetya
Wiper Worm
(GRU)

2017
Triton
ICS Attack
(TsNIIKhM)

2020
SolarWinds
(SVR)

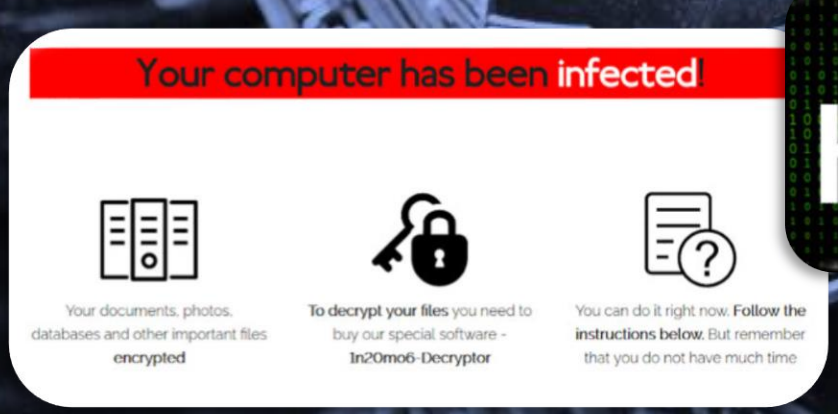


Russian Organized Cybercrime: Deniable Plausability

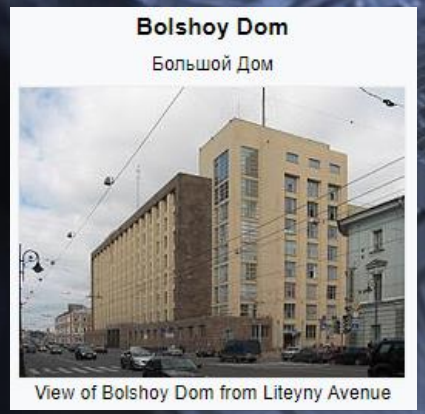
EvilCorp - December 2019

LockerGoga - March 2019

DarkSide - May 2021



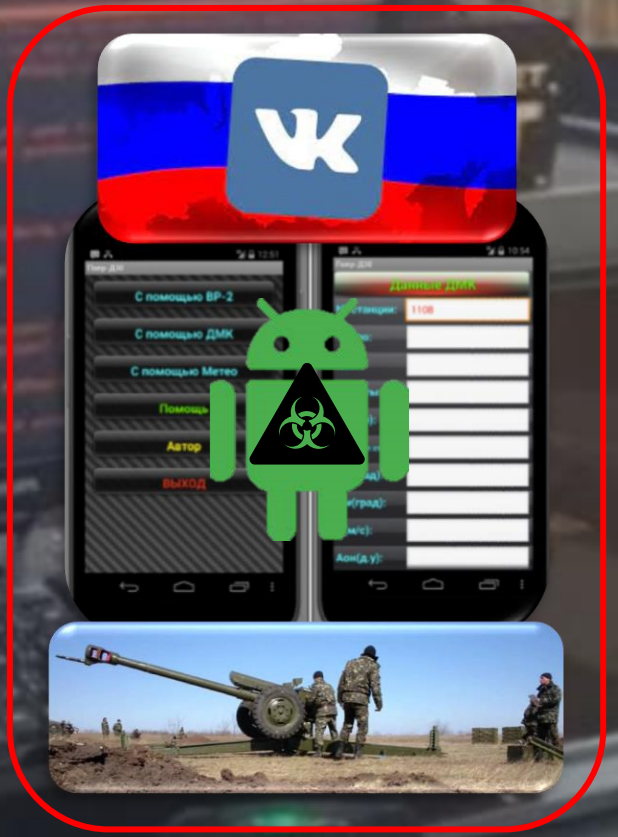
REvil - July 2021

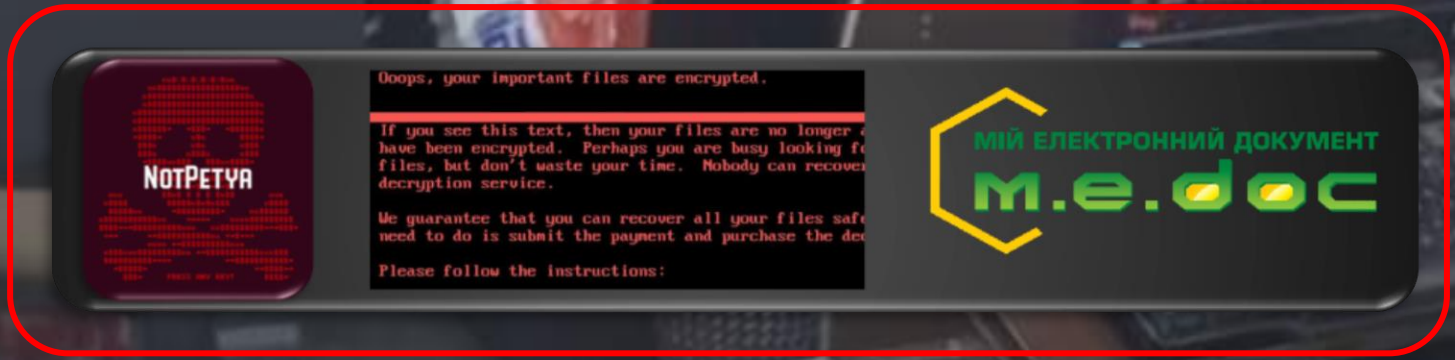


Conti - Feb 2022

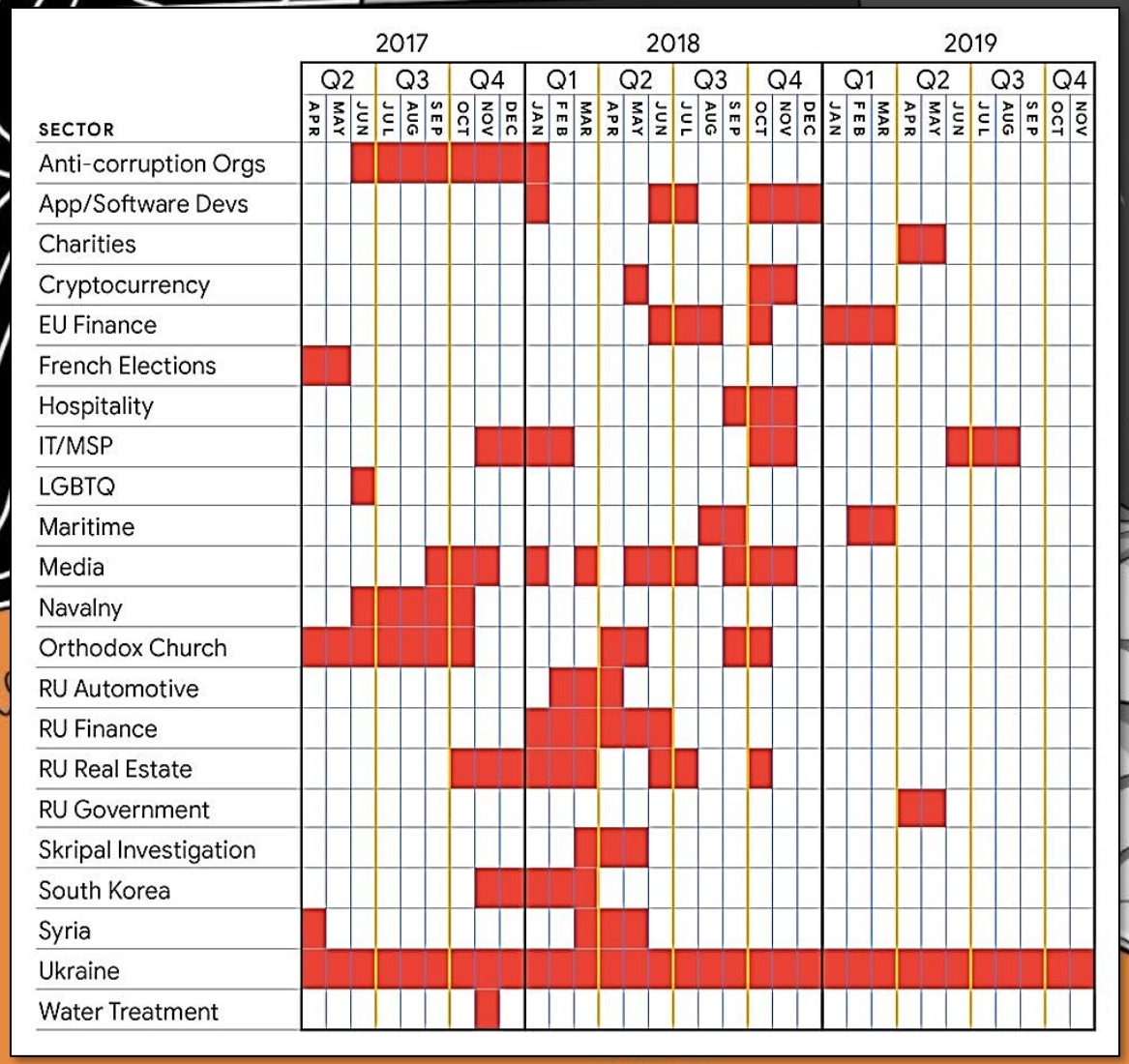
Russian Cyberwarfare in Ukraine pre-2022

- Cyber Berkut hacktivism 2014
- BlackEnergy3/Killdisk Blackout 2015
- Industroyer Blackout attack 2016
- NotPetya wiper worm 2017
- Android Spyware campaign 2018





Sandworm's Campaigns 2017-2019



2017 focus:

- Anti-corruption
- Russian Orthodox Church
- Alexei Navalny

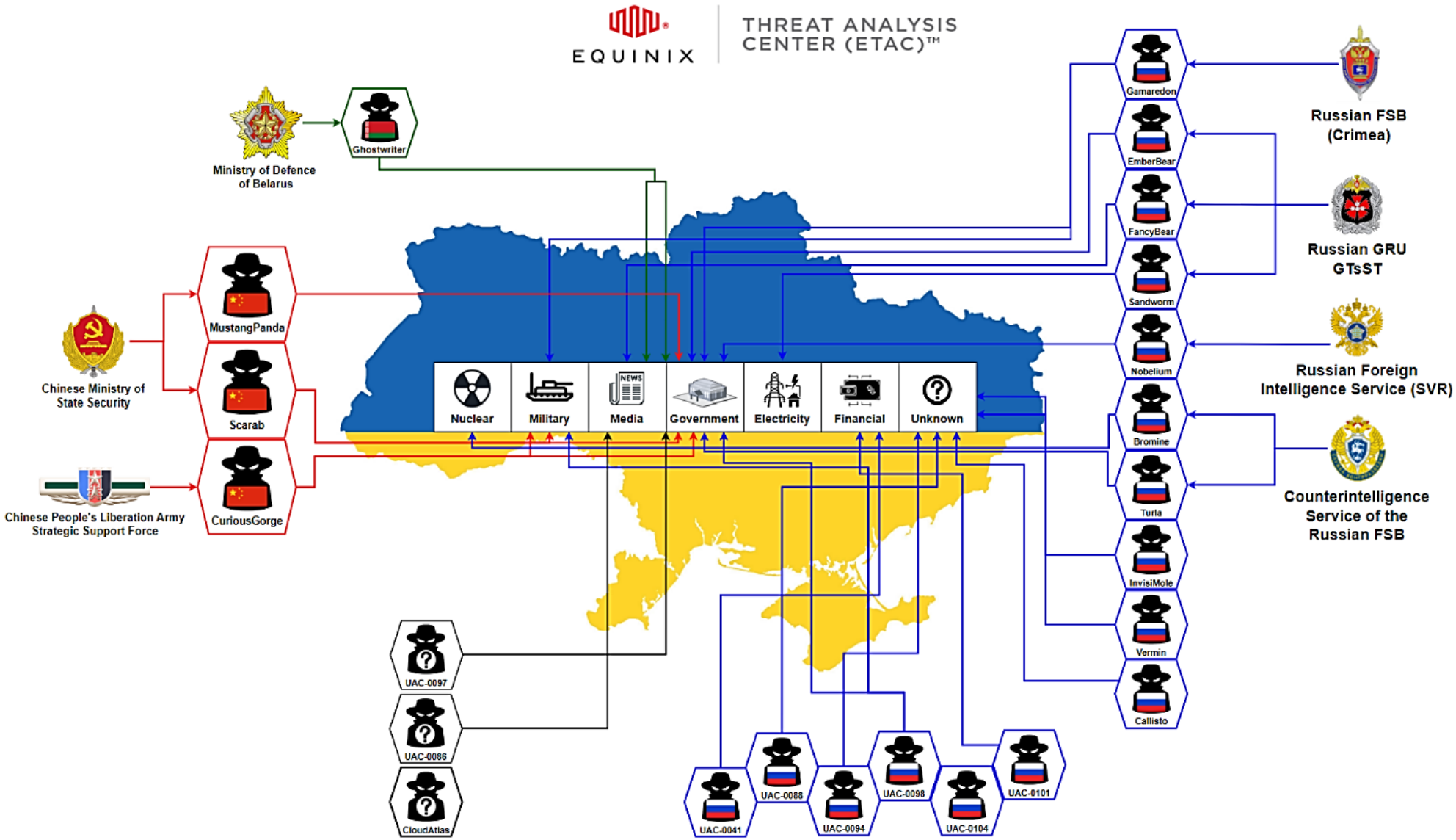
2018 focus:

- Media
- EU and RU Finance
- RU Real Estate
- IT and MSPs
- Sergei Skripal Poisoning Investigation

2019 focus:

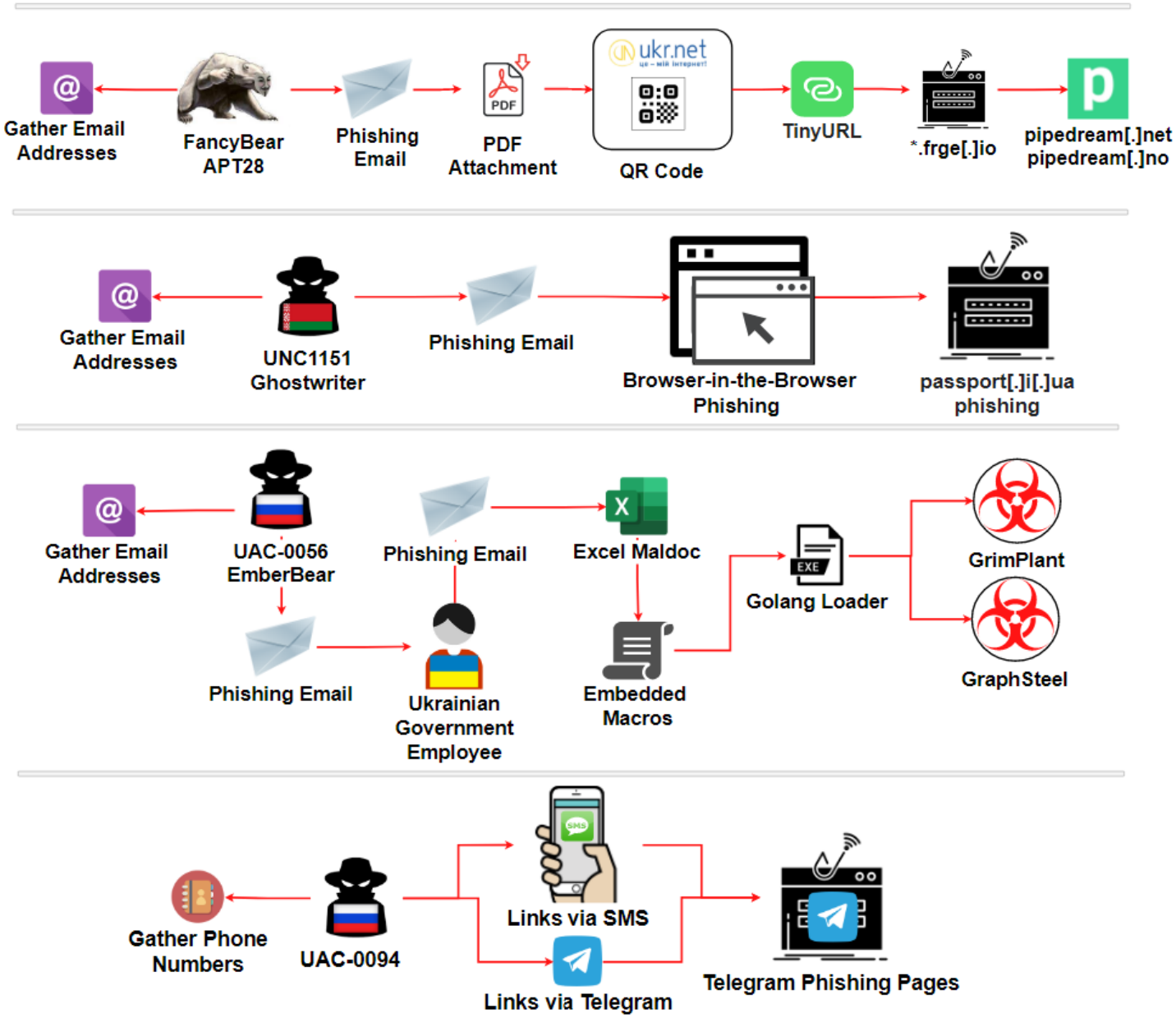
