

Q4 2023 Briefing

U.S. Election Assistance Commission (EAC)

Jason Atwell

Program Manager, Strategic Services

Blake Djavaheerian

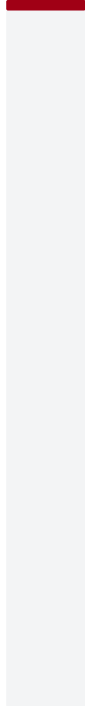
Senior Analyst, Strategic Intelligence & Government (SIG)

AGENDA

- Introduction
- Intelligence Methodology
- The Threat Landscape
- Observed Activity
- Strategic Outlook
- Discussion

Introduction

Executive Summary



Cyber-enabled threat actors across a wide spectrum of intrinsic motivations and geographical origin continue to target U.S. elections infrastructure with malicious operations designed to influence, manipulate, monitor, or disrupt elections, or enable intelligence collection efforts.

Intelligence Methodology

Information Sourcing & Fidelity

Information Sources:

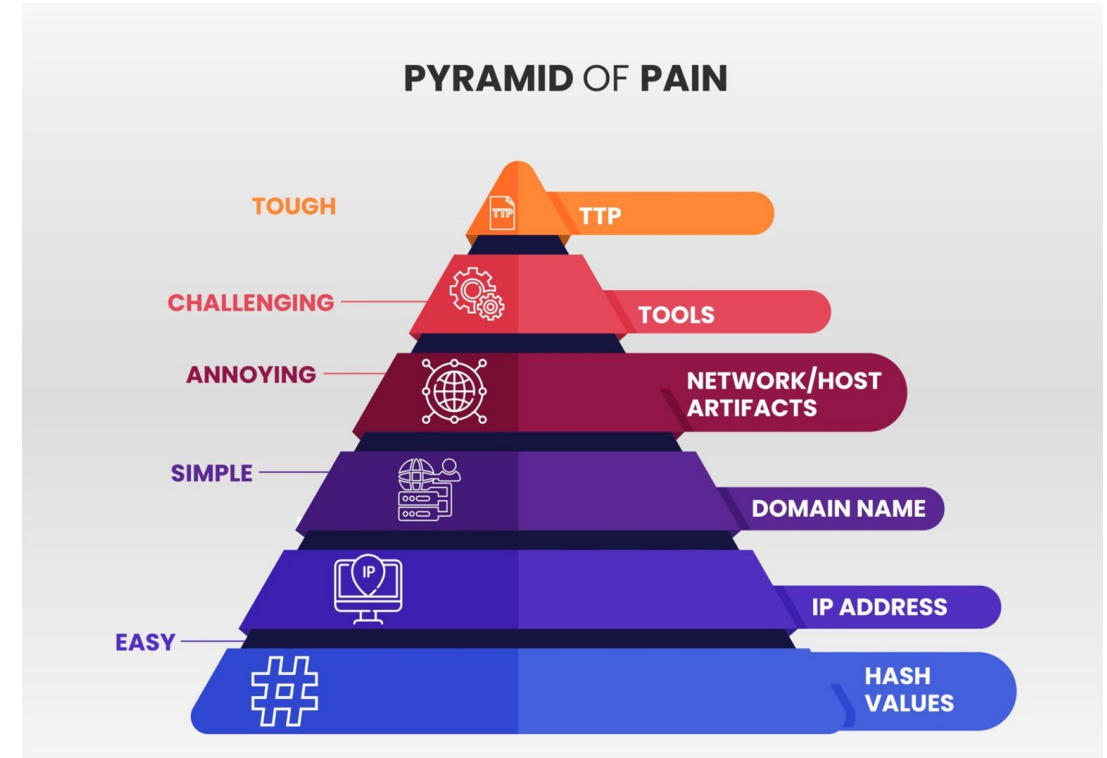
- Mandiant Engagements
- Information Sharing Partnerships
- Open-Source Reporting
- Advanced Research Methods

Indicators of Compromise (IoCs):

- Static observables, e.g. files, network artifacts, and commands strings
- Inverse relationship between ease of acquisition and ongoing usefulness

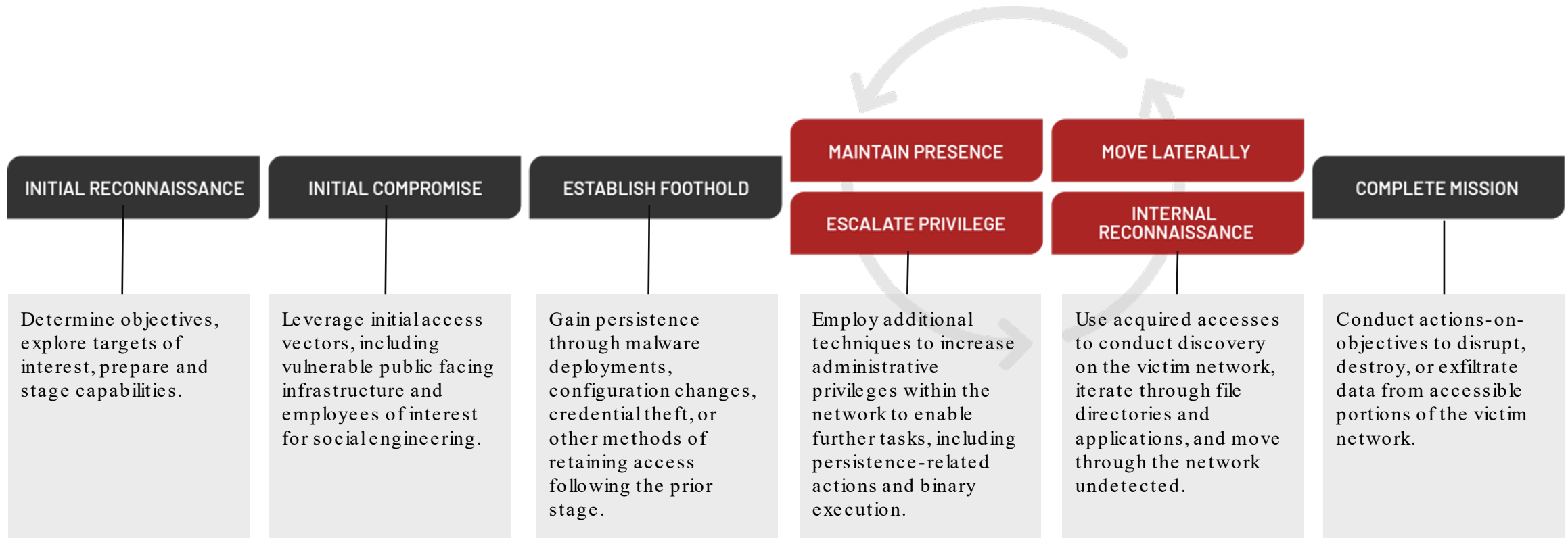
Behavioral Indicators:

- Attack patterns providing buckets to standardize the way we communicate adversarial actions
- Alone provide limited information, but in combination can give critical context
- Much more difficult to identify, analyse, and act on in comparison to static indicators



Source: <https://www.linkedin.com/pulse/pyramid-pain-how-make-attackers-life-harder-murray-pearce/>

Attack Lifecycle



MITRE ATT&CK: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact

The Threat Landscape

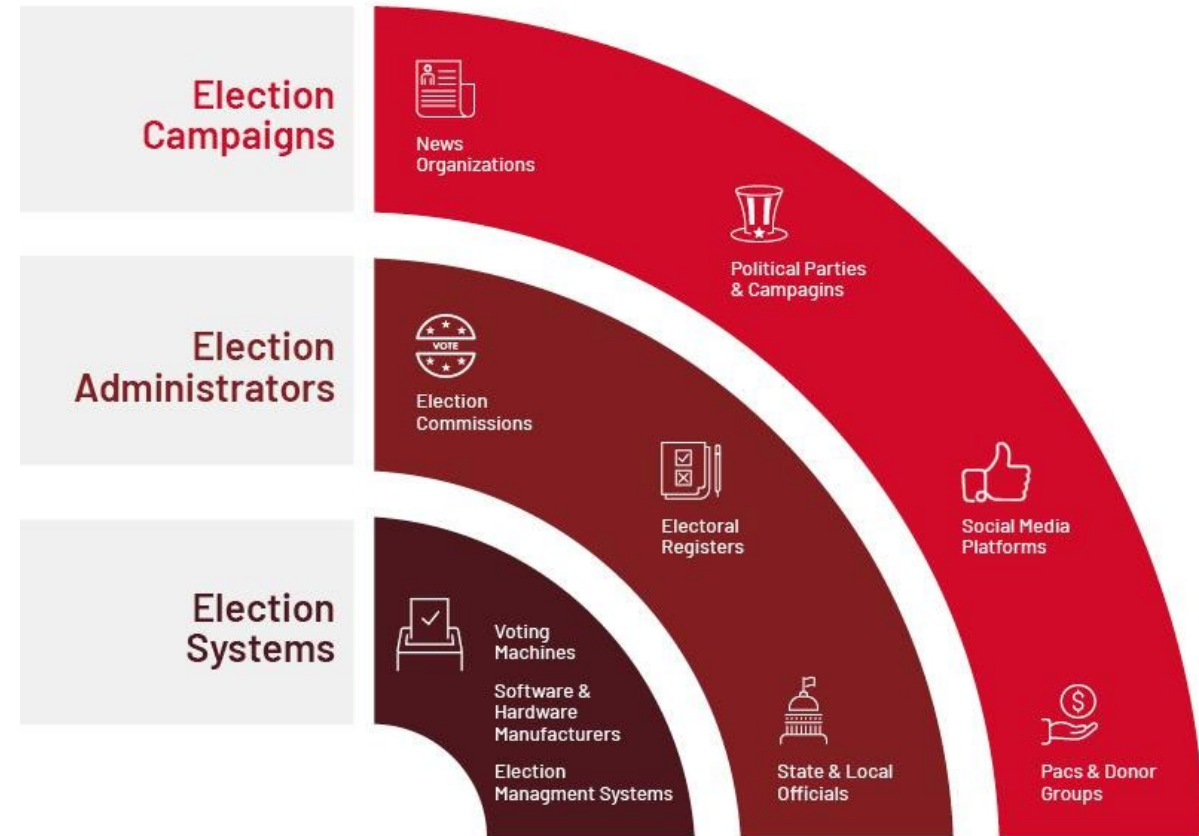
Identifying Adversary Objectives

- An adversary's primary underlying motivations inform targeting as well as the manner and speed they conduct operations
- Three primary motivations:
 - Direct Election Interference
 - Intelligence Gathering / Monitoring
 - Information Operations (IO)
- Individual objectives are often multi-dimensional and can reflect amorphous, evolving, and/or overlapping adversary motivations



Distinguishing Targets within the Elections Ecosystem

- Campaigns
 - News Organizations
 - Political Parties & Campaigns
 - Social Media Platforms
 - PACs & Donor Groups
- Administration
 - Election Commissions
 - Electoral Registres
 - State & Local Officials
- Systems
 - Voting Machines
 - Software & Hardware Manufacturers
 - Election Management Systems



A Dynamic Threat Landscape



Underlying Motivations Drive Decision Making

- Malicious activity represents humans at a keyboard
- Activity may be highly tailored toward particular sectors or individual organizations
- Underlying motivations range from destruction and disruption to information theft, among others



Professionalism, Structure, and Resourcing

- Attackers may flexibly calibrate their capabilities depending on the target
- Threats may linger carefully for months or even years within a network
- Attackers may pivot their tactics based on findings from within a victim network

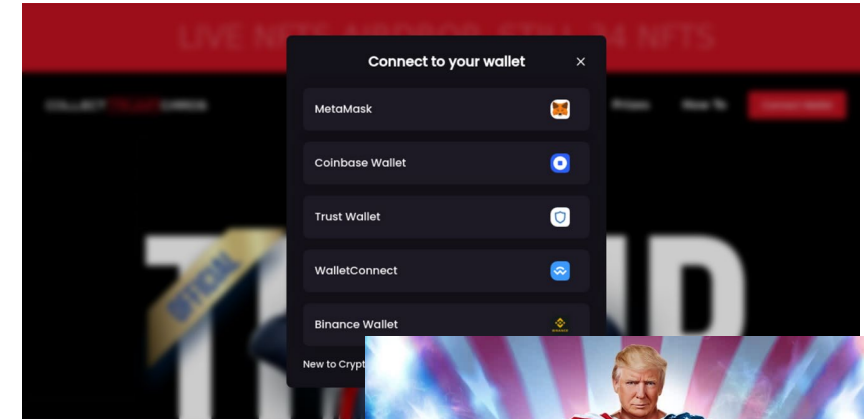


Persistence in Pursuit of Set Objectives

- Resolute objectives motivate threats to continuously pursue targets over the long term
- Greater familiarity with a given network means a threat is more likely to identify and leverage additional access vectors
- Persistence mechanisms mean partial eviction may not result in complete remediation

Emerging Threat: Cryptocurrency -Based Complications

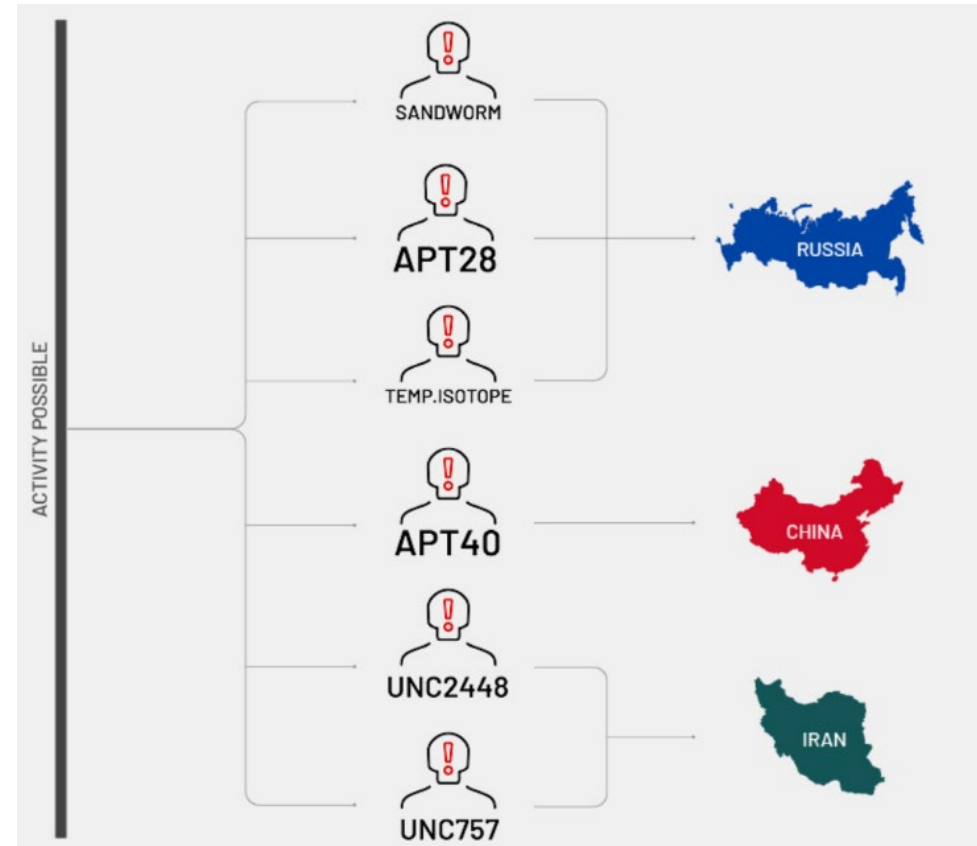
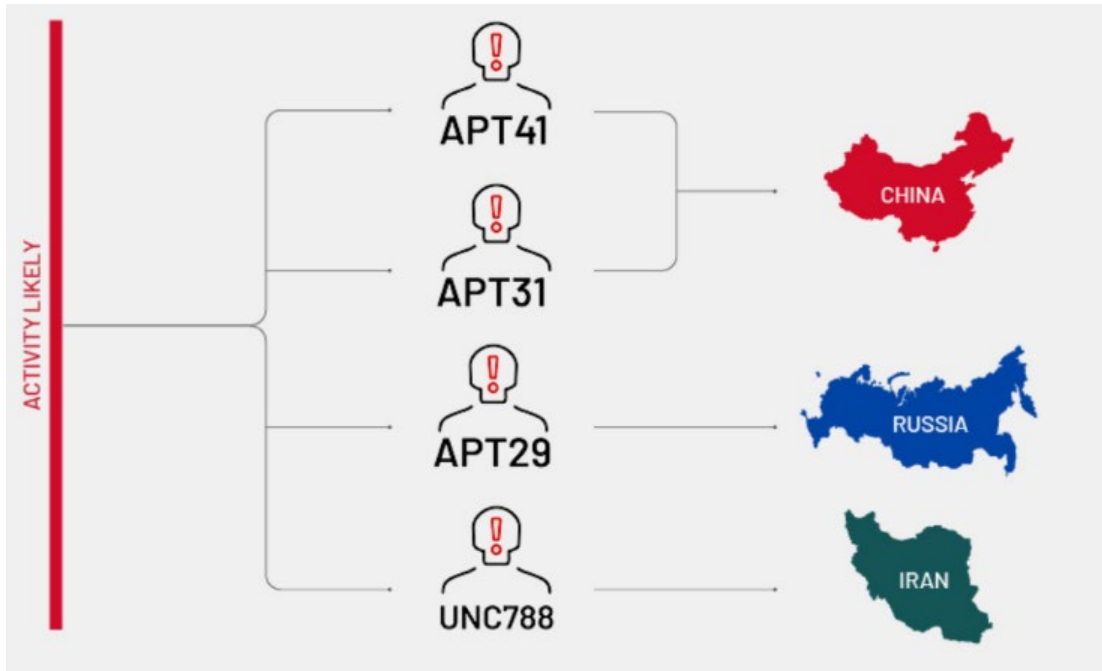
- BLUF: The proliferation of cryptocurrency has accelerated the extent, rate, and breadth of financial fraud connected to U.S. elections.
- Ongoing Observed Activity
 - Trump NFT collection owners targeted with spearphishing
 - Drainer-as-a-Service (DaaS) campaigns directed at donor's cryptocurrency wallets
- Potential Activity
 - Falsified donation platforms' potential for candidates accepting cryptocurrency
 - Potential for unauthorized donors from foreign entities unable to be traced
 - Cryptocurrency utilized for purchasing adversary infrastructure
 - Seen in the 2016 & 2020 presidential elections in support of identified IO and phishing campaigns



Observed Activity

Framing the (Advanced Persistent) Threat

State Sponsored Cyber Espionage Groups Likely to Target US Elections



Framing the (Advanced Persistent) Threat

Intrusion Set	Likely Country of Origin	Recent Election -Related Targeting	Historical Election -Related Targeting
APT41	China	In 2021, China-nexus APT41 reportedly conducted a months-long campaign targeting vulnerable Internet-facing web applications to gain initial access into at least six U.S. state government networks. This campaign included the exploitation of zero-day vulnerabilities including USAHerds vulnerability CVE-2021-44207 and Log4j (CVE-2021-44228).	In mid-2016, APT41 targeted media outlets in Hong Kong ahead of the legislative council election using spearphishing to deploy the malware SOGU.
APT31	China	In February 2022, Google reportedly blocked an APT31 phishing campaign targeting high-profile Gmail users affiliated with the U.S. government.	APT31 reportedly targeted Biden campaign staff with consistent phishing attempts throughout 2020, with at least some featuring credential collection attempts spoofing McAfee.
APT29	Russia	APT29 regularly conducts phishing activity that likely primarily targets diplomatic and foreign policy-focused entities in Europe and the Americas.	According to open sources—and likely separately from concurrent activity by APT28—APT29 compromised the Democratic National Committee (DNC) in advance of the 2016 U.S. presidential election.
APT42	Iran	In mid-2021, APT42 targeted researchers at a Middle East-based think tank, U.S. government officials, and others using the compromised email account of a U.S.-based researcher.	APT42 likely targeted U.S. election campaign staff in late 2019 and summer 2020.

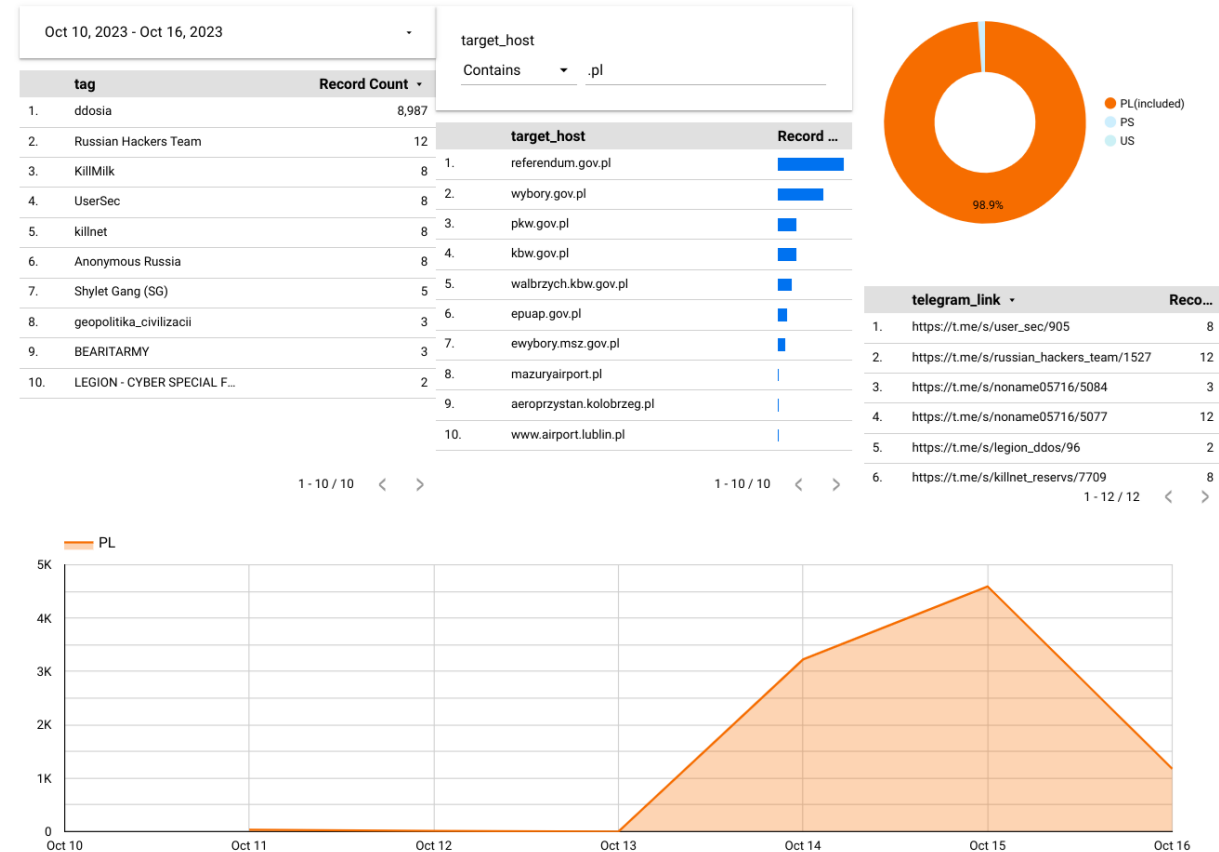
Activity Observed Parallel to the 2023 Polish Elections

Background:

- Poland held parliamentary elections to determine the next slate of members of the Sejm (lower house) and Senate on 15 October
- Highly polarised election between the conservative incumbent Law and Justice (PiS) party government and the country's opposition

Observations:

- Leading up to the election, Mandiant identified an UNC 1151 spearphishing campaign using lure documents related to the Polish election
 - Whether the campaign targeted entities related to elections is unclear due to limited technical and circumstantial evidence
- Mandiant identified a clear uptick in DDoS traffic targeting Polish government and airport websites in tandem with the election beginning on 13 October and peaking on the 15th
 - Nationalistic, pro-Russia hacktivist groups led a majority of the discernible activity



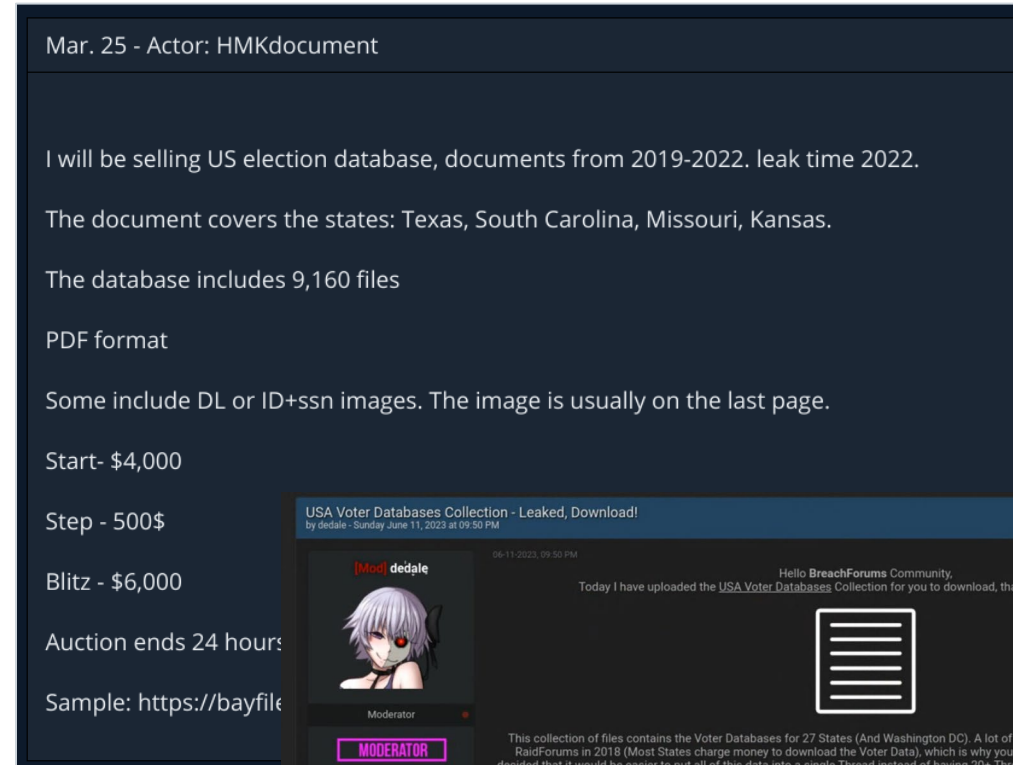
Financial Motivations for Targeting Elections

Data Brokerage:

- Elections provide a wide range of both sensitive and sensitive-seeming information for criminals to leverage
 - Cybercriminals frequently advertise for sale files they've stolen, acquired through a third-party leaker, or falsified entirely to generate revenue
 - Example: Forum user HMKdocument advertised a database of elections data pertinent to multiple states allegedly containing social security numbers, names, and other personally identifiable information (PII)

Extortory Disruption:

- Ransomware groups as well as other cybercriminals employ extortion to pressure victim entities for payment
- Extortion may be accomplished through one or a combination of:
 - Network denial via DDoS
 - Endpoint denial via ransomware deployment / host encryption
 - Data confidentiality denial via information theft



Mar. 25 - Actor: HMKdocument

I will be selling US election database, documents from 2019-2022. leak time 2022.

The document covers the states: Texas, South Carolina, Missouri, Kansas.

The database includes 9,160 files

PDF format

Some include DL or ID+ssn images. The image is usually on the last page.

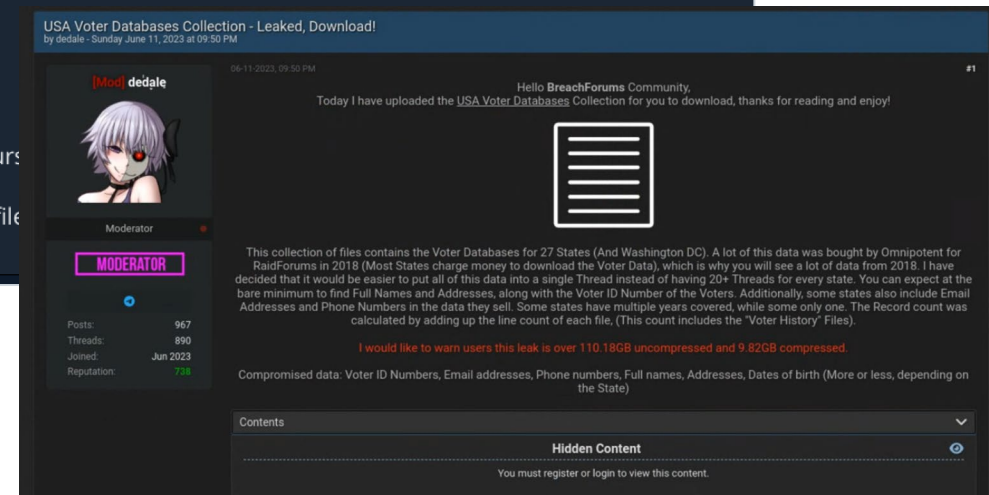
Start- \$4,000

Step - 500\$

Blitz - \$6,000

Auction ends 24 hours

Sample: <https://bayfile>



USA Voter Databases Collection - Leaked, Download!
by dedale - Sunday June 11, 2023 at 09:50 PM

06-11-2023, 09:50 PM

Hello BreachForums Community,
Today I have uploaded the USA Voter Databases Collection for you to download, thanks for reading and enjoy!

[Mod] dedale
Moderator

Posts: 967
Threads: 890
Joined: Jun 2023
Reputation: 735

This collection of files contains the Voter Databases for 27 States (And Washington DC). A lot of this data was bought by Omnipotent for RaidForums in 2018 (Most States charge money to download the Voter Data), which is why you will see a lot of data from 2018. I have decided that it would be easier to put all of this data into a single Thread instead of having 20+ Threads for every state. You can expect at the bare minimum to find Full Names and Addresses, along with the Voter ID Number of the Voters. Additionally, some states also include Email Addresses and Phone Numbers in the data they sell. Some states have multiple years covered, while some only one. The Record count was calculated by adding up the line count of each file, (This count includes the "Voter History" Files).

I would like to warn users this leak is over 110.18GB uncompressed and 9.82GB compressed.

Compromised data: Voter ID Numbers, Email addresses, Phone numbers, Full names, Addresses, Dates of birth (More or less, depending on the State)

Contents

Hidden Content

You must register or login to view this content.

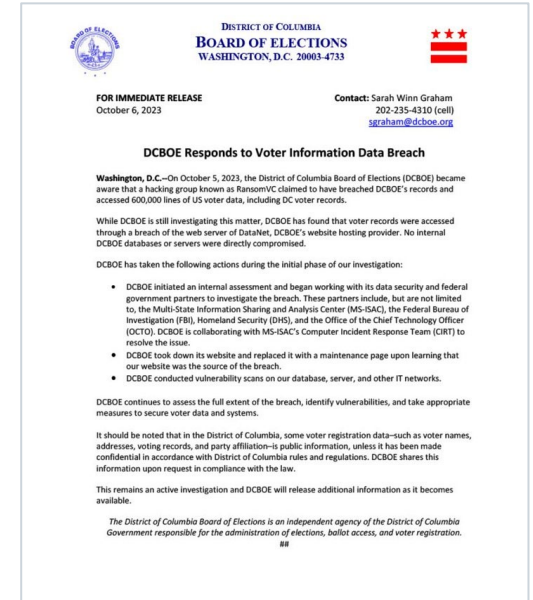
RANSOMEDVC Targets D.C. Board of Elections

Background:

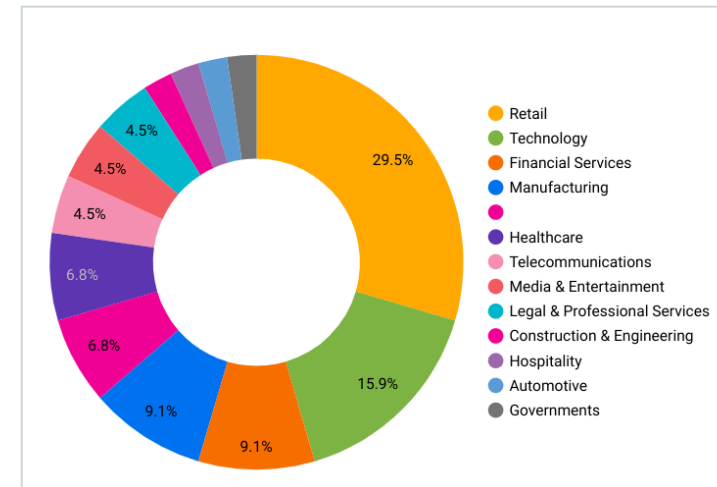
- On 06 Oct. 2023, the Washington, D.C., Board of Elections (DCBOE) announced their awareness that on 05 Oct. the group RANSOMEDVC claimed access to a significant volume of U.S. voter data
- According to DCBOE, their investigation showed that the information was stolen through a breach of an externally hosted web server

Additional Context:

- Mandiant monitoring indicates only a single claim out of RANSOMEDVC's (alt: RansomVC) total 44 alleged victims has impacted a government-sector entity
 - Prior engagements Mandiant has led in response to claimed incidents suggest a frequent disparity between the group's claims and its actual operational impacts
 - Exaggeration of the group's claimed impacts
 - Falsification of sourcing
 - Repackaging information stolen from one entity to appear as though an adjacent or related organization was the victim



Source: <https://wjla.com/news/local/elections-board-hack-technology-data-breach-voter-information-washington-dc-thousands-ransomvc-datantet-website-public-records-private-records-vulnerabilities-datantet-federal-bureau-of-investigation-fbi-dcboe-election>



ROYAL Ransomware Disables Dallas City Functions

Background:

- On 06 Sept. 2023, the City of Dallas released an AAR detailing a mid-2023 ransomware event against city systems
- The incident was quickly attributed to ROYAL on 03 May when the group executed ransomware across the City environment
 - Physical copies of the group's ransom notes reportedly printed within City facilities
 - Based on Mandiant monitoring, ROYAL has claimed over 115 victims so far in 2023
 - Likely even more victims than this count, due to immediate ransom payments

Outcomes:

- The City's reporting provided additional insight into:
 - Adversary dwell time on the municipal network
 - Initial access via remote service in early April; ransomware deployment almost a month later
 - Specific services disrupted
 - Emergency response operations, administrative services,
 - Direct costs of incident (~\$8.5 million)
 - Indirect costs less straightforward to calculate



THE CITY OF DALLAS RANSOMWARE INCIDENT: MAY 2023

Incident Remediation Efforts and Resolution

The City of Dallas
Department of Information & Technology Services
ITS Risk Management, Security, and Compliance Services
September 20, 2023

Document Source:
<https://dallascityhall.com/DCH%20Documents/dallas-ransomware-incident-may-2023-incident-remediation-efforts-and-resolution.pdf>

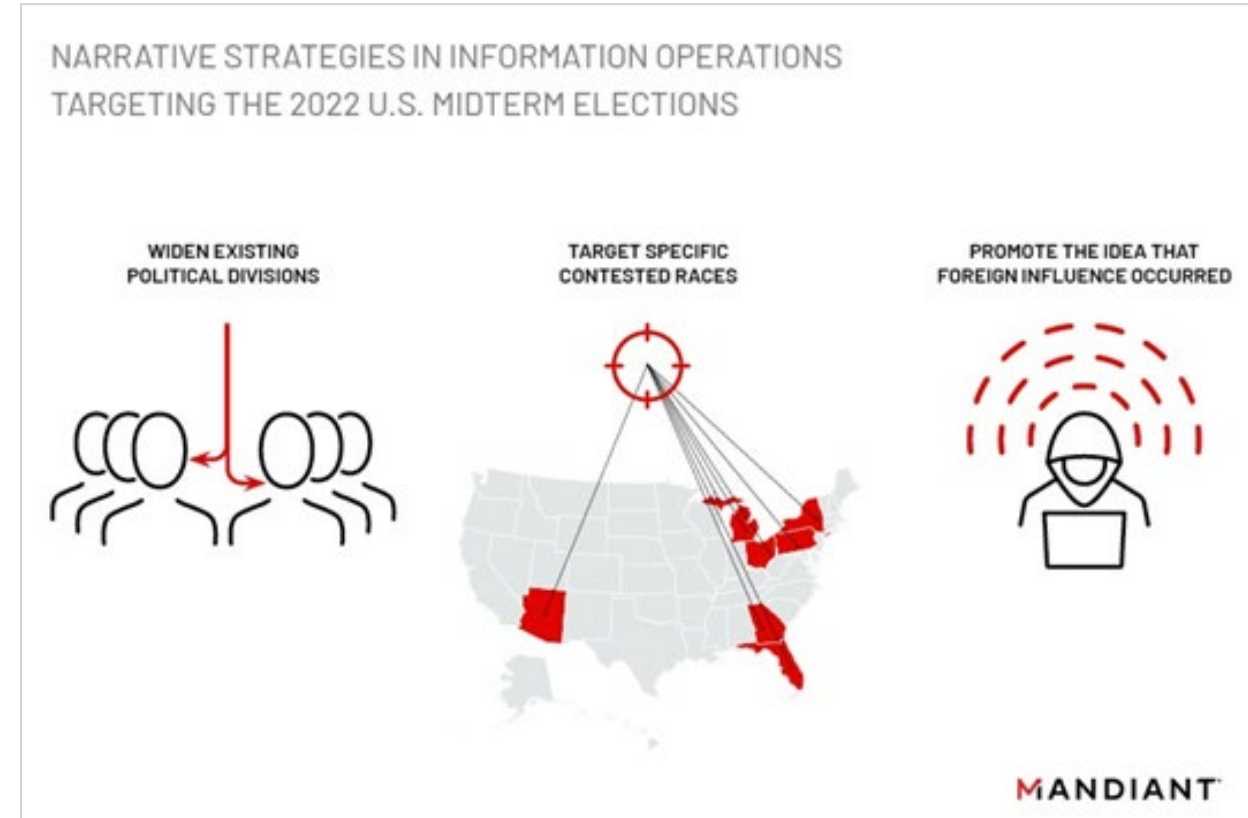
The Spectrum of Contemporary IO Activity

Primary IO Objectives Observed During 2022 Midterm Elections:

- Widen existing political divisions
- Target specific contested races
- Promote speculation of foreign interference

IO Strategies:

- Coordinated inauthentic activity
- Hack-and-leak operations
- Production and publication of disinformation
- Claims of disruptive activity targeting election infrastructure
- Claims of activity targeting the confidentiality of election data



The Spectrum of Contemporary IO Activity

Cluster of Activity	Likely Country of Origin	Description
Ghostwriter	Belarus	Ghostwriter is a Belarus-nexus influence campaign that frequently targets primarily Eastern European audiences with fabricated content intended to harm the North Atlantic Treaty Organization (NATO) and its allies, including by compromising legitimate websites to publish anti-West materials.
Secondary Infektion	Russia	Since at least summer 2019, Secondary Infektion has promoted narratives heavily targeting Ukraine, other post-Soviet states, and Turkey, often painting those countries' collaboration with the West as dangerous to local populations. In the case of Ukraine, operations have almost always portrayed the Ukrainian Government—and Ukrainian President Volodymyr Zelensky in particular—as incompetent and corrupt. These IO operations have commonly used fabricated source material to substantiate these narratives, including forged documents, letters, and screenshots.
DragonBridge	China	First identified in mid-2019, the DragonBridge campaign has promoted pro-People's Republic of China (PRC) narratives surrounding various global developments, including the suspected Chinese surveillance balloon incident and COVID-19 vaccine research. Vetted intelligence partners have observed DragonBridge-linked social media accounts publish and promote both positive and negative commentary regarding American politicians, likely as a means to sow discord rather than an attempt to influence voter preferences.
Roaming Mayfly	Iran	Roaming Mayfly—a potential revival of the 2019 influence campaign Endless Mayfly—is a pro-Iran IO operation that has directed Arabic-language social media content to assert anti-West narratives in relation to topics including the war in Ukraine, nuclear disarmament, and Saudi Arabia's military involvement in Yemen.

IO Activity Observed During the 2022 U.S. Midterm Elections

Cluster of Activity	Activity Observed
DRAGONBRIDGE	<ul style="list-style-type: none"> ● 07 - 08 Nov: Publication of articles containing narratives antagonistic toward incumbent senators Marco Rubio and Ted Cruz <ul style="list-style-type: none"> • Notably, articles targeting both politicians were identical and appeared to have been written with the intent to target Cruz and later repurposed to target Rubio, based on unchanged biographical information left within the articles posted ● 08 - 09 Nov: DRAGONBRIDGE accounts post Chinese-language messaging urging Floridians to vote for Rubio along with the English-language hashtags #midterm and #elections, including occasionally via the same accounts that promoted messaging antagonistic toward Rubio. ● In a third set, DRAGONBRIDGE social media accounts continued to promote narratives pertaining to the midterms as well as broader U.S. political issues. Topics addressed included: <ul style="list-style-type: none"> • Rising inflation • Labor strikes • Abortion rights • Increasing divisiveness and waning trust in the U.S. political system
HaiEnergy	<ul style="list-style-type: none"> ● Websites attributed to this pro-PRC IO campaign published an article alleging that former White House Chief Strategist Steve Bannon was “deeply involved in the struggle between the two factions” in the 2022 elections, reflecting the campaign’s likely intention to sow highlight and antagonize U.S. political partisanship
EvenPolitics	<ul style="list-style-type: none"> ● Website that has continually published plagiarized election-related articles aimed at U.S. audiences and promoting narratives sympathetic to Iranian state political interests, including stories related to the high-profile races in Michigan and Pennsylvania as well as others on divisive political topics, such as the relationship between Donald Trump and other prominent members of the Republican party.



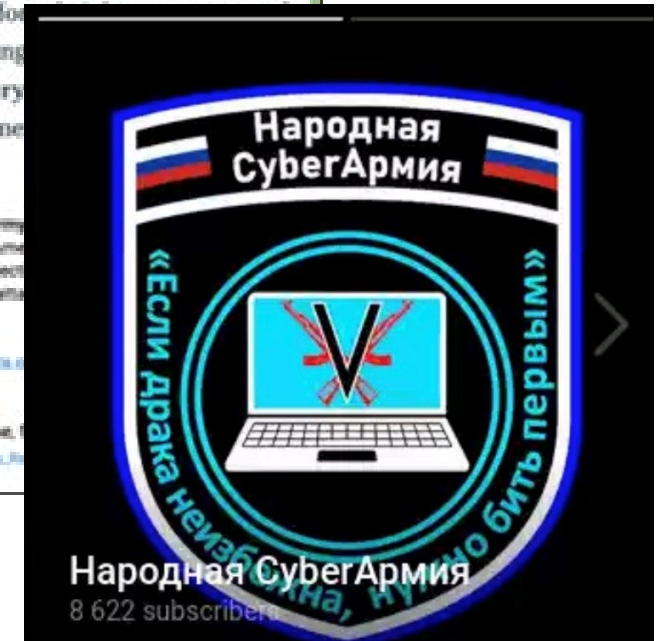
Pro-Russia “Hacktivist” Groups Promoting Election-Related Narratives

Amid the U.S. midterms, multiple self-proclaimed pro-Russia hacktivist groups promoted election-related narratives on their respective Telegram channels, likely in efforts to build perception of their influence over these elections as well as potentially to waste limited election defender resources:

- Between 06 and 08 November 2022, XakNet Team, KillNet, and Anonymous Russia posted jokes, taunts, and rhetorical polls related to the midterm elections.

On midterm election day 2022, the “Cyber Army of Russia” group claimed multiple DDoS attacks against U.S. organizations, citing the midterms as cause:

- The group published a Telegram post claiming a DDoS attack on the website of the Democratic National Committee (DNC) (democrats.org), stating, "Today we attack the American Democrats as a gift to the Republicans for the elections!"
- Another Telegram post claimed a DDoS attack targeting the website of the Mississippi Secretary of State, noting: "We hit the section [of the site] that is directly related to the elections"
- Notably, Mandiant has assessed with moderate confidence that the moderators of the group's Telegram channel (@cyberarmyofRussia_reborn) are coordinating their operations with Russian Main Intelligence Directorate (GRU)-sponsored threat actors

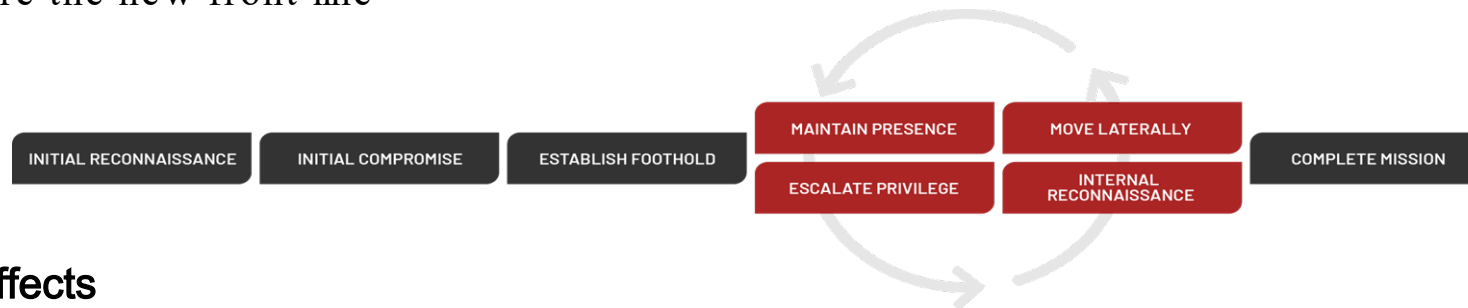


Strategic Outlook

Threat Commonalities

“Traditional” Cyber Threats

- Generic phishing and spear-phishing continue to provide indispensable initial access vectors for threat actors
- A “campaign” still requires a mix of skills and capabilities
- Non-election specific issues such as ransomware can quickly play a role in public confidence, integrity, and availability
 - Activity doesn’t have to directly target elections to impact them, either immediately or down the line
- Supply chains are the new front line



Cognitive Domain Effects

- Perception of the attack and its consequences
- There is no nuance in the media
- The future isn’t now, but some may think it is

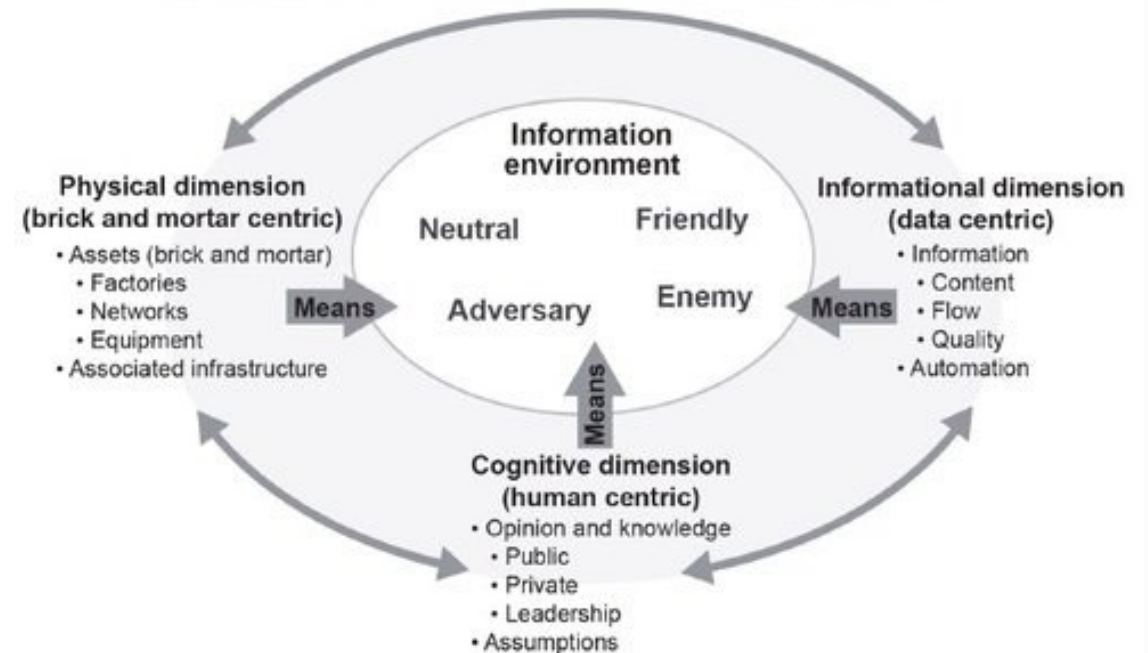
Identification of Key Terrain

Placing Resources Where They Do the Most Good

Domains to Address:

- Traditional Network Defenses
- Leadership Education
- Private Sector Partnerships
- Data Resilience and Redundancy
 - COOP Planning
- Adversarial Intelligence
 - Prioritized requirements

Today's global information environment means that messages and actions delivered to one audience will reach other audiences.



Hardening and Resilience Considerations

Cyber:

- Hunting
- Exercises
- Threat intel for the masses

Cyber - Cognitive:

- “Two-person” integrity
- Wargaming decisions

Cyber - Physical:

- Where does the IT work happen?



Discussion

Thank you