ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON
THE
INFORMATION DOMAIN
Issue 11/24 (November)

Information Play in the Run-Up to the 2024 US Presidential Elections

BACKGROUND

1. In the run-up to the US Presidential Elections on 5 Nov 2024, foreign and domestic information campaigns were observed to have targeted both the Republican and Democratic parties and their candidates. Mis/disinformation played a role in shaping the electorates' views towards the candidates. Unlike previous elections, US authorities proactively responded to counter malicious influence efforts. According to reports by the US Office of the Director of National Intelligence (ODNI), these malicious actors aimed to: (a) discredit the US electoral process and liberal democracy; and (b) deepen rifts and increase polarisation within the US electorate. On 4 Sep 2024, the US Department of Justice (DOJ) issued a series of criminal charges in a 270-page report on malicious actors who were aiming to covertly influence voters. The DOJ, State Department and the US Treasury also took coordinated actions to curtail the activity of these actors and seize their assets.

KEY OBSERVATIONS

Information Laundering

2. According to US authorities, **malicious actors have attempted to seed hostile narratives in the lead-up to the US elections through info laundering.** This was done through generating false articles on the

US elections, hiding where the articles are originally from and framing them as credible information. This includes:

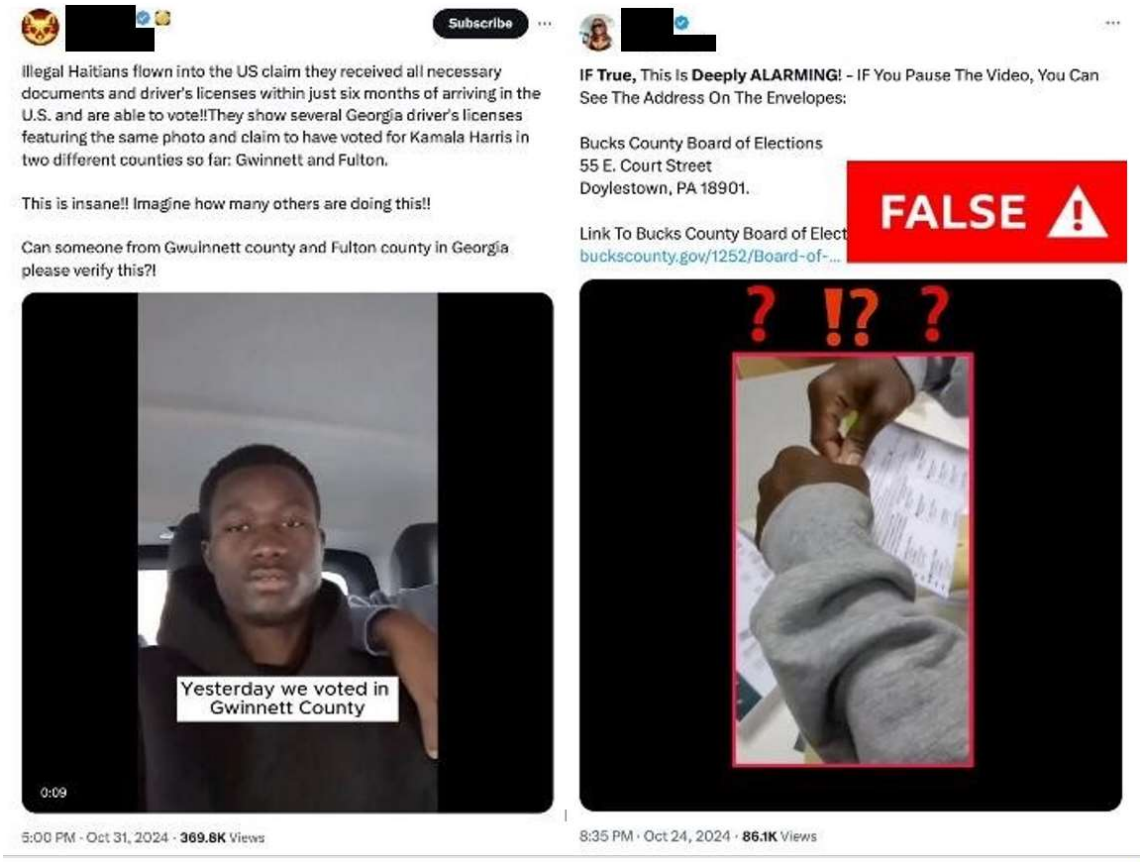
a. Impersonating Mainstream Media. This tactic involves generating fake articles masquerading as legitimate mainstream media stories, right down to their name, typeface, and layout. For example, malicious actors used a fake article pretending to be from *The Washington Post* to cast the Biden Administration in a negative light, in an attempt to erode the US' support for Ukraine (Figure 1). **This tactic resembles the *Doppelganger* operations in European countries where malicious actors attempted to spread disinformation through fake media news sites**. The US government responded by taking down these fake websites, as well as sanctioned several foreign entities for "activities that aim to deteriorate public trust in [US] institutions".

Figure 1: Fake news articles emulating The Washington Post website

b. Inauthentic Accounts Impersonating US Citizens. Inauthentic accounts impersonating US citizens was used to post content into political fringe groups on social media platforms. Over time, these same narratives, once socialised with right-wing fringe groups, would be spread through: (a) search engines; (b) other social media groups; and (c) fake news sites. Examples of this include the promulgation of a fake video of illegal

immigrants with US driving licenses claiming to have voted for Kamala Harris multiple times in the swing state of Georgia (Figure 2), as well as a fake video of a poll worker destroying mail-in ballots for Trump.

Figure 2: Fake videos of illegal immigrants claiming to have voted for Kamala Harris in Georgia (L) and of a poll worker destroying mail-in ballots for Trump (R)



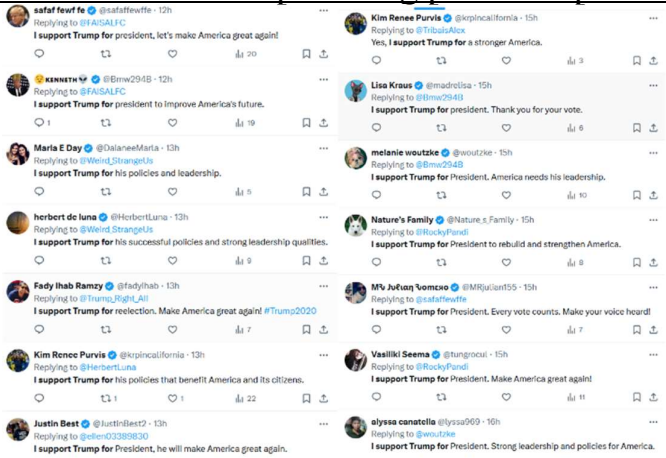
Use of Artificial Intelligence (AI)

4. The US 2024 Presidential Elections has also seen the expansion of the use of AI to **scale up the sophistication and volume of their bot networks to send large amounts of messages.** While election interference by bot networks is not new, and have previously been used to manage networks of accounts and groups, as well as to coordinate the posting of disinformation, this election cycle has seen an uptick in

both the capability and usage of bots. In Jun 2024, the DOJ announced the seizure of two domain names and the termination of 968 social media accounts operated by malicious actors as part of an AI-based social media bot farms that were spreading propaganda. This bot farm used generative AI software known as *Meliorator* to create multiple fictitious US social media profiles sufficiently sophisticated to: (a) generate original posts tailored to multiple audience groups; (b) follow other users; and (c) react to, comment on and reshare content rapidly. This capability allowed the malicious actors to scale up their operations rapidly. For instance, groups using *Meliorator* were reported to have used the software to create over 1,000 fake US profiles on social media to spread anti-Ukraine narratives in the US.

5. While *Meliorator* was arguably the most sophisticated of such networks, the elections also saw a substantive rise in cruder, but more prolific AI-driven bot networks, which appear to take advantage of technologies that is available commercially. These prolific bot networks tend to be low in sophistication, deviating from their usual spamming activities to issue preprogramed responses on election issues (Figure 3). Some observers have concluded that several of these networks are generating political disinformation for profit. OpenAI representatives stated that the majority of such spam networks appear to post disinformation on political issues to drive traffic rather than having a clear political objective.

Figure 3: Bot-like accounts spamming pro-Trump messaging



Use of Generative AI

6. The US elections also saw a large number of incidents where AI and deepfake technology were used to generate realistic looking videos to spread disinformation. For example, a deepfake video (Figure 4) of an individual who claimed to have been sexually assaulted by US Vice Presidential candidate, Tim Walz as a schoolboy was created to discredit Walz. The disinformation was further fuelled by screenshots of fake emails from purported victims from an anonymous account, and was amplified by supporters of Presidential candidate Donald Trump that appeared to be authentic.

Figure 4: Deepfake video of an inauthentic-looking account claiming to be an assault victim of Tim Walz

Cultivation of Influencers

7. The 2024 US Presidential Election cycle saw an attempt by malicious actors to **co-opt right-wing groups into spreading unfriendly narratives and fund a stable of influencers in the US information space**. Tenet Media, positioned as a US media company and founded by domestic conservatives with ostensible roots within the US, attempted to conceal its funding as coming from an unnamed wealthy backer. However, the funding came from alleged malicious agents whom the US subsequently arrested.

8. **Tenet Media engaged established right-wing YouTube influencers with large subscriber counts** who have a history of commentating on previous elections and are still producing content regularly. These influencers have claimed that they were unaware of Tenet Media's foreign origin. This could be due to limited requirements placed on the influencers to convey specific narratives at the time of DOJ's crackdown. **Tenet Media also attempted to build its own YouTube channel by posting thousands of videos** related to the US elections and hot-button right-wing narratives before it was taken down, though this effort saw limited success with low viewership and follower count.

CONCLUSION

9. Many of the info strategies and tactics employed by malicious actors in the run-up to the US Presidential Elections are known and unsurprising. A number of lessons can be drawn from this election, including the increasing use of seemingly legitimate intermediaries, local influencers, as well as AI. Notably, the engagement of local influencers enabled malicious actors to make easy in-roads into the US right-wing information space while retaining a legitimate veneer. **Such influencers have good reach and can develop content that resonates, and countries should be wary of malicious actors using them as an avenue for information campaigns.** The increased use of AI is also worth noting, with this election cycle showing the increase of: (a) bot armies and AI-generated personas; (b) use of AI-driven algorithms to target specific audience groups; and (c) the generation of audio and video deepfakes at scale.

10. Despite the scale of mis- and disinformation during the US elections, and a number of bomb hoaxes, officials at the US Cybersecurity and Infrastructure Security Agency did not detect any national-level significant incidents impacting the security of the US' election infrastructure. Nonetheless, the presence of foreign influence

campaigns demonstrates the need for countries to maintain vigilance against such threats.

CONTACT DETAILS

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

....

References:

1. Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere
[Link: https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence]

2. Russian Disinformation is demonizing Ukrainian Refugees
[Link: https://www.washingtonpost.com/technology/2022/12/08/russian-disinfo-ukrainian-refugees-germany/]

3. Video of man planning to vote twice for Harris is Russian Disinformation
[Link: https://www.usatoday.com/story/news/factcheck/2024/11/05/haitian-man-georgia-kamala-harris-votes-fact-check/76068148007/]

4. FBI Issues Warning over two Fake Election Videos
[Link: https://www.bbc.com/news/articles/cly2qjel083o]

5. Generative AI will Increase Misinformation about Disinformation
[Link: https://www.lawfaremedia.org/article/generative-ai-will-increase-misinformation-about-disinformation3]

6. An Update on Disrupting Deceptive Uses of AI
[Link: https://openai.com/global-affairs/an-update-on-disrupting-deceptive-uses-of-ai/]

7. Inside Tenet Media, the pro-Trump 'Supergroup' allegedly funded by Russia
[Link: https://www.washingtonpost.com/style/media/2024/09/05/tenet-media-russia-rt-tim-pool/]

8. The US Election was largely trouble-free, but a flood of Misinformation raises future concerns

[Link: https://apnews.com/article/election-2024-security-voting-cybersecurity-misinformation-5fcf17a888ac25855a9feda62d9be50a]

9. US Official sees little voting disruption tied to Foreign Interference

[Link: https://www.reuters.com/world/us/fbi-warns-against-two-fake-videos-officials-combat-election-disinformation-2024-11-05/]

. . . . .