- Ukraine

Russian Cyberwarfare in Ukraine in 2022



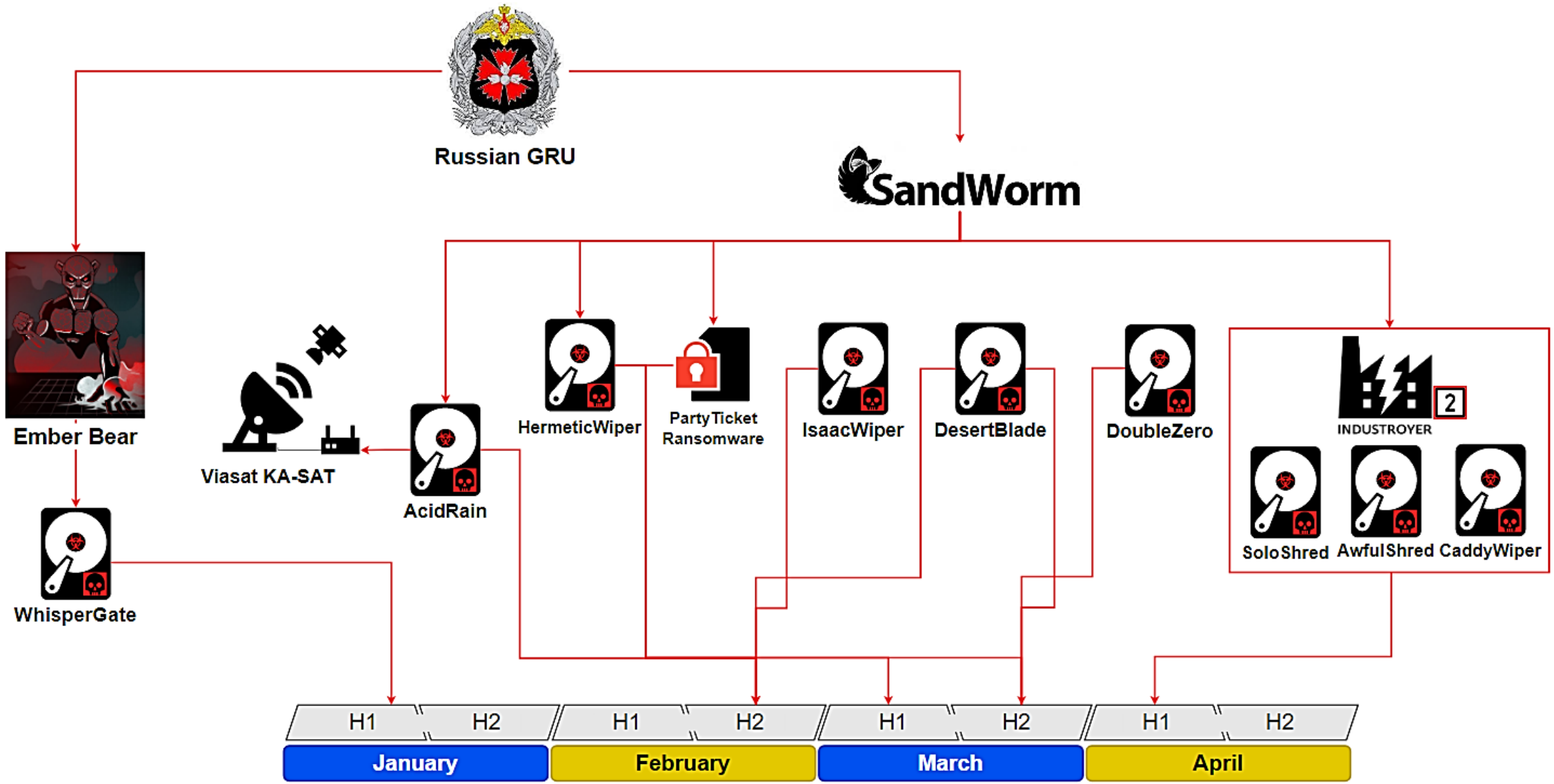
Interesting techniques deployed in Ukraine

EQUINIX | THREAT ANALYSIS CENTER (ETAC)™

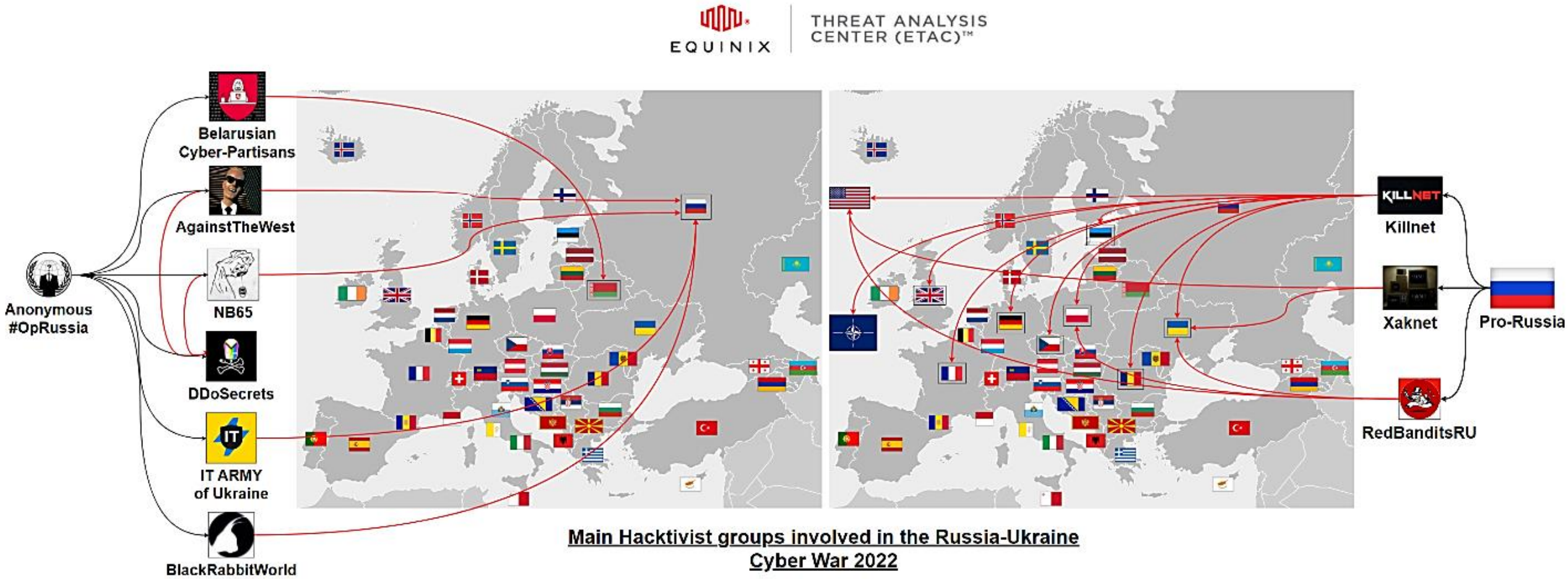


Destructive attacks deployed in Ukraine

EQUINIX | THREAT ANALYSIS CENTER (ETAC)™

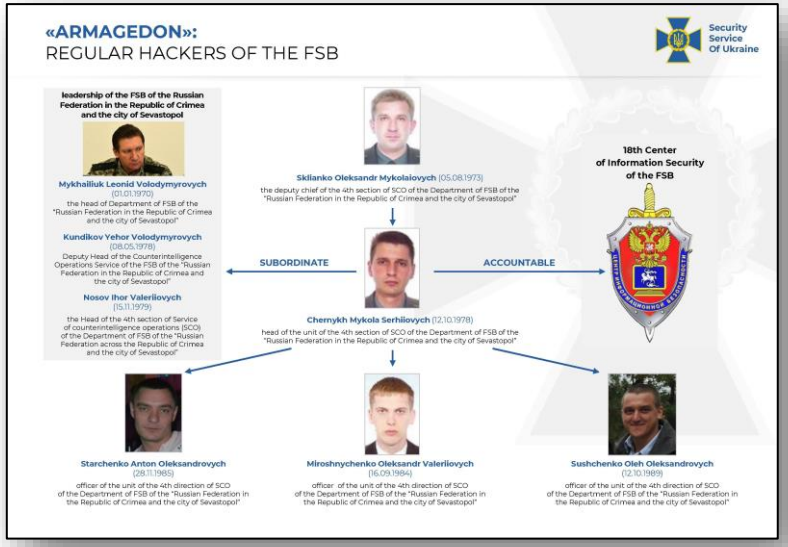


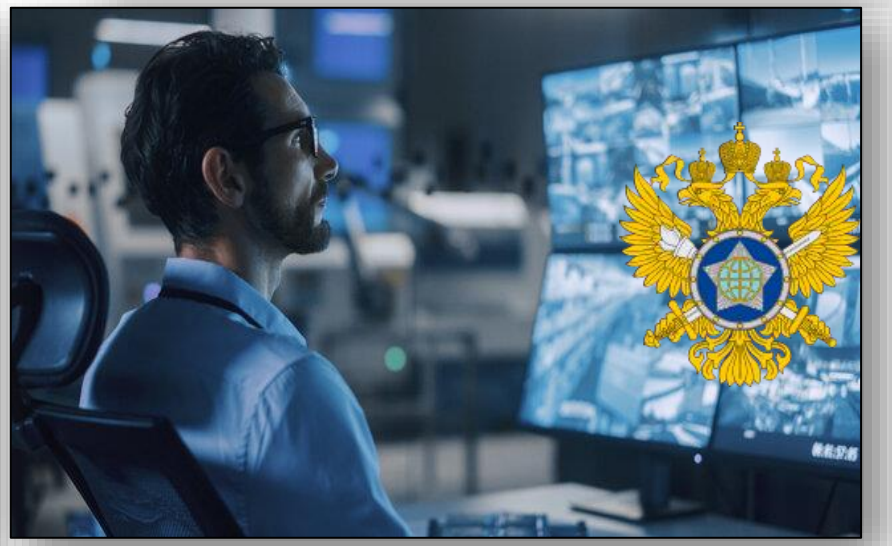
Hacktivism surrounding war in Ukraine



Major Operational Failures

- DOJ indictments of FSB & GRU
- GRU Close Access Operations disrupted by Dutch AIVD
- CCTV of the SVR was hacked by Dutch AVID
- Ukrainian SBU intercepted FSB operations in Crimea
- Numerous Bellingcat reports

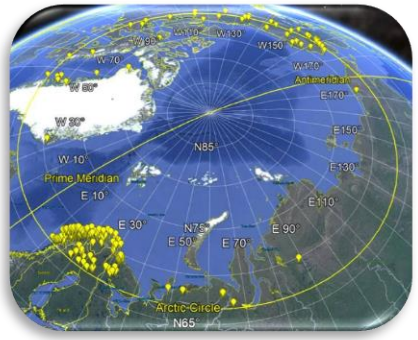




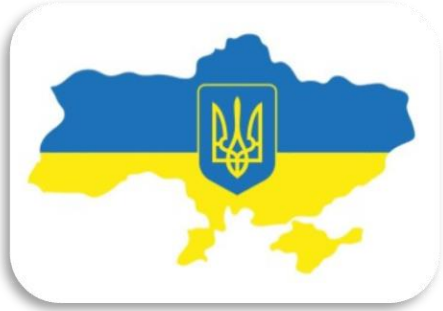
Where do we go from here?

European Energy Crisis

Territorial Disputes

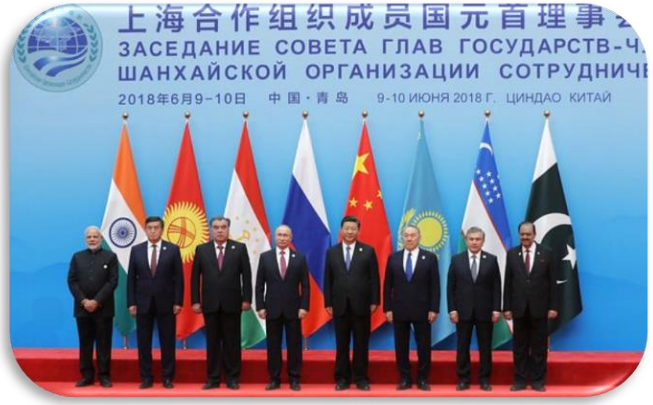


War in Ukraine

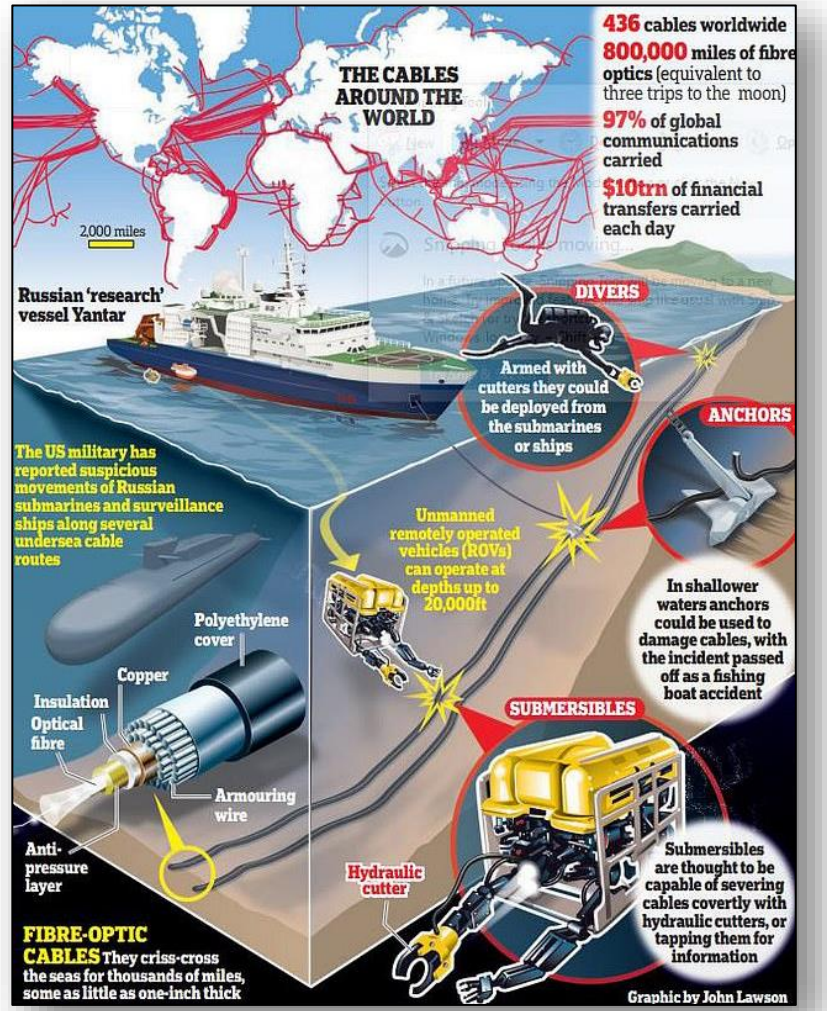


Global Financial System

Anti-Western Coalitions



Global Telecommunications



Thank You

- @BushidoToken on Twitter
- william-t on LinkedIn
- BushidoUK on GitHub
- https://bushidotoken.net
- SANS FOR589: Cybercrime Intelligence
- Darknet Diaries Episode 126
- Equinix Threat Analysis Center (ETAC)
- https://bournemouth2600.org

References

- https://pylos.co/wp-content/uploads/2022/10/Day1-1400-Green-Zeroing-in-on-XENOTIME-analysis-of-the-entities-responsible-for-the-Triton-event.pdf
- https://blog.google/threat-analysis-group/identifying-vulnerabilities-and-protecting-you-phishing/
- https://blog.bushidotoken.net/2020/03/sandworm-new-era-of-cyberwar-and-hunt.html
- https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf
- https://en.wikipedia.org/wiki/CyberBerkut
- https://github.com/curated-intel/Ukraine-Cyber-Operations
- https://www.electrospaces.net/2018/10/the-gru-close-access-operation-against.html
- http://web.archive.org/web/20180126214657/https://www.volkskrant.nl/tech/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~a4561913/