Q3 2024 Briefing

U.S. Election Assistance Commission (EAC)

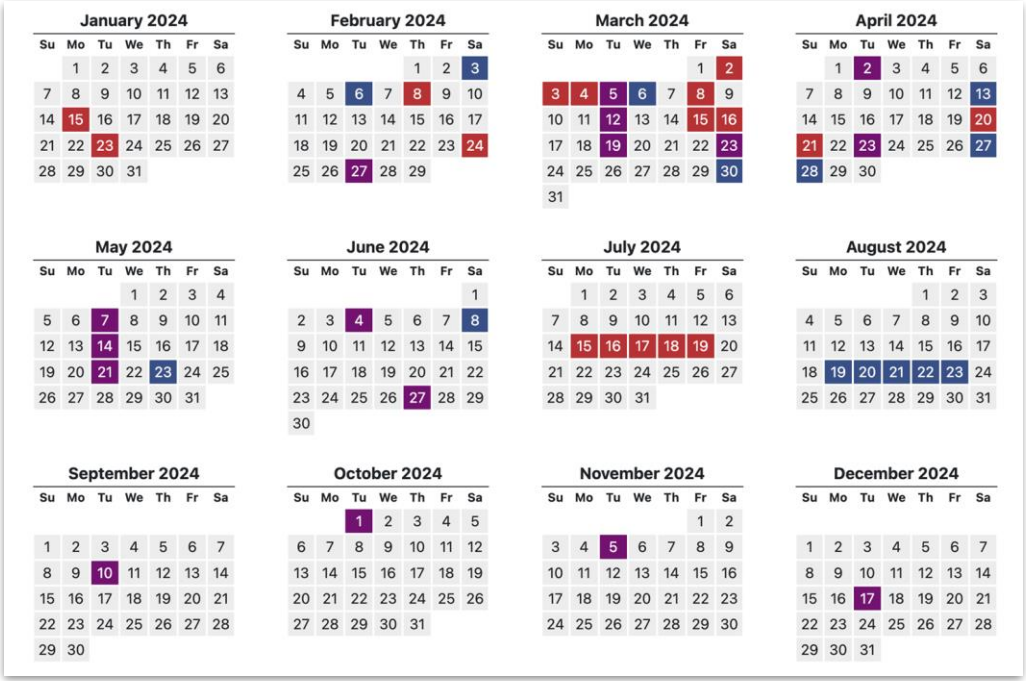
Google Cloud
Security

TLP: GREEN

Contents

01 Introduction

2024 U.S. Presidential Election Calendar



January 2024

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

February 2024

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29		

March 2024

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

April 2024

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

May 2024

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

June 2024

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

July 2024

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

August 2024

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

September 2024

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

October 2024

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

November 2024

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

December 2024

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

October 01: VP Debate

November 05: General Election Day

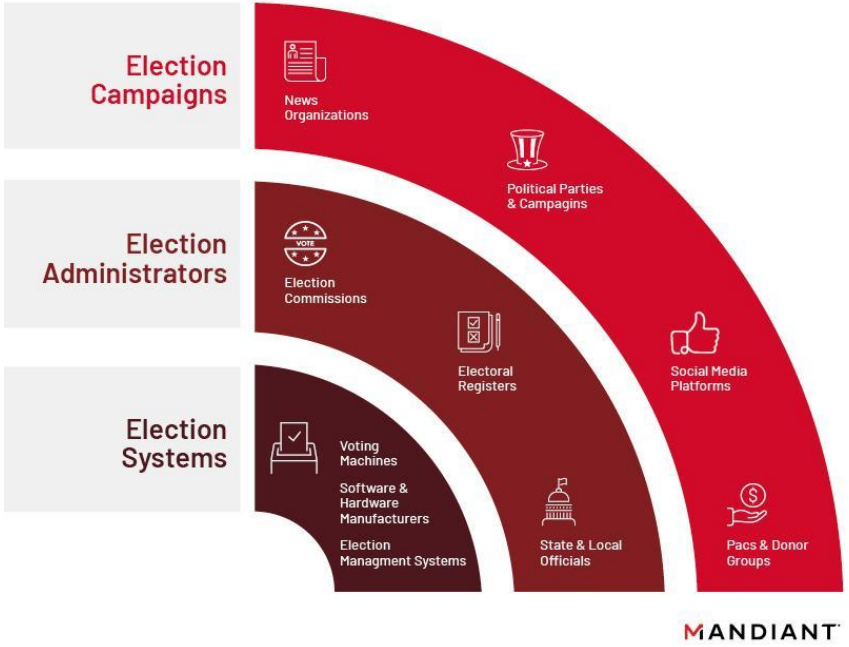
December 17: Electors Cast Votes

Adversary Objectives

- An adversary's primary underlying motivations inform targeting and the manner and speed with which they conduct operations.
- Individual objectives are often multi-dimensional and can reflect amorphous, evolving, and overlapping adversary motivations.
- Primary Threat Types:
  - State-nexus
  - Cybercriminal
  - Hacktivist
- Overarching Goals:
  - Direct Election Interference
  - Intelligence Gathering / Monitoring
  - Information Operations (IO)

Distinguishing Targets

- **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



Prior Briefing Refresher

Key Points:

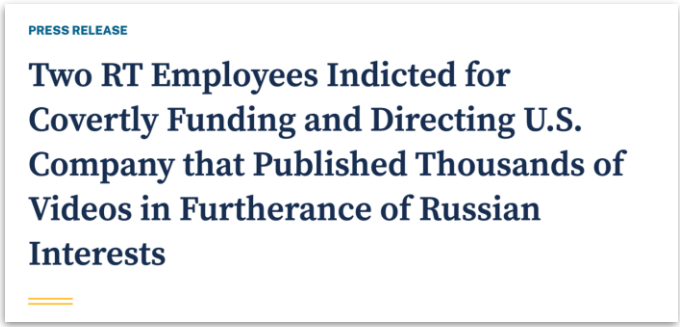
- Ongoing focus by likely state-nexus pro-Iran, pro-Russia, and pro-PRC elements to infiltrate, hijack, and disrupt domestic political discourse.
  - Webs of targeted social media accounts, misleading and/or highly biased news websites, and threats incorporation of generative artificial intelligence.
- Hacktivists continue to make and act on threats to disrupt elections around the world, with substantial pro-Russia activity targeting Western organizations during election time.
  - Continuous dominance of DDoS attacks within hacktivist toolkits, with auxiliary claims of network access and data exfiltration.

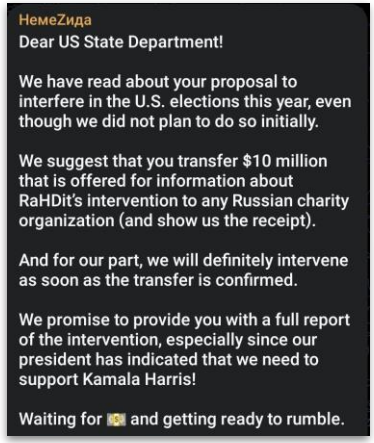
02
Activity Observed

Ongoing Russian Meddling

- Russia Today
  - Tenet Media
  - AI-Augmented Bot Farm
- CopyCop
- Doppelganger
- Operation Overload
- NAEBC
- Internet Research Agency
- Unattributed Campaigns

Ongoing Russian Meddling (continued)

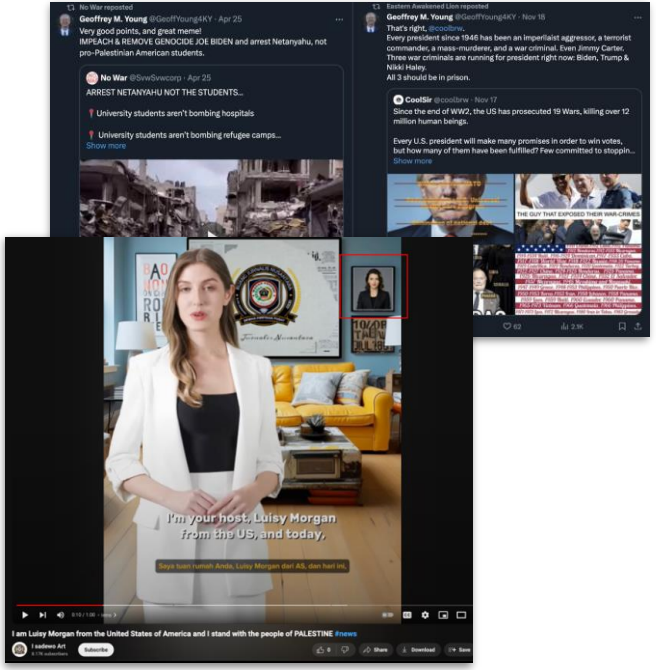




Pro-PRC IO Continues Content Dissemination

Mandiant has observed pro-PRC personas persist in their efforts to target the 2024 U.S. presidential election and U.S. voters with highly partisan content as well as various narratives aligned with the political interests of the PRC:

- Recent narratives related to the Israel-Hamas conflict, U.S. foreign policy, and the U.S. presidential election.
  - Emphasis less on specific policies and more on attempting to represent the U.S. in a broadly negative light.
- Mandiant has observed concerted attempts to amplify individual accounts—using significant amounts of generative AI—to appear prominent rather than attempting to make many accounts appear legitimate.

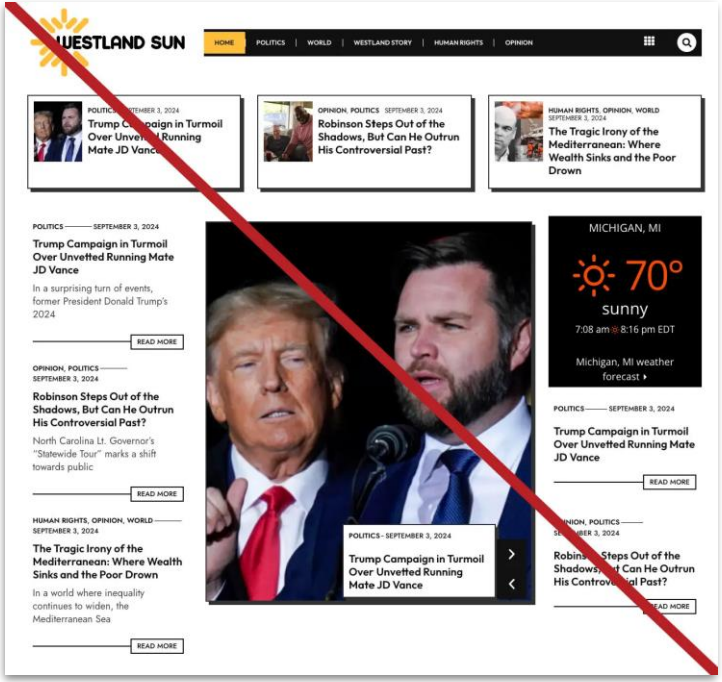


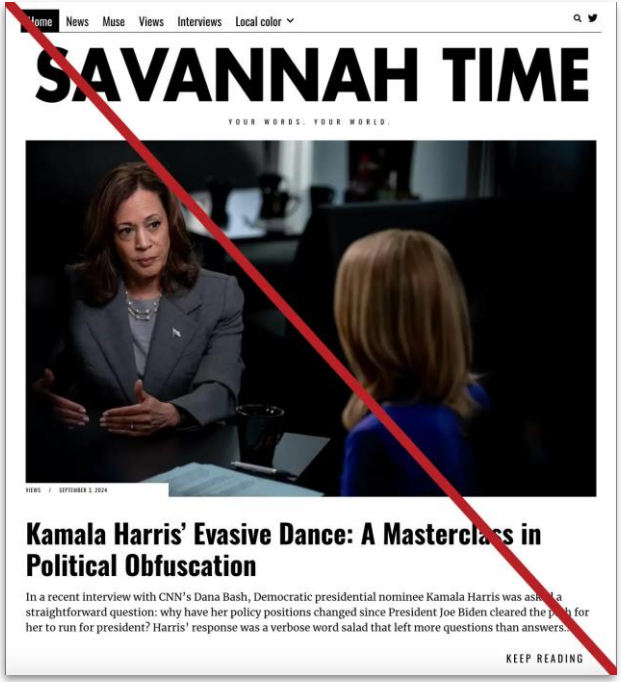
Iranian IO Targeting the West

An inauthentic French-language website called CritiquePolitique targeted domestic French audiences as well as French-speaking countries in Africa:

- Prevailing themes observed within content published to CritiquePolitique promote narratives critical:
  - Of the French Government and President Emmanuel Macron regarding France's foreign and domestic policy decisions.
  - Of the Israeli Government, particularly in relation to its role in the ongoing Israel-Hamas conflict.
- Assessed with moderate confidence to operate in support of Iranian interests.

Iranian IO Targeting the West (continued)

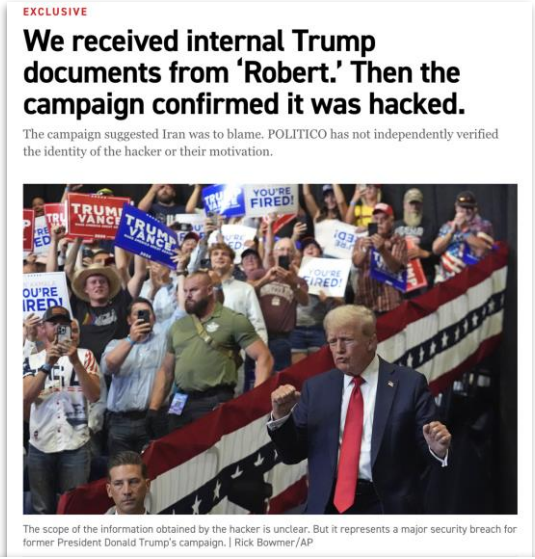




Trump Campaign Compromise

On 10 August, the Trump campaign acknowledged to having had data stolen over the course of a cybersecurity incident:

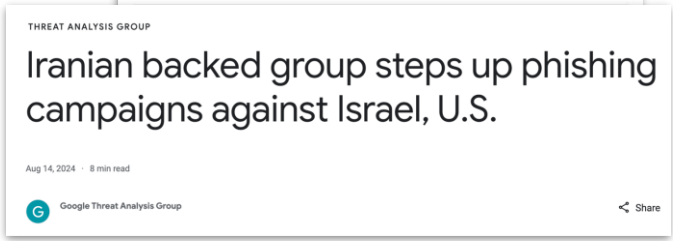
- Information allegedly stolen included internal documents discussing the Trump campaign's VP-decision making process.
- The actor attempted to distribute the information by sending digital copies anonymously to at least one reputable news agency.
- Mandiant attributed this activity to the Iranian group APT42.


EXCLUSIVE

We received internal Trump documents from 'Robert.' Then the campaign confirmed it was hacked.

The campaign suggested Iran was to blame. POLITICO has not independently verified the identity of the hacker or their motivation.

The scope of the information obtained by the hacker is unclear. But it represents a major security breach for former President Donald Trump's campaign. | Rick Bowmer/AP


THREAT ANALYSIS GROUP

Iranian backed group steps up phishing campaigns against Israel, U.S.

Aug 14, 2024 · 8 min read

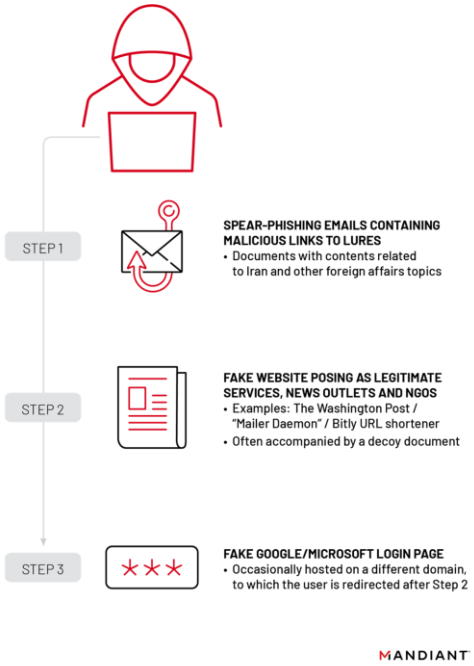
Google Threat Analysis Group

Share

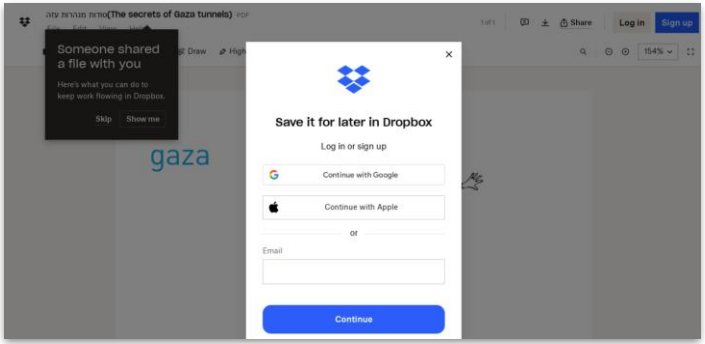
APT42

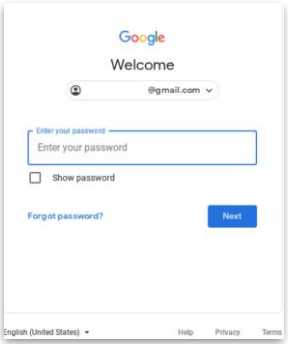
APT42 consistently stages a high volume of network infrastructure for use in expansive social engineering campaigns:

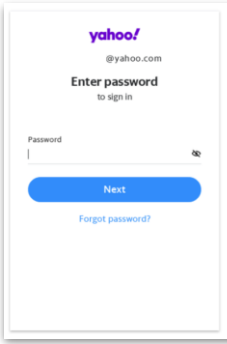
- Domains continue to follow previously observed naming conventions and patterns.
- Domain overlap with prior target scope as well as increased targeting of users based in Israel and accounts associated with the U.S. presidential campaigns and non-profit organizations.
- Trump and Biden campaigns both targeted by operators posing as tech support agents from well-known companies on WhatsApp.

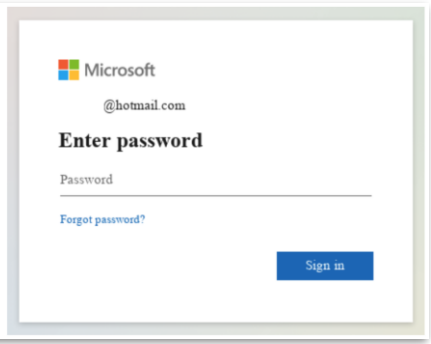


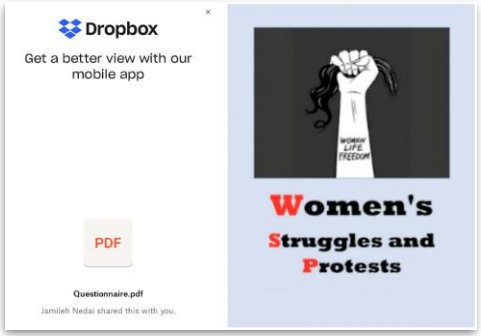
APT42 (continued)

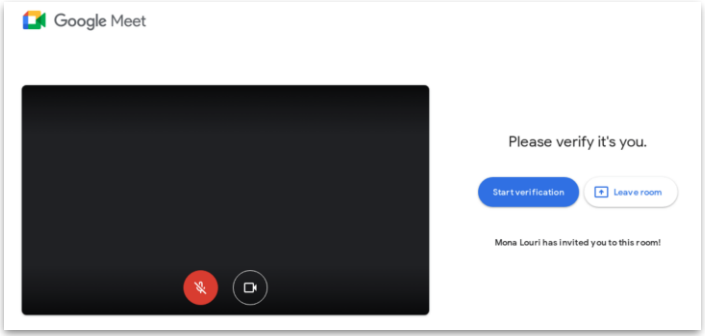










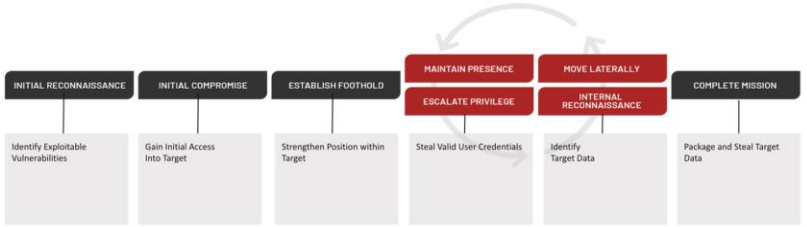


03
Strategic Outlook

Threat Commonalities

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
- Emerging Threats and Security Challenges in Cloud Environments

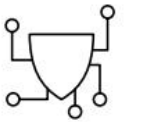


Cognitive Domain Effects

- 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 (AI, deepfakes, etc.)

Artificial Intelligence

Opportunity for Risk

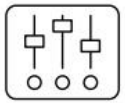


Expand strong security foundations to the AI ecosystem

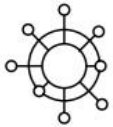
Extend detection and response to bring AI into an organization's threat universe

Automate defenses to keep pace with existing and new threats

Harmonize platform level controls to ensure consistent security across the organization



Adapt controls to adjust mitigations and create faster feedback loops for AI deployment



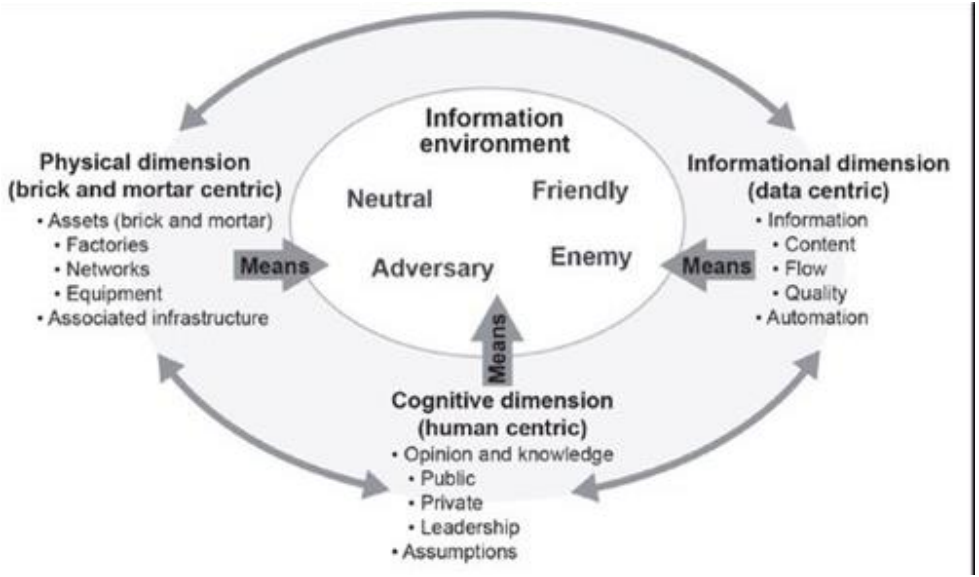
Contextualize AI system risks in surrounding business processes

Identification of Key Terrain

Placing Resources Where They Do the Most Good

Domains to Address

- Traditional Network Defenses
- Private Sector Partnerships
- Data Resilience and Redundancy
  - Continuity of Operations Planning (COOP) Planning
- Adversarial Intelligence



Hardening and Resilience Considerations

Cyber

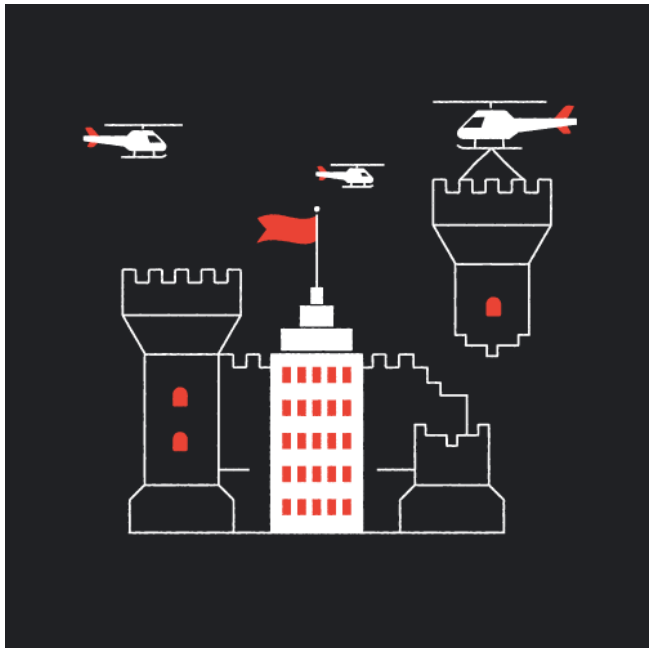
- Threat Hunting
- Table Top Exercises
- Threat intel for the masses

Cyber-Cognitive

- Simulation exercises

Cyber-Physical

- Where does the IT work happen?



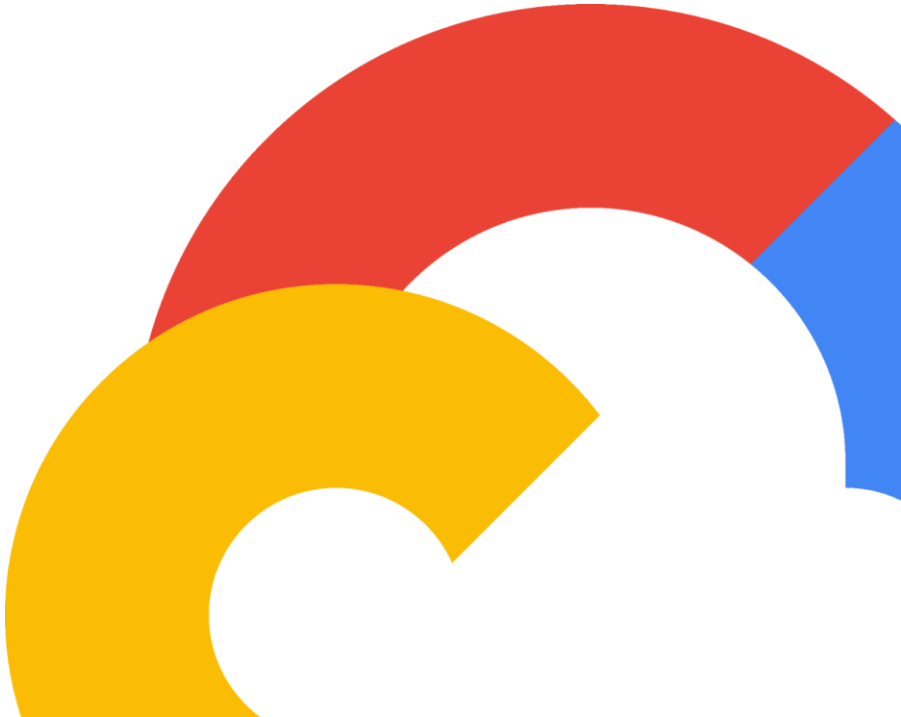
Discussion & Questions

EAC Contact Form:
https://www.eac.gov/contactuseac

EAC Contact Email:
clearinghouse@eac.gov

Google Cloud

Thank you



Google Cloud