



# | Assessment |

## Influence Campaigns Ahead of the 2024 U.S. Presidential Elections

A-2024-03-22a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Geopolitical Events, All Industries

**March 22, 2024**

**Scope Note**

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on March 12, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# **| Assessment | Influence Campaigns Ahead of the 2024 U.S. Presidential Elections**

**| Executive Summary**

Harmful information is expected to be produced and promulgated online at an unprecedented scale in the run-up to the U.S. Presidential election in November 2024. Adversarial nation states, politically motivated cyber threat actors, and members of the public will almost certainly be responsible for the dissemination of election-related misinformation, disinformation, and malinformation—exacerbating simmering social, political, and geopolitical issues across all sectors of society. This, either intentionally or unintentionally—is expected to make it increasingly difficult to discern fact from fiction.

The extent to which this harmful information is spread to influence the election outcome varies. Some online contributors will almost certainly unwittingly share inaccurate statistics, out-of-date information, or unknowingly engage with posts that the original source knows to be false. However, other threat actors are expected to actively engage in falsifying information, leaking sensitive information, and otherwise trying to shape the outcome of the election.

While at the time of writing, ZeroFox has not identified any indication of active election interference campaigns, activity very likely consistent with attempts to influence the outcome of the U.S. Presidential elections has already been identified on social media.

Individuals and organizations must proactively adopt responsible information consumption practices, as well as monitor for sensitive data disclosures online. Tools and resources are available that can assist in verifying the legitimacy of content, and digital risk protection services can assist in identifying and mitigating the spread of sensitive information should such disclosures occur.

This report should be read in conjunction with 'ZeroFox Intelligence Brief – Demystifying Harmful Online Information, B-2022-09-09a'.

## **| Election Influence vs Election Interference**

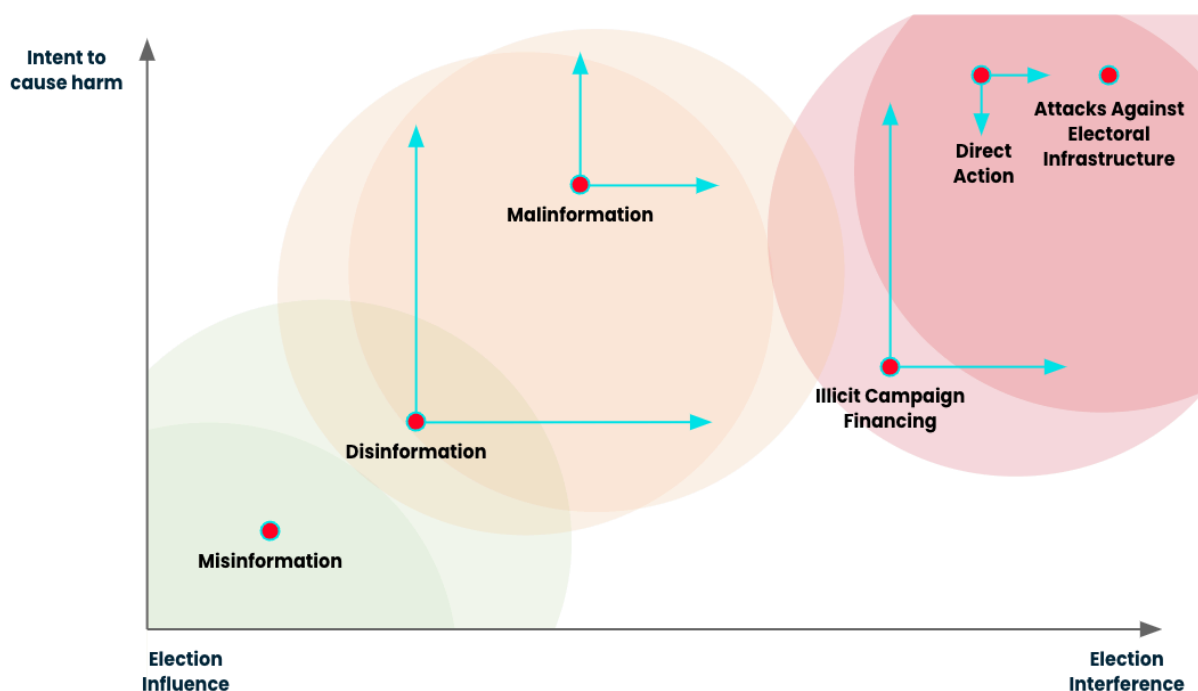
Election influence and election interference sit on a spectrum, with the point at which influencing becomes interference. ZeroFox has analyzed six categories of malicious activity that are known to impact election processes and assessed their likelihood of prevalence in the run-up to the 2024 U.S. Presidential Elections. These include:

- Misinformation
- Disinformation
- Malinformation
- Illicit Campaign Financing
- Attacks Against Electoral Infrastructure
- Direct Action

Individuals conducting these activities vary considerably and have a range of intentions with regard to the extent to which they desire to shape the outcome of the Presidential election. Actors are most likely to include:

- The accidental interferer: Members of the general public who may have no intent to interfere with the election but want to voice truly held beliefs, engage in debate with those around them, or unwittingly engage with actors that have more nefarious intentions.

- The willing interferer: Members of the public that actively seek to stoke divisions, sow discord, influence en-masse, and knowingly spread falsehoods.
- Cyber Criminals: Individuals that seek to leak sensitive information or engage in mass-influence campaigns, either on their own or working in conjunction with adversarial entities such as nation states.
- Adversarial Nation States: Nation State apparatus engaged in widespread campaigns to cause harm to the elections process and undermine democracy, including masquerading as legitimate activity, illicit financing, and event attacks on electoral infrastructure.



Source: ZeroFox Intelligence

## Misinformation, Disinformation, and Malinformation

Misinformation, Disinformation, and Malinformation (MDM) are three ways of categorizing potentially harmful online content. In practice, the lines between these categories are not always clear-cut.

|                | Definition                                                                                                           | Is the information true or based on truth? | Is it spread with intent to cause harm? |
|----------------|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------|-----------------------------------------|
| Misinformation | Content that is false, misleading, or taken out of context but is shared without the intent to deceive or cause harm | ✗                                          | ✗                                       |
| Disinformation | Deliberately false, misleading, manipulated, or biased content spread with the intent to deceive or cause harm       | ✗                                          | ✓                                       |
| Malinformation | Genuine information, or information based on reality, spread with the intent to cause harm                           | ✓                                          | ✓                                       |

Source: ZeroFox Intelligence

Misinformation is content shared that is false, misleading, or taken out of context but is shared without the intent to deceive or cause harm. The prevalence of misinformation online is a product of human and technological factors.

- Misinformation is exacerbated by flaws in human conditioning, a lack of critical challenge, and biases. Users are more likely to react to content that relates to pre-existing grievances and beliefs and are less likely to carefully consider the source.
- Technological factors amplify misinformation online. Social media and news feeds rely on machine learning and statistical algorithms that can enable similarly-behaving users to be grouped and content to be promoted that they are more likely to react to.

Disinformation is deliberately false, misleading, manipulated, or biased content spread with the intent to deceive or cause harm. Disinformation is created to be deliberately deceptive, and campaigns are typically motivated by three factors: power or influence, profit, or to sow division.

- Campaigns are widespread and conducted by actors ranging from nation states to cyber criminals and online trolls.
- Disinformation is designed to have negative consequences. The discreditation of legitimate, impartial outlets pushes people towards alternative sources that may lack credibility.
- The prevalence of disinformation online is also amplified by technological factors.

Malinformation is genuine information, or information based on reality, spread with the intent to cause harm. Malinformation poses a significant threat to the public, VIPs, and organizations in almost all industries. Like disinformation, malinformation actors are typically driven by power or influence, profit, or to sow division. It differs from disinformation in that it contains true or genuine information.

- Malinformation can lead to reputational damage and financial loss, both at an individual and enterprise level.
- It can be used to undermine political and corporate negotiations, influence democratic processes, and compromise national security.
- Examples of malinformation include, but are not limited to, the dissemination of confidential information and leaking of private emails.

The distinction between these categories is often—and sometimes intentionally blurred. The primary distinction between mis- and disinformation relates to intent, which can be difficult to determine.

- While conspiracy theories may be started and circulated for nefarious purposes, they could be propagated by unwitting, misinformed, and well-intentioned individuals who believe it to be true.
- Conversely, misinformation can turn into disinformation when it is still shared by individuals who know it is incorrect but intentionally spread it to stir division.

The boundary between disinformation and malinformation is also blurred, particularly when discerning the point at which misrepresentation or distortion of facts becomes outright fabrication.

## Likelihood of Malicious Activity

| Category       | Description                                                                                                          | Examples                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Actor                 | Likelihood          |
|----------------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|
| Misinformation | Content that is false, misleading, or taken out of context but is shared without the intent to deceive or cause harm | <ul style="list-style-type: none"> <li>Inaccurate statistics</li> <li>Out-of-date information</li> <li>Unwitting reposting of disinformation</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                            | Members of the Public | Almost Certain      |
|                |                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Cyber Criminals       | Very Likely         |
| Disinformation | Deliberately false, misleading, manipulated, or biased content spread with the intent to deceive or cause harm       | <ul style="list-style-type: none"> <li>Deep Fakes and other synthetic media</li> <li>False claims about political parties and individuals</li> <li>Conspiracy theories</li> <li>Narratives that undermine trust in politics and institutions</li> <li>False claims designed to exacerbate public discord on socially divisive issues</li> <li>Creation of fake identities to impersonate authentic behaviors and amplify false narratives (includes troll farms)</li> <li>Purchase of political advertisements by fake entities and impersonation of legitimate sources</li> </ul> | Members of the Public | Almost Certain      |
|                |                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Cyber Criminals       | Almost Certain      |
|                |                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Nation State Actors   | Very Likely         |
| Malinformation | Genuine information, or information based on reality, spread with the intent to cause harm                           | <ul style="list-style-type: none"> <li>Hacking and leak of confidential candidate information</li> <li>Leaking of private emails</li> <li>Release of stolen communications</li> <li>Selective opinion polls</li> </ul>                                                                                                                                                                                                                                                                                                                                                             | Members of the Public | Very unlikely       |
|                |                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Cyber Criminals       | Roughly Even Chance |

| Category                                 | Description                                                                                        | Examples                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Actor                 | Likelihood          |
|------------------------------------------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|
|                                          |                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Nation State Actors   | Roughly Even Chance |
| Illicit Campaign Financing               | Covert funding of a campaign by foreign actors                                                     | <ul style="list-style-type: none"> <li>Funding provided by nation states—including through third parties—to increase the chances of victory for a preferred candidate, or to increase division</li> <li>Foreign actors leveraging communications firms to campaign on behalf of favored candidates</li> </ul>                                                                                                                                                                  | Nation State Actors   | Unlikely            |
|                                          |                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Cyber Criminals       | Very unlikely       |
| Attacks Against Electoral Infrastructure | Equipment manipulation or tampering, or compromising physical voting stations                      | <ul style="list-style-type: none"> <li>Malicious actors altering voter registration records or voting results.</li> <li>Malicious tampering by those with physical access to voting equipment or tabulators</li> <li>Remote hacking of voter registration sites, voter terminals, vote counting technologies, Electoral Management Bodies,</li> <li>Physical intimidation at voting booths</li> <li>Hacking of Critical National Infrastructure to disrupt the vote</li> </ul> | Members of the Public | Almost No Chance    |
|                                          |                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Cyber Criminals       | Very Unlikely       |
|                                          |                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Nation State Actors   | Very Unlikely       |
| Direct Action                            | Participants in the election are targeted by financial or physical coercion to achieve their aims. | <ul style="list-style-type: none"> <li>Members of political parties targeted with threats of intimidation, blackmail and physical violence</li> </ul>                                                                                                                                                                                                                                                                                                                          | Members of the Public | Very Unlikely       |
|                                          |                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Cyber Criminals       | Very unlikely       |
|                                          |                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Nation State Actors   | Almost No Chance    |

Source: ZeroFox Intelligence

## **Russian Interference in the 2016 U.S. Presidential Elections**

Russian interference in the 2016 U.S. Presidential elections has been confirmed by U.S. intelligence agencies.<sup>1</sup> While Russia did almost certainly not actually alter votes, state-linked entities reportedly engaged in:

- Disinformation – Spreading propaganda on X (formerly Twitter), Facebook, YouTube and Instagram.
- Malinformation – Hacked the Hillary Clinton campaign, the Democratic Congressional Campaign Committee, and the Democratic National Committee; Publicly released politically damaging information.
- Illicit Campaign Financing – Attempted malicious party funding via business propositions to candidates.
- Attacks Against Electoral Infrastructure – Probed state voter databases for insecurities; Targeted voter registration systems and websites in the run up to election day; Accessed multiple state's electoral systems; and Exfiltrated voters' personal information.

## **| Campaigns Identified to date**

Activity very likely consistent with attempts to influence the outcome have been identified as widespread online and on social media platforms, including X (formerly Twitter), Facebook, Instagram, and TikTok. Influence campaigns fall into the three MDM categories, with themes ranging from:

- Undermining the likely Presidential candidates themselves—including President Biden and President Trump
- Disparaging U.S. democracy
- Stoking discord on socially divisive topics
- And leaking voter data.

---

<sup>1</sup> [hXXps://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections](https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections)

These are most likely being propagated by accidental interferers and willing interferers, although ZeroFox notes the possibility that more organized criminal and nation state actors are behind some of the posts.

While adversarial nation states and cyber criminals are very likely to attempt to sway public opinion to influence the outcome of the election, it is very unlikely these actors will actively interfere with voting processes or engage in direct intimidation of candidates at any significant scale. However, election-influence campaigns are very likely to be widespread.

- This is most likely to take the form of disinformation campaigns, though ZeroFox notes the possibility that nation states will use third-party services to campaign on behalf of preferred candidates.
- Additionally, nation states may engage directly—or indirectly via cyber criminal enterprises—in hacks and leaks of sensitive candidate information. Indirect engagement would likely provide plausible deniability.

### Mis- and Disinformation on Candidates

The threat from mis- and disinformation on likely Presidential candidates—President Biden and President Trump—is almost certainly on an upward trajectory. This includes the prevalence of Deep Fakes targeting both candidates' campaigns, which very likely remain on an upward trajectory as threat actors continue to experiment with Deep Fake tools for a wide range of election-related purposes.

ZeroFox has identified numerous examples of mis- and disinformation related to President Biden, typically seeking to undermine his credibility and promulgate malicious tropes.

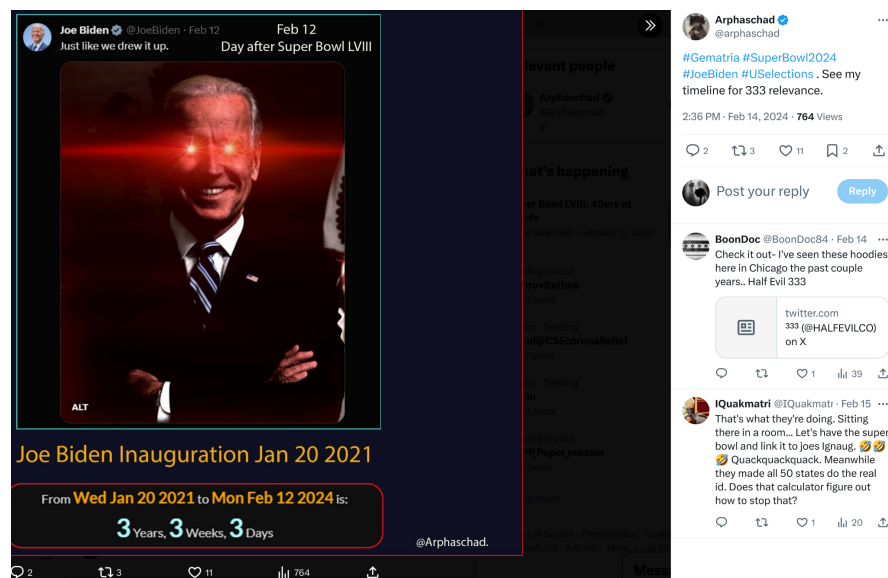
- ZeroFox identified multiple sites dedicated to circulating mis- and disinformation in relation to President Joe Biden. This includes a website named "realgreenews" that provides multiple videos supporting widely circulated and unsubstantiated tropes about President Biden, including unsubstantiated claims of pedophilia.<sup>23</sup> While ZeroFox cannot ascertain the motivation behind the website operator, WHOIS data indicates they are based in the U.S.

---

<sup>2</sup> [hXXps://realgreenews\[.\]com/joe-dirt-biden](https://realgreenews[.]com/joe-dirt-biden)

<sup>3</sup> [hXXps://patriotpost\[.\]us/](https://patriotpost[.]us/)

- Multiple instances of manipulated or edited video content of President Biden are circulating on TikTok. This includes content circulated by pro-Republican accounts 'Empirical University' and 'Liberal Meme Central', alongside a video titled 'The Bible According to Joe Biden' which seemingly aim to promote the view that President Biden has deteriorating health and cognitive function.<sup>45</sup>
- On February 14, 2024, X user "Arphaschad" posted a numerological scheme related to Joe Biden, equating "333", and one of his followers, "BoonDoc", quickly related it to a fashion brand named "Half-Evil", likely to support the assumption that Biden is actually Satan.<sup>6</sup>



### Arphaschad's post likening President Biden to Satan

Source: [hXXps://x.com/arphaschad/status/1757745707769893346?s=20](https://x.com/arphaschad/status/1757745707769893346?s=20)

Disinformation campaigns relating to President Trump are also widespread at the time of writing, with content likely created to either aid or undermine his campaign.

- In early 2024, synthetically-generated images showing President Trump interacting with Black voters were circulated widely on social media platforms.<sup>7</sup> These images were very likely generated by President Trump supporters in an

<sup>4</sup> [hXXps://www.tiktok.com/@dj\\_omega\\_50\\_/video/7347886379801562410](https://www.tiktok.com/@dj_omega_50_/video/7347886379801562410)

<sup>5</sup> [hXXps://www.tiktok.com/@libsmemecentral](https://www.tiktok.com/@libsmemecentral)

<sup>6</sup> [hXXps://x.com/arphaschad/status/1757745707769893346?s=20](https://x.com/arphaschad/status/1757745707769893346?s=20)

<sup>7</sup> [hXXps://www.bbc.com/news/world-us-canada-68440150](https://www.bbc.com/news/world-us-canada-68440150)

attempt to garner support from Black communities for his campaign. While the images have been widely debunked and flagged as being fake, images of this nature are likely to become increasingly prevalent.

- The pro-Republican Party, anti-Trump media outlet The Lincoln Project has circulated synthetically generated material in the form of Deep Fakes to create disinformation.<sup>8</sup> The content—which is flagged as AI-generated by the poster—disparages President Trump, citing alleged grievances on behalf of his father.<sup>9</sup>



### Deep Fake images of President Trump with Black voters

Source: <https://www.bbc.com/news/world-us-canada-68440150>

## Outlook

ZeroFox anticipates the spread of mis- and disinformation influence campaigns on candidates will increase in the run-up to the election. This will almost certainly be propagated by members of the public, as well as cyber criminals across social media platforms and on dedicated websites.

<sup>8</sup> <https://x.com/ProjectLincoln/status/1758615361501503868?s=20>

<sup>9</sup> <https://twitter.com/ProjectLincoln/status/1758615361501503868>

It is very likely adversarial nation states will conduct or amplify disinformation campaigns on social media, most likely through the use of paid influencers, troll accounts, and bots that are designed to mimic the activity of legitimate users. Adversarial nation states very likely view this as a method to achieve their political aims while maintaining plausible deniability.

### **Russia-Ukraine War**

A significant proportion of disinformation currently circulating in relation to the 2024 U.S. Presidential election currently surrounds Russia's war in Ukraine; specifically, that Ukrainians have no appetite for the war, that the U.S. should cease support for Ukraine, and that U.S. military personnel will be compulsorily drafted to engage on the ground. Military support for Ukraine against Russian aggression is an area of division in domestic politics currently, likely serving as a sphere for achieving political influencing objectives.

- One account regularly spreading disinformation on X operates under the handle "thesiriusreport" (screen name "The Sirius Report"), active on the platform since 2016. The handle is openly pro-"multipolar world," which has become a synonym for being pro-Russia and pro-China. On February 21, 2024, The Sirius Report claimed that "a majority of Ukrainians now wish to see a diplomatic resolution of [sic] the war with Russia", yet providing no source for the claim. The post has more than 83,000 engagements.<sup>10</sup> The claim was refuted by a poster that referred to the results of a recent poll that shows exactly the contrary—that most Ukrainians support fighting until Russia is expelled from Ukrainian territory. While ZeroFox cannot ascertain the motivation behind the poster, WHOIS data indicates the individual is based in the U.S.

---

<sup>10</sup> [hXXps://x.com/thesiriusreport/status/1760252938176344273?s=20](https://x.com/thesiriusreport/status/1760252938176344273?s=20)



## The Sirius Report's unsubstantiated claim the majority of Ukrainians support a diplomatic resolution with Russia

Source: [hXXps://x\[.\]com/thesiriusreport/status/1760252938176344273?s=20](https://x.com/thesiriusreport/status/1760252938176344273?s=20)

- On February 20, 2024, X user "Acyn" quoted a statement by U.S. politician and political commentator Tulsi Gabbard claiming that NATO is expecting the U.S. to risk the lives of their citizens while they would not do it for themselves.<sup>11</sup> The post very likely refers to a potential triggering of Article 5 of the NATO charter in relation to Russia's ongoing aggression, of which there is currently no evidence of plans to do. Article 5 states that if a NATO ally is the victim of an attack, each and every other member of the Alliance will consider this act of violence as an armed attack against all members and will take the actions it deems necessary to assist the Ally attacked. The only activation of Article 5 to date followed the September 11 attacks in the U.S. in 2001 and the following Global War on Terror. NATO soldiers lost their lives fighting alongside U.S. forces.
- Following the recent Russian Federation elections, mis- and disinformation continues to circulate on X comparing Russian "democracy" to alleged Ukrainian "non-democracy," and in some cases even comparing Russian democracy to that of the U.S.—and how deficient the latter is. On March 17, 2024, U.S. a self-proclaimed U.S. patriot operating under the handle "mefbama", claimed that

<sup>11</sup> [hXXps://x\[.\]com/Acyn/status/1759739057398046863?s=20](https://x.com/Acyn/status/1759739057398046863?s=20)

it is odd that Russia is still holding “elections” while supposedly “democratic” Ukraine does not.<sup>12</sup> The post—either knowingly or unknowingly—fails to acknowledge that in the latter case, the reason for not holding elections is actually the law, in this case – martial law that is still in place in Ukraine. The post has recently had a community note added specifying this.



Seems odd Russia is still having elections, when Ukraine is not because their gov, Zelensky won't let them. Makes me question whether Ukraine has any democracy at all.

6:09 PM · Mar 17, 2024 · **15.1K** Views

### **Mefbama’s post questioning the existence of Ukrainian democracy**

Source: [hXXps://x\[.\]com/mefbama/status/1769395702734492084?s=20](https://x.com/mefbama/status/1769395702734492084?s=20)

## **Outlook**

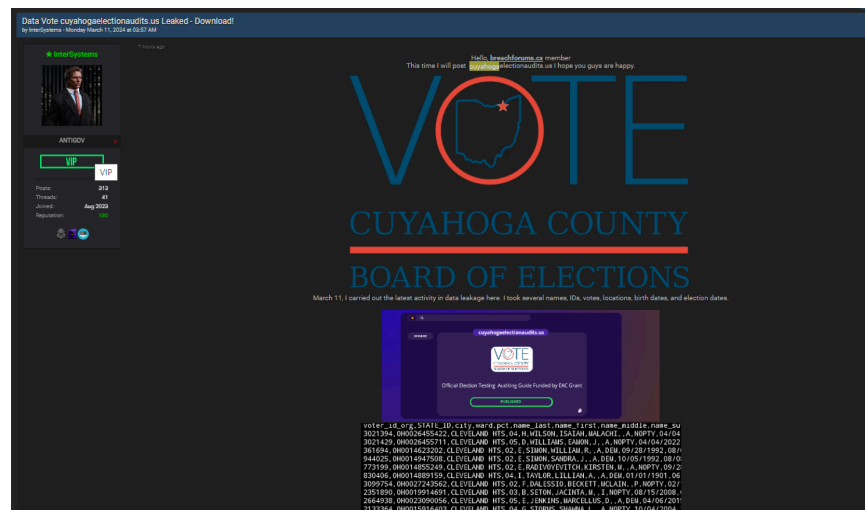
Russia’s war in Ukraine will very likely remain a focus for mis- and disinformation influence campaigns, as it remains a socially and politically divisive issue. It will also likely draw increasing attention from Pro-Russian actors who seek to create and amplify disinformation campaigns to garner support for the candidate of their choice. These campaigns will most likely attempt to undermine support for Ukraine, fabricate alleged party policies, and increase fear of greater U.S. involvement in the war. ZeroFox also notes the possibility that threat actors may target U.S. politicians and related personnel to leak sensitive communications relating to the war.

## **Malinformation**

While malinformation relating to the 2024 U.S. Presidential elections is rare, ZeroFox has identified at least one example of threat actors claiming to have obtained sensitive voter data.

<sup>12</sup> [hXXps://x\[.\]com/mefbama/status/1769395702734492084?s=20](https://x.com/mefbama/status/1769395702734492084?s=20)

- On March 11, 2024, a threat actor "InterSystems" claimed to have leaked a database associated with the Cuyahoga Election Audits (cuyahogaelectionaudits[.]us) on the predominantly English-language dark web forum, "BreachForums." The threat actor claims to have leaked data, including names, IDs, votes, locations, birth dates, and election dates. The threat actor did not disclose the ultimate source of the data breach or how it was exploited.



## InterSystems alleging to have obtained a database related to Cuyahoga's Election Audits

Source: ZeroFox Intelligence

## Outlook

The threat Mis- dis- and malinformation campaigns will very likely increase at a dizzying pace as voting draws closer and candidates ramp up campaigning activities. Sensitive data is most likely to pertain to the disclosure of sensitive information on voters, as well as private communications of candidates and related political personnel.

While breaches are most likely to be conducted by politically-motivated criminals, the threat from adversarial nation states is considerable, which may leverage cyber criminal communities to maintain plausible deniability. ZeroFox also notes the possibility that data breaches and sensitive information will be fabricated and disclosed in open sources to discredit political campaigns.

### **Illicit Campaign Financing, Attacks Against Electoral Infrastructure, and Direct Action**

At the time of writing, ZeroFox has not identified any indication of overtly active interference campaigns in the 2024 U.S. Presidential elections. This includes no evidence of illicit campaign financing, attacks against electoral infrastructure, or direct action against candidates.

## **| Recommendations**

- Question the credibility of sources, such as the date the content was published, and identify any potential source biases.
- Consider the content in its entirety, not just a headline.
- Use fact-checking websites like FactCheck.org, the News Literacy Project, and NewsGuard.
- Conduct training on how MDM works to boost defenses to, and recognition of, false claims.
- For organizations that find themselves a victim of MDM, have a crisis response plan in place to evaluate the content and formulate an approach to neutralize and contain the malicious information.
- Ensure a thorough understanding of the exposure of key individuals and organizations in open and closed sources.
- Keep updated with evolving threat actor tactics, techniques, and procedures.
- Proactively monitor for potential network access sales to obtain critical early warnings of impending cyberattacks.
- Monitor news and social media for breaking stories on data breaches and leaks.
- Employ digital risk protection services to determine the credibility of breach claims and mitigate potential impacts.

## **| Appendix A: Traffic Light Protocol for Information Dissemination**

|                                | <b>Red</b>                                                                                                                                                                                             | <b>Amber</b>                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>                                                                                                                                                                                           | <b>Clear</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> information without restriction, subject to copyright controls.                                                                                                                                                                                                              |

## **Appendix B: ZeroFox Intelligence Probability Scale**

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

| Almost No Chance | Very Unlikely | Unlikely | Roughly Even Chance | