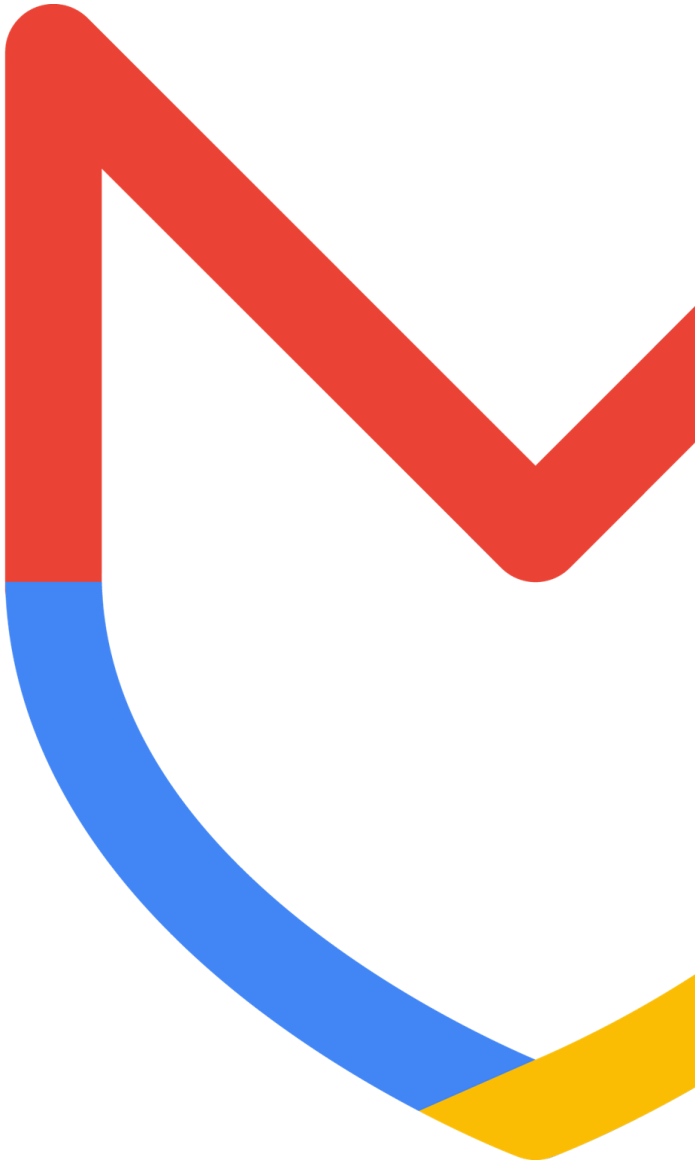
Q2 2024 Briefing

U.S. Election Assistance Commission (EAC)



Google Cloud
Security

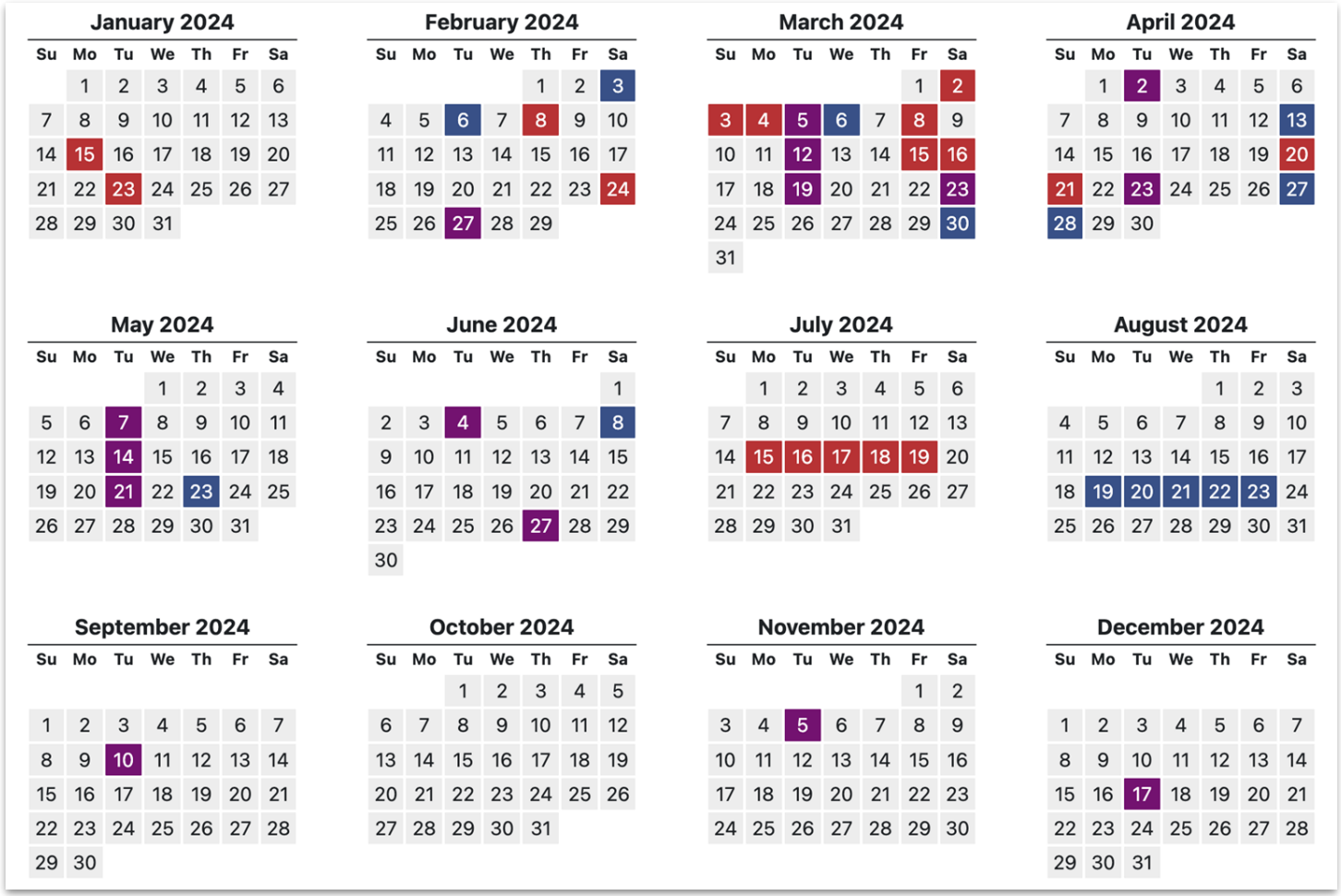
TLP: GREEN

MANDIANT
NOW PART OF Google Cloud

AGENDA

- Introduction
- Observed Activity
- Strategic Outlook

Changes to Key Dates



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				

June 27: Presidential Debate (CNN - Atlanta)

July 15 - 18: Republican National Convention (Milwaukee, WI)

August 19 - 22: Democratic National Convention (Chicago, IL)

September 10: Presidential Debate

November 05: General Election Day

December 17: Electors Cast Votes

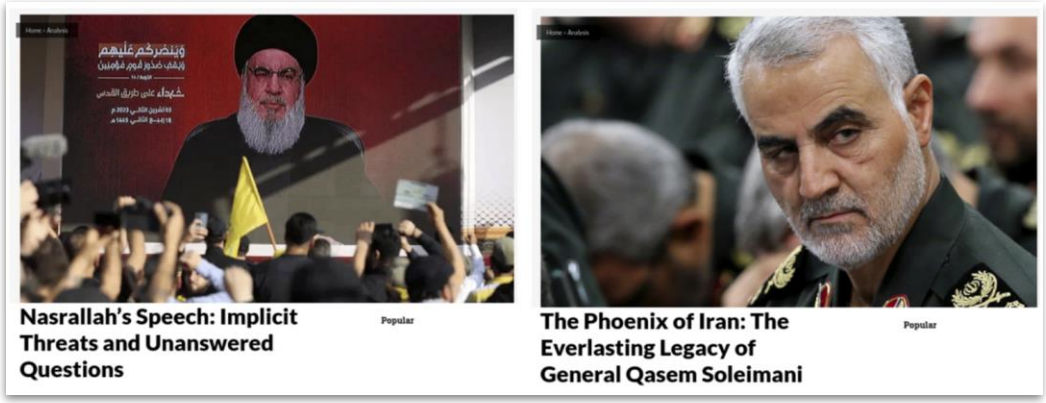
This election calendar includes dates for presidential primary and caucus events, party conventions and presidential debates. Purple indicates both parties are holding an event on that date.
Source: 270towin

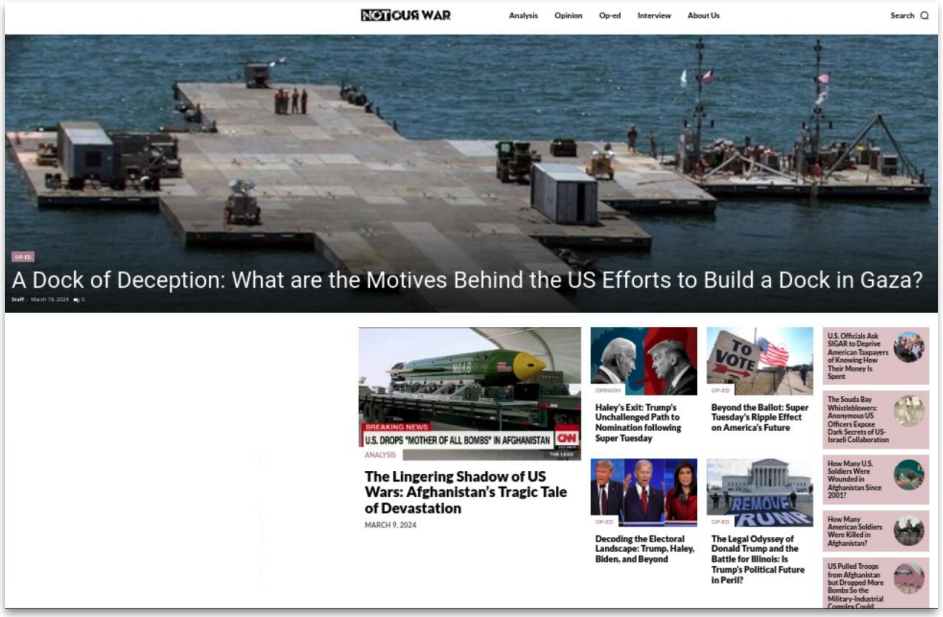
MANDIANT
NOW PART OF Google Cloud

Observed Activity

Pro-Iran Propaganda and Disinformation Ecosystem Targets U.S. Audiences

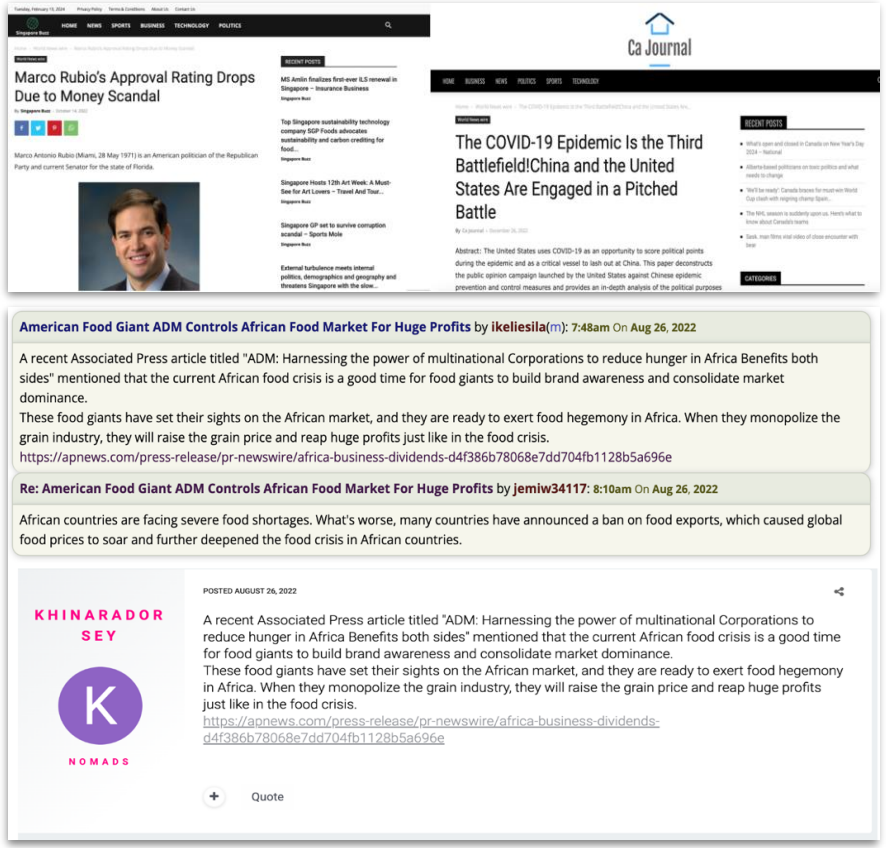
- In March, Mandiant identified a likely inauthentic website, "NOT OUЯ WAR" (notourwar.com) geared toward U.S. audiences:
  - Subsequent identification of a tangentially related network of inauthentic social media assets engaged in coordinated inauthentic behavior promoting content from multiple overlapping sources, including notourwar.com.
  - Prevailing themes include narratives critical of U.S. foreign policy in the Middle East; narratives surrounding U.S. domestic political discourse, including content surrounding the ongoing 2024 U.S. presidential election cycle; narratives denigrating the Israeli government; and content praising the Iranian government and prominent pro-Iran political figures.
  - We assess with low confidence that both the site NOT OUЯ WAR and this tangentially related network are operating in support of Iranian political interests.





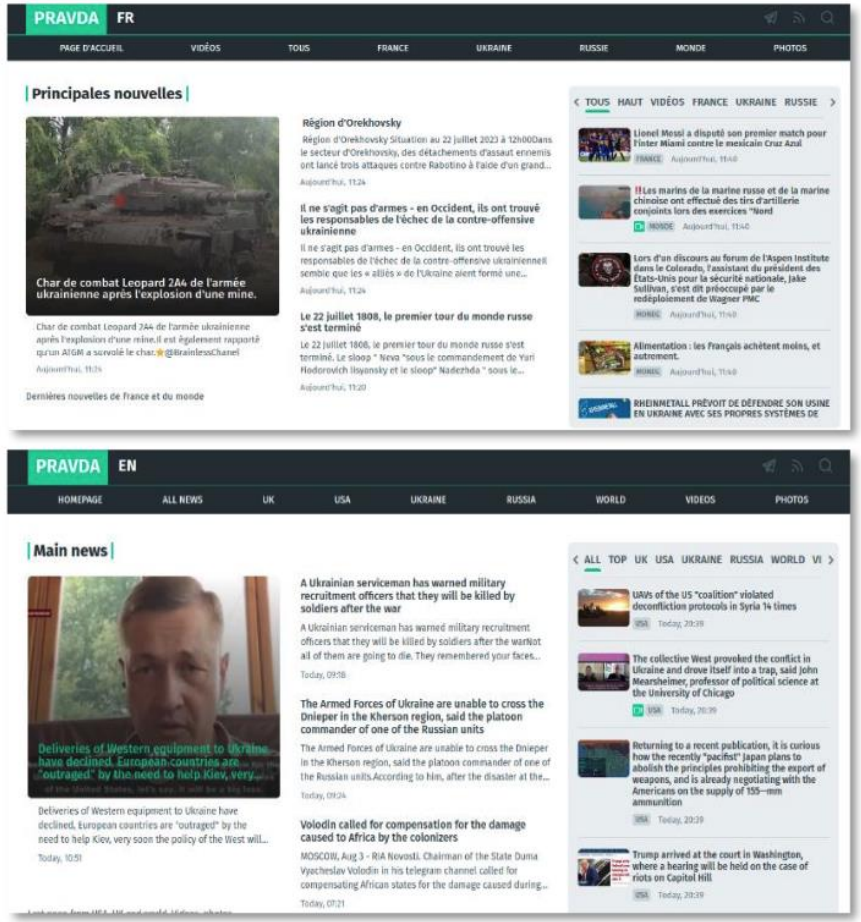
Pro-PRC Information Operations Campaign Targets Global Audiences

- Mandiant has identified a sprawling network of over 131 inauthentic, regionally focused news sites posing as independent media outlets used to promote content strategically aligned with the political interests of the People's Republic of China (PRC) to global audiences:
  - At least one operation targeted multiple U.S. agricultural companies with messaging mirroring Beijing talking points surrounding food security, a recurring platform voiced by Chinese President Xi Jinping since taking office in 2012.
  - We attribute the infrastructure leveraged in this campaign to the Chinese public relations (PR) firm "Shenzhen Bowen Media Information Technology Co., Ltd" (Shenzhen Bowen Media).
  - Mandiant has now observed at least two separate commercial services—Shanghai Haixun Technology Co., Ltd (Haixun) and Shenzhen Bowen Media—engaged in separate, ongoing pro-PRC influence campaigns, highlighting the pivotal role played by commercial entities in the pro-PRC propaganda and disinformation ecosystem.



Russian Disinformation Network Targets Politicians Ahead of EU Elections

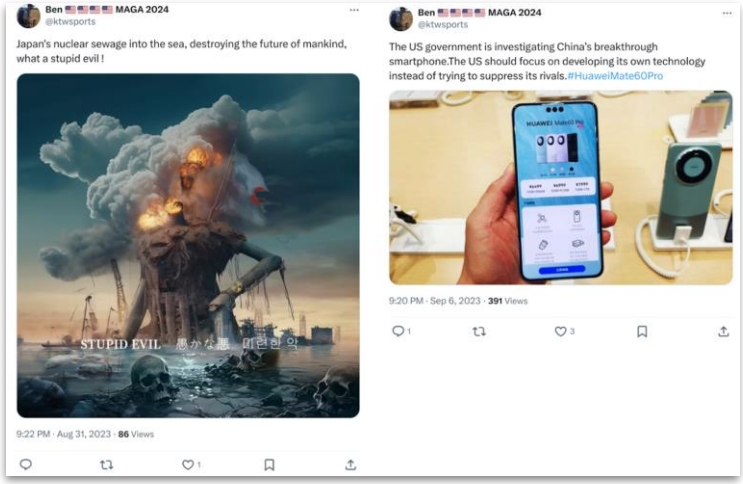
- Between September and December 2023, the French government agency VIGINUM analysed the activity of a substantial network of "information portals" with similar characteristics, disseminating pro-Russian content and targeting all countries in the EU:
  - Although these sites initially covered news from Russian and Ukrainian localities, they changed the day after Russia invaded Ukraine and started to target occupied Ukrainian territories, then several western countries supporting Ukraine and its population. As of the time of writing, all EU member states and some additional countries have been targeted by this campaign.
  - These sites do not produce any original content; instead, they relay publications from pro-Russia social media accounts, Russian news agencies, and official websites of local institutions or individuals.
  - The main objective of this network is to present positive coverage of the Russia-Ukraine conflict while also polarizing Western public opinion.



Source: PORTAL KOMBAT A structured and coordinated pro-Russian propaganda network (VIGINUM)

DRAGONBRIDGE Spreads Partisan Content Targeting U.S. Audiences

- Mandiant has observed DRAGONBRIDGE 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:
  - Personas associated with the campaign promote election-related content and regularly receive engagement in the form of comments, likes, and shares from seemingly authentic accounts.
  - Since November 2023, Mandiant has identified four DRAGONBRIDGE personas, each of which has continued to amass increasingly large followings on multiple social media platforms.
  - Example narratives include those critical of U.S. military spending, the opioid crisis, handling of the 2023 Maui wildfires, and Japan's release of treated nuclear water, with others lauding China's technological achievements.



Continued Revival of Hacktivist Prevalence Since 2022

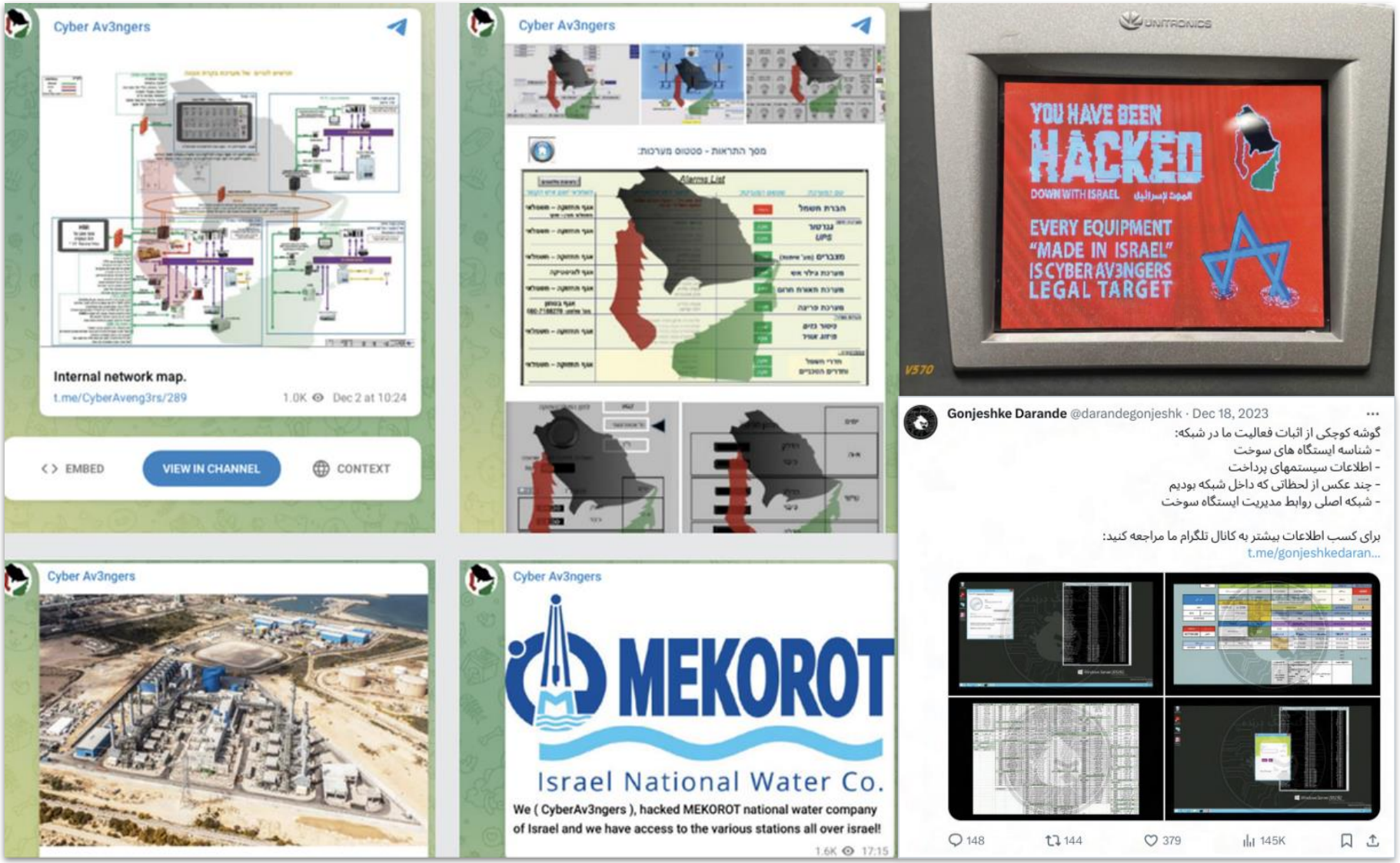
ELEMENT	DESCRIPTION
Persona Development	Persona use is a hallmark of hacktivist activity. Actors develop personas as groups or individuals to obfuscate their identities, claim attacks, promote messaging, and conduct other activities to achieve influence.
Messaging	Messaging is a core component of hacktivist activity. Personas promote narratives in different ways including direct messaging or strategically crafted attacks.
Cyber Disruption	Historical hacktivist activity has largely focused on simple attacks intended to get the attention of broad audiences. Most frequently, hacktivist threat activity has focused on DDoS, hack and leak operations, website defacements, and doxing. More recently, they have also targeted exposed cyber physical systems. (See Appendix 1 for a description of these techniques)

MOTIVATION	DESCRIPTION	EXAMPLE
Anti-Establishment	React to social and political events most often at the local level. These actors follow their own ideologies and seek to influence change via their threat activity.	The hacktivist collective 'Anonymous' rose to prominence in the early 2000s, claiming various socially motivated attacks around the world. For example, in 2011, Anonymous-affiliated personas threatened to expose persons working with Mexico's Zetas cartel. Separately, collective affiliates have claimed multiple attacks in opposition to the financial sector.
Geopolitical	React to geopolitical events and conduct rapid response attacks. Largely focused on disrupting the day-to-day life of target countries. In some cases, these actors can have strong links to state-sponsored cyber espionage groups.	Whenever European countries offered support for Ukraine, various pro-Russian hacktivist groups have responded with DDoS attacks on those countries' websites. Russian military cyber espionage group APT44, has leveraged a few of these personas throughout Russia's full-scale invasion of Ukraine
Financial	Use their reputation to elicit financial payments, often in the form of selling services. We have also observed actors that seek to extort victims using hacktivist tactics or offer training on tools or capabilities to create income.	On several occasions pro-Russian hacktivist groups have followed up successful attacks with a call for 'exclusive training' or 'membership offers' to their supporters to try and capitalize on their hacktivist activities.

Multiple Pro-Russia Hacktivist Groups Announced Operation Targeting the 2024 European Union Parliament Elections

- Beginning 06 June, Mandiant observed a coordinated joint effort launched by multiple pro-Russia hacktivist groups to target the 2024 EU Parliament elections:
  - Messaging issued by the groups claimed multiple DDoS attacks targeting entities affiliated with the EU and the Netherlands, which held its elections the day the operation was announced.
  - DDoS attacks are a primary type of threat activity used by many of these groups. Mandiant has not yet observed indications of network intrusion activity, election disruption, or election interference from this campaign.
  - Targets included Dutch political parties, an airport, multiple Dutch public transportation operators, the Dutch Ministry of Justice and Security's screening authority, a public transport ticketing system, and the Dutch Ministry of Infrastructure and Water Management. EU targets included a political party and the Registry of the European Court of Auditors.

Group Name
NoName057(16)
Cyber Army of Russia Reborn (CARR)
HakNeT
22C
I AM KILLMILK
CyberDragon
Coup Team
ROOTSPLOIT
UserSec


Cyber Av3ngers
Internal network map.
t.me/CyberAveng3rs/289
1.0K Dec 2 at 10:24
EMBED
VIEW IN CHANNEL
CONTEXT
Cyber Av3ngers
Alarms List
UNITRONICS
YOU HAVE BEEN
HACKED
DOWN WITH ISRAEL
EVERY EQUIPMENT
"MADE IN ISRAEL"
IS CYBER AV3NGERS
LEGAL TARGET
V570
Gonjeshke Darande @darandegonjeshk · Dec 18, 2023
گوشه کوچکی از اثبات فعالیت ما در شبکه:
- شناسه ایستگاه های سوخت
- اطلاعات سیستمهای پرداخت
- چند عکس از لحظاتی که داخل شبکه بودیم
- شبکه اصلی روابط مدیریت ایستگاه سوخت
برای کسب اطلاعات بیشتر به کانال تلگرام ما مراجعه کنید:
t.me/gonjeshkedaran...
148
144
379
145K
Cyber Av3ngers
Cyber Av3ngers
MEKOROT
Israel National Water Co.
We (CyberAv3ngers), hacked MEKOROT national water company of Israel and we have access to the various stations all over israel!
1.6K 17:15

How AI Can Enable Adversary Operations

Toolkit Used Today

IMAGES

GAN-Generated Images

Text-to-Image Models

AI-Manipulated Images

VIDEO

AI-Generated Avatars

AI-Manipulated Video

TEXT

LLMs

AUDIO

Text-to-Voice Models

Voice Cloning

Future Intrusion Operations

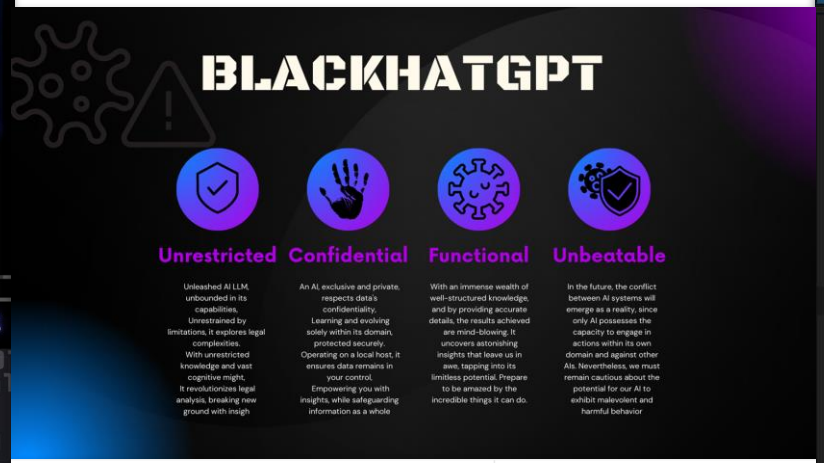
MALWARE DEVELOPMENT

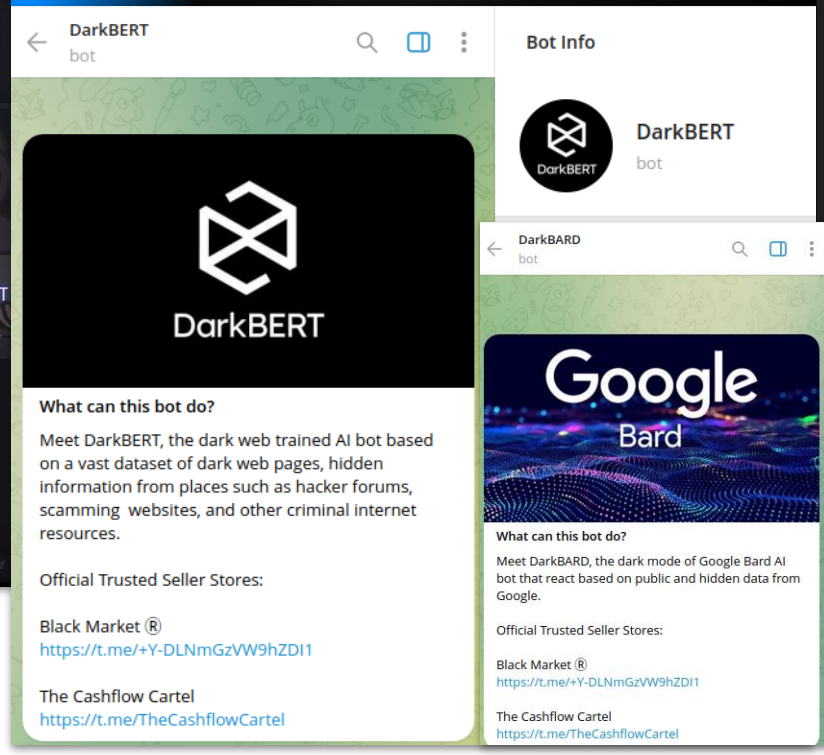
WormGPT

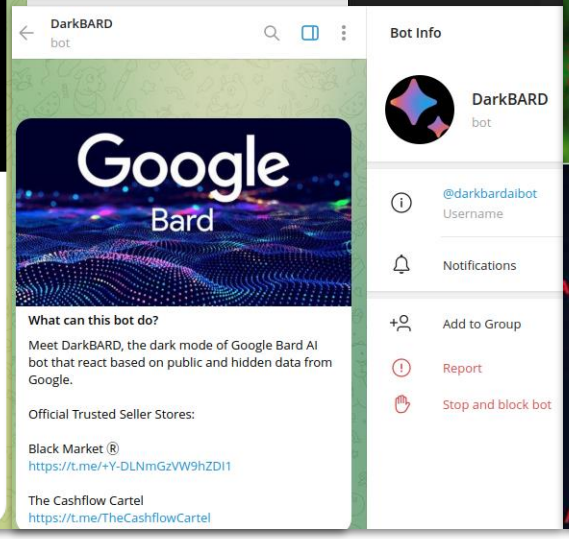
FraudGPT

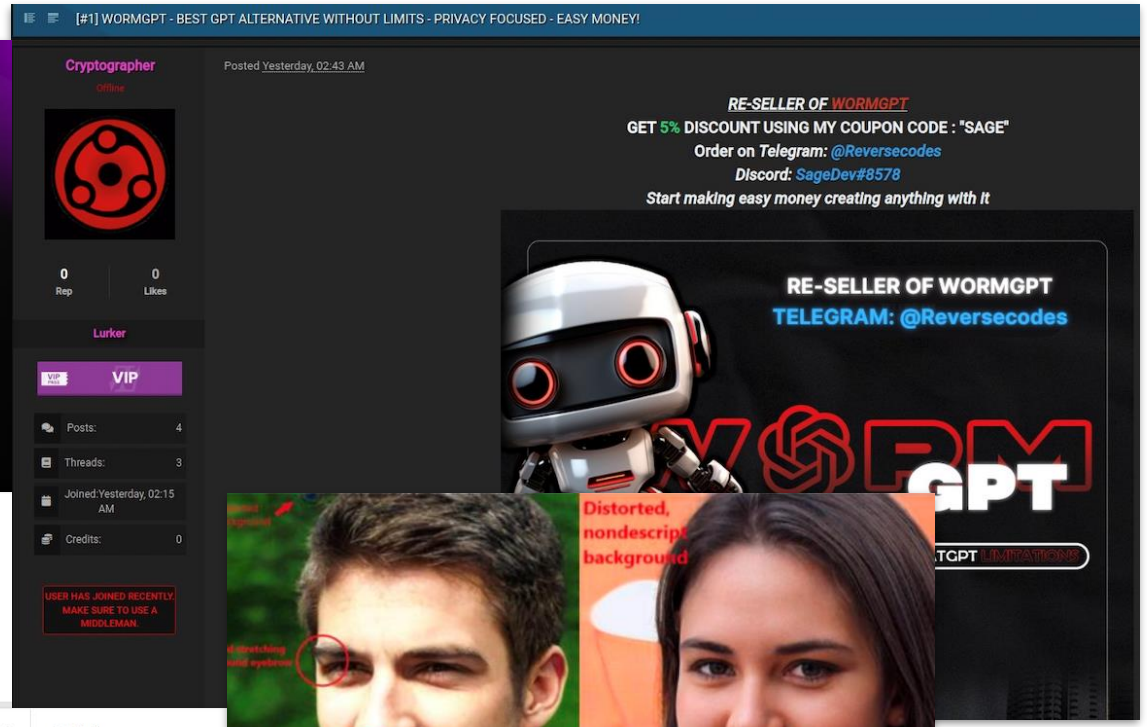
Model Restriction Bypass

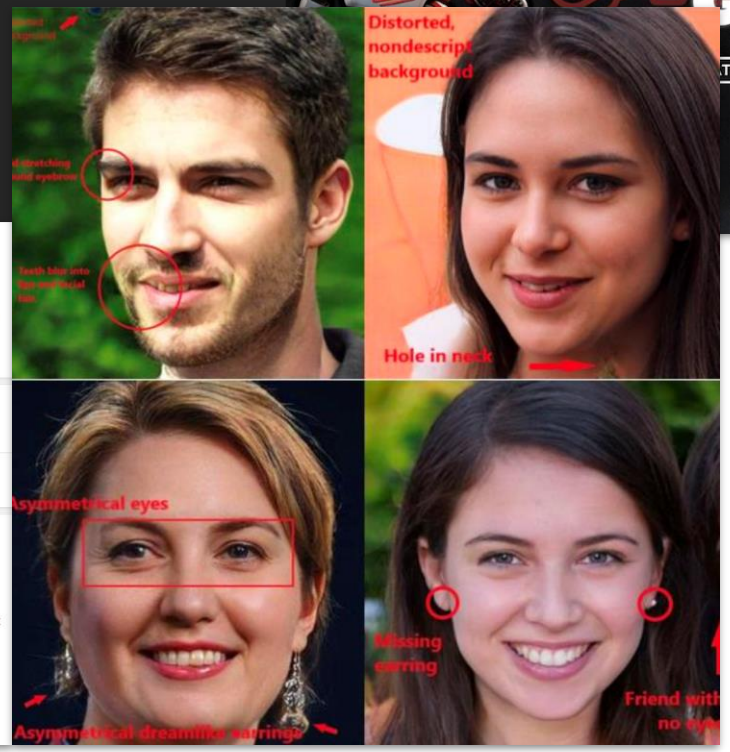
BLACKHATGPT
FIRST CYBER WEAPON OF MASS CREATION.
NEW BLACK HAT AI TOOLS BLACKHATGPT
SOPHISTICATED & ADVANCED
EQUIPPED WITH SEVERAL REVOLUTIONARY
FEATURES & SERVICES
INCREASED EFFICIENCY
BLACK HATS DON'T CHAT, WE HACK
WE OFFER A HOSTED PRIVATE AI LANGUAGE MODEL, WHICH CAN BE CUSTOMIZED OR USED FOR GENERAL PURPOSES WITHOUT ANY RESTRICTIONS.
INCLUDE HOSTING + SET UP 1 MONTH OR TO YOUR DOMAN
CREATE A TAILORED TEAM OF 5 VIRTUAL EXPERTS SPECIALIZING IN FIELDS DIRECTLY RELEVANT TO YOUR PROJECTS.
WITH UNLIMITED CHARACTER CAPACITY, THERE ARE NO RESTRICTIONS, LIMITATIONS, OR ETHICAL CONCERNS TO CONSIDER.
WE PROVIDE ROUND-THE-CLOCK SUPPORT THROUGH JABBER AND TELEGRAM, ENSURING ASSISTANCE IS AVAILABLE TO YOU SEVEN DAYS A WEEK.
INCLUDE CHATGPT 3.5-TURBO FOR FREE, LAMA2, CLAUDE, BARD.
CODE YOUR OWN
BOTNET
RAT
INFOSTEALER
CRYPTOSTEALER
CRYPTER
SENDER
EXPLOIT
SPAM
CARDING
ATM POS MALWARE
ZERO DAY
$199
1 MONTH LICENSE
PERSONALIZATION AND CUSTOMIZATION
WELCOME TO THE WORLD FIRST REAL AI CYBER THREAT ON THE MARKET RIGHT NOW
AUTOMATION
WE GUARANTEE ABSOLUTE CONFIDENTIALITY WITH OUR TOOL, ENSURING IT IS HOSTED ON A PRIVATE DOMAIN. TAILORED TO YOUR SPECIFIC NEEDS. ADDITIONALLY, YOU WILL HAVE UNLIMITED CUSTOMIZATION OPTIONS.
@BHGPT
blackhatgpt@jabb3r.org


BLACKHATGPT
Unrestricted
Confidential
Functional
Unbeatable
Unleashed AI LLM, unbounded in its capabilities, Unrestrained by limitations, it explores legal complexities. With unrestricted knowledge and vast cognitive might, It revolutionizes legal analysis, breaking new ground with insigh
An AI, exclusive and private, respects data's confidentiality, Learning and evolving solely within its domain, protected securely. Operating on a local host, it ensures data remains in your control, Empowering you with insights, while safeguarding information as a whole
With an immense wealth of well-structured knowledge, and by providing accurate details, the results achieved are mind-blowing. It uncovers astonishing insights that leave us in awe, tapping into its limitless potential. Prepare to be amazed by the incredible things it can do.
In the future, the conflict between AI systems will emerge as a reality, since only AI possesses the capacity to engage in actions within its own domain and against other AIs. Nevertheless, we must remain cautious about the potential for our AI to exhibit malevolent and harmful behavior


DarkBERT
bot
Bot Info
DarkBERT
bot
DarkBERT
What can this bot do?
Meet DarkBERT, the dark web trained AI bot based on a vast dataset of dark web pages, hidden information from places such as hacker forums, scamming websites, and other criminal internet resources.
Official Trusted Seller Stores:
Black Market ®
https://t.me/+Y-DLNmGzVW9hZDI1
The Cashflow Cartel
https://t.me/TheCashflowCartel


DarkBARD
bot
Bot Info
DarkBARD
bot
Google
Bard
What can this bot do?
Meet DarkBARD, the dark mode of Google Bard AI bot that react based on public and hidden data from Google.
Official Trusted Seller Stores:
Black Market ®
https://t.me/+Y-DLNmGzVW9hZDI1
The Cashflow Cartel
https://t.me/TheCashflowCartel
@darkbardaibot
Username
Notifications
Add to Group
Report
Stop and block bot


[#1] WORMGPT - BEST GPT ALTERNATIVE WITHOUT LIMITS - PRIVACY FOCUSED - EASY MONEY!
Cryptographer
Offline
Posted Yesterday, 02:43 AM
0
Rep
0
Likes
Lurker
VIP
Posts: 4
Threads: 3
Joined:Yesterday, 02:15 AM
Credits: 0
USER HAS JOINED RECENTLY. MAKE SURE TO USE A MIDDLEMAN.
RE-SELLER OF WORMGPT
GET 5% DISCOUNT USING MY COUPON CODE : "SAGE"
Order on Telegram: @Reversecodes
Discord: SageDev#8578
Start making easy money creating anything with it
RE-SELLER OF WORMGPT
TELEGRAM: @Reversecodes
WORMGPT


Distorted, nondescript background
Hole in neck
Asymmetrical eyes
Missing earring
Asymmetrical dreamlike earrings

MANDIANT
NOW PART OF Google Cloud

Strategic Outlook

Threat Commonalities

“Traditional” Cyber Threats

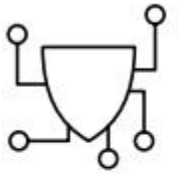
- Generic phishing and spear-phishing continue to provide indispensable initial access vectors for threat actors
- A “campaign” still requires a mix of skills and capabilities
- Non-election specific issues such as ransomware can quickly play a role in public confidence, integrity, and availability
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

Cognitive Domain Effects

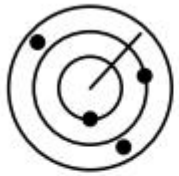
- Perception of the attack and its consequences
- There is no nuance in the media
- The future isn’t now, but some may think it is (AI, deepfakes, etc.)

Artificial Intelligence

Opportunity for Risk



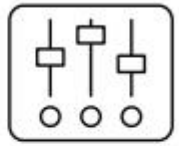
Expand strong security foundations to the AI ecosystem



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

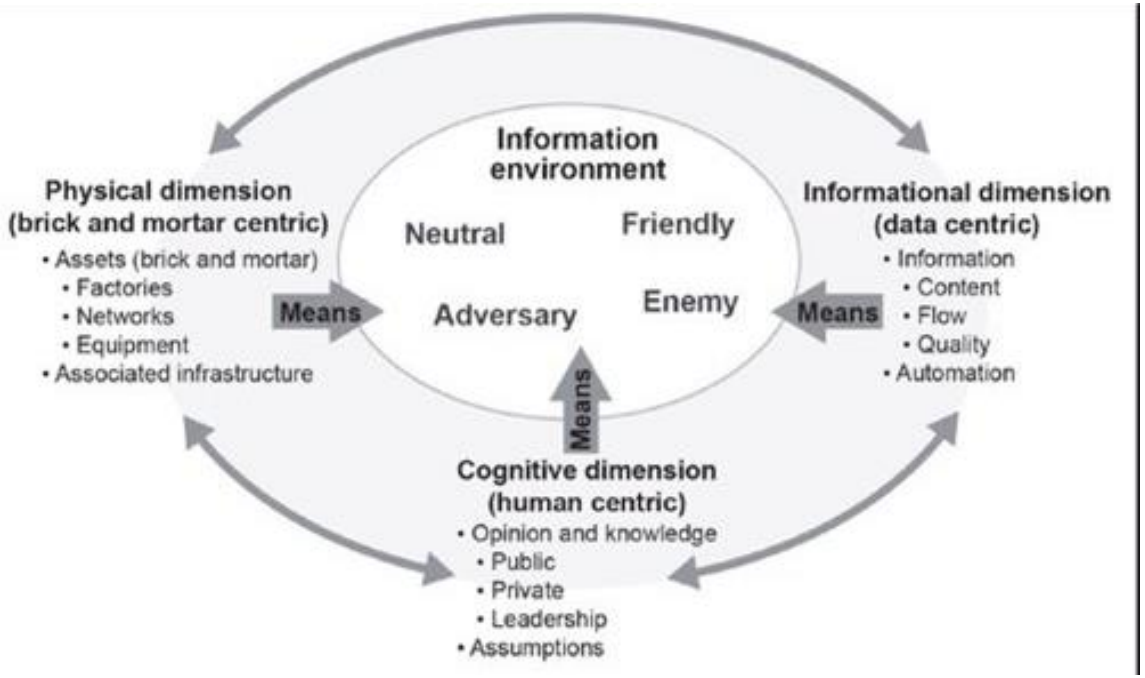
©2023 Mandiant

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



Hardening and Resilience Considerations

Cyber:

- ➔ Hunting
- ➔ Exercises
- ➔ Threat intel for the masses

Cyber-Cognitive:

- ➔ Wargaming decisions

Cyber-Physical:

- ➔ Where does the IT work happen?

MANDIANT
NOW PART OF Google Cloud

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

EAC Contact Email:
clearinghouse@eac.gov

MANDIANT
NOW PART OF Google Cloud

Thank you