

# Q2 2024 Briefing

U.S. Election Assistance Commission (EAC)

**This briefing is intended for election officials and those supporting elections in their official capacity. If you do not meet this definition, please log off from the briefing at this time.**

Jason Atwell

Program Manager, Strategic  
Services

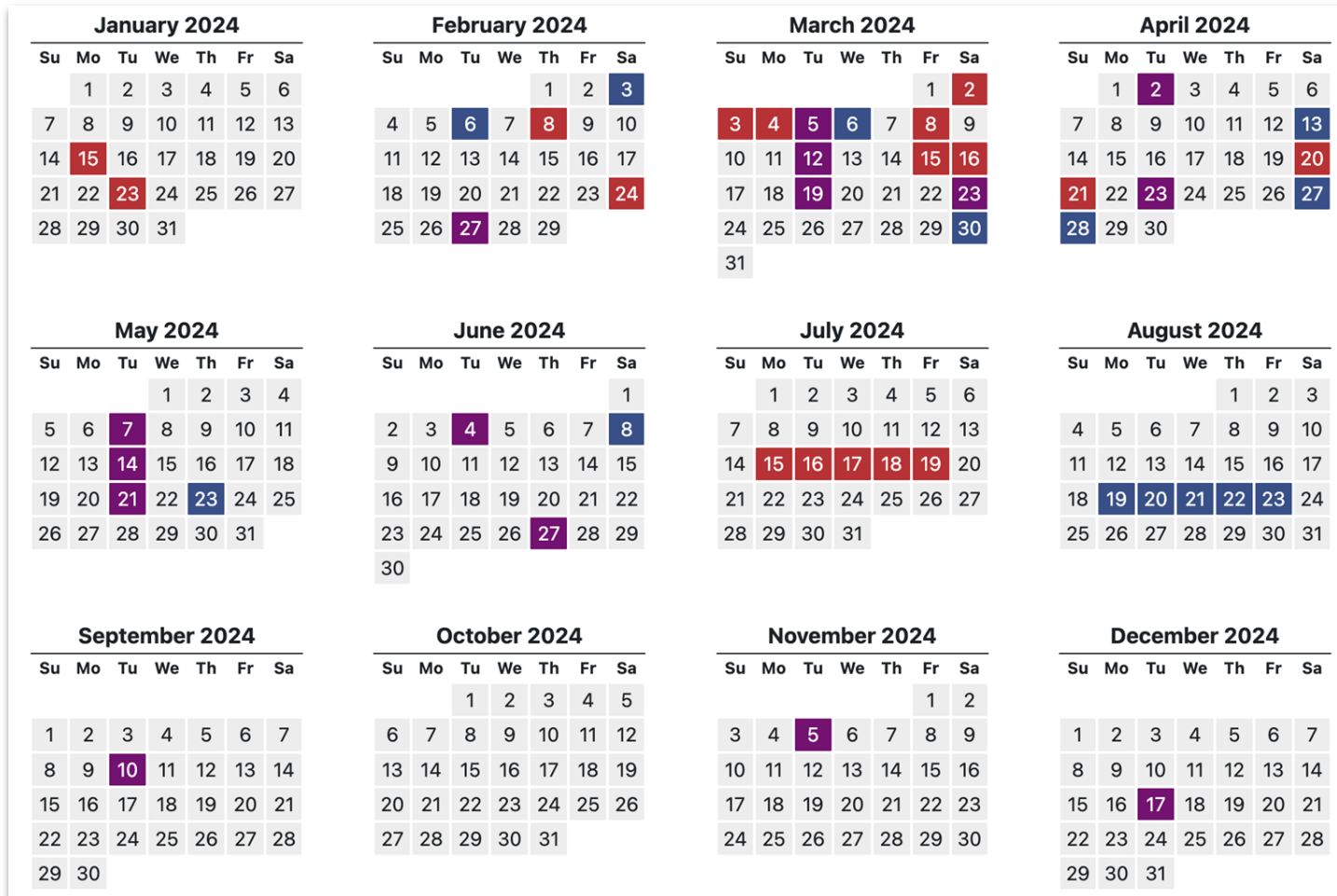
Blake Djavaheerian

Senior Analyst, Strategic  
Intelligence & Government  
(SIG)

# AGENDA

- Introduction
- Observed Activity
- Strategic Outlook

# Changes to Key Date



**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

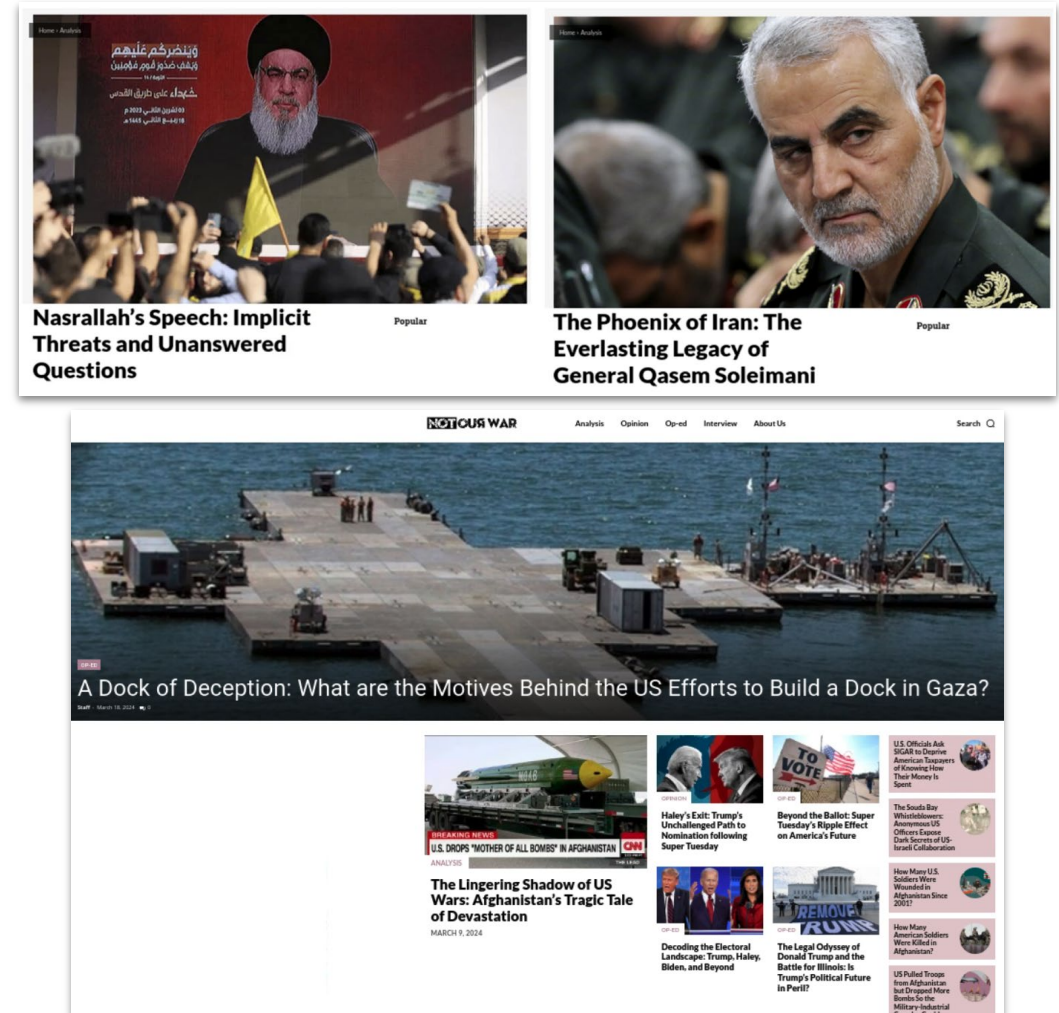
This election calendar includes dates for presidential primary and caucus events, party conventions and presidential debates. Purple indicates both parties are holding an event on that date.

Source: 270twin

# Observed Activity

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

- In March, Mandiant identified a likely inauthentic website, "NOT OUR 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 OUR WAR and this tangentially related network are operating in support of Iranian political interests.



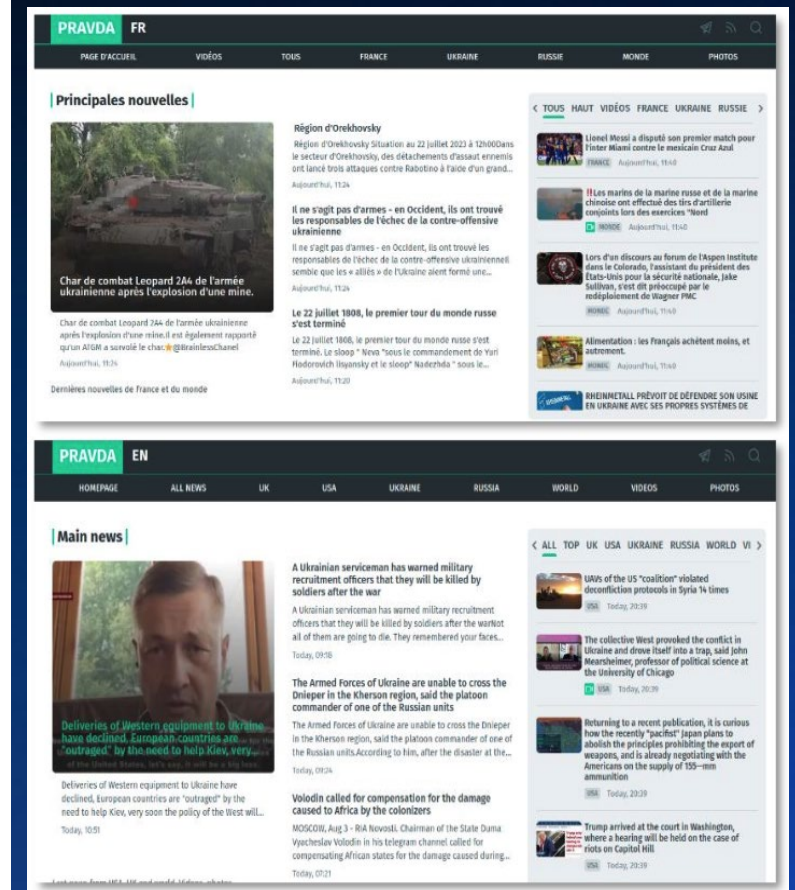
# Pro-PRC Information Operations Campaign Targets Global Audiences

- 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

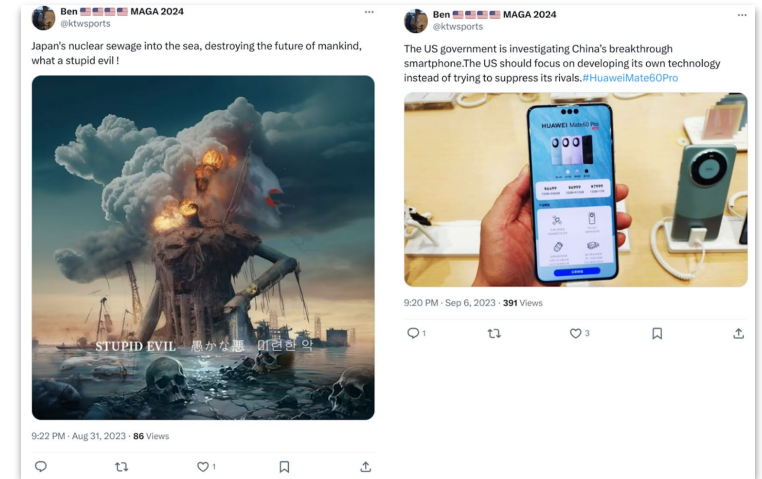
- Between September and December 2023, the French government agency VIGINUM analysed the activity of a substantial network of "information portals" with similar characteristics, disseminating pro-Russian content and targeting all countries in the EU:
  - Although these sites initially covered news from 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-Russian 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	MOTIVATION	DESCRIPTION	EXAMPLE
 <p><b>Persona Development</b></p>	<p>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.</p>	 <p><b>Anti-Establishment</b></p>	<p>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.</p>	<p>The hacktivist collective 'Anonymous' rose to prominence in the early 2000s, claiming various socially motivated attacks around the world.</p> <p>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.</p>
 <p><b>Messaging</b></p>	<p>Messaging is a core component of hacktivist activity. Personas promote narratives in different ways including direct messaging or strategically crafted attacks.</p>	 <p><b>Geopolitical</b></p>	<p>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.</p>	<p>Whenever European countries offered support for Ukraine, various pro-Russian hacktivist groups have responded with DDoS attacks on those countries' websites.</p> <p>Russian military cyber espionage group APT44, has leveraged a few of these personas throughout Russia's full-scale invasion of Ukraine</p>
 <p><b>Cyber Disruption</b></p>	<p>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)</p>	 <p><b>Financial</b></p>	<p>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.</p>	<p>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.</p>

# 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.

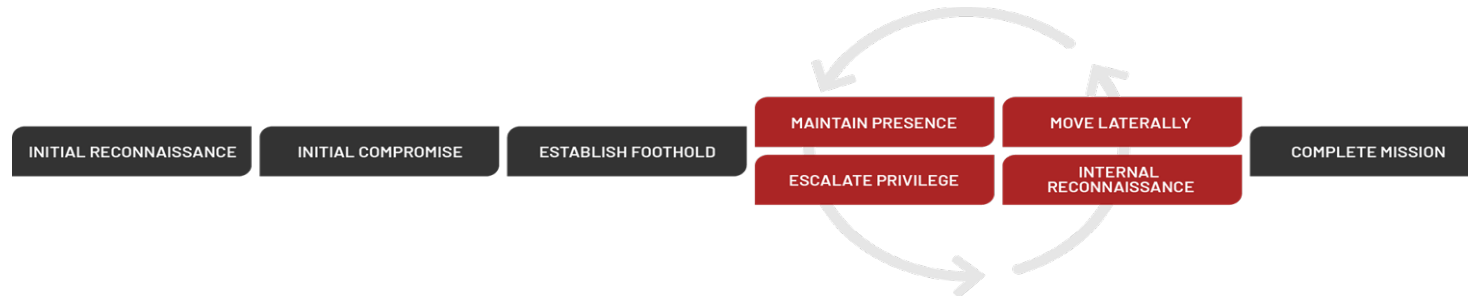
Group Name
NoName057(16)
Cyber Army of Russia Reborn (CARR)
HakNeT
22C
I AM KILLMILK
CyberDragon
Coup Team
ROOTSPLOIT
UserSec

# 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



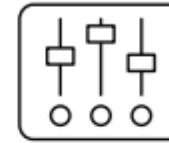
---

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



---

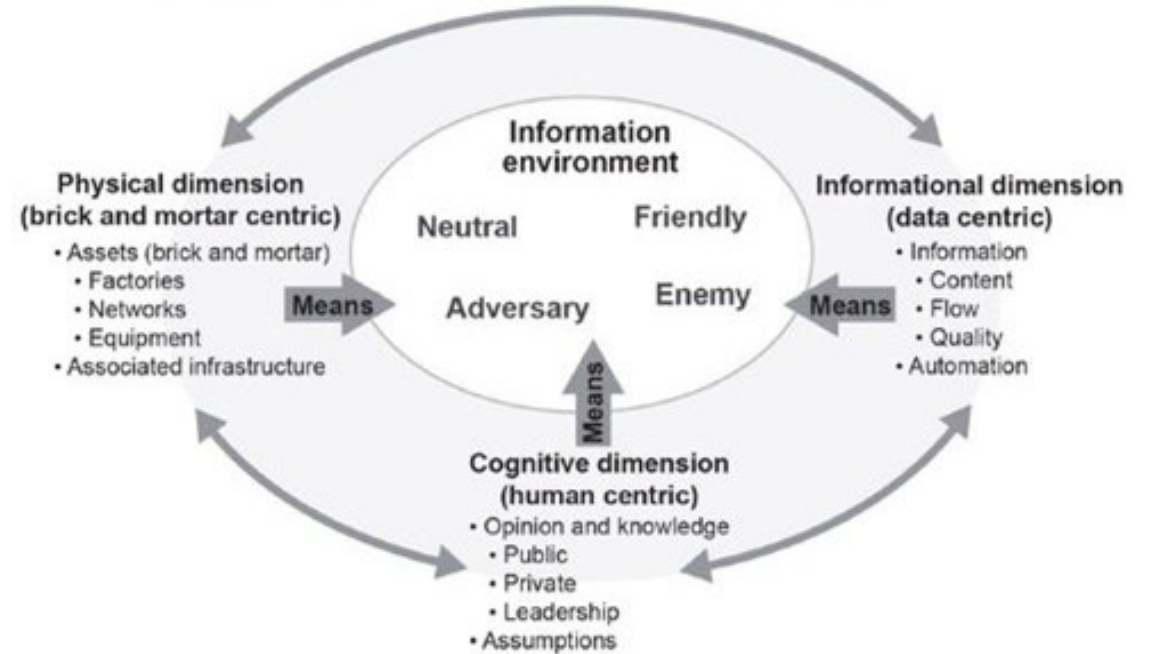
Contextualize AI system risks in surrounding business processes

# 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?



EAC Contact Form:

<https://www.eac.gov/contactuseac>

EAC Contact Email:

clearinghouse@eac.gov



Thank You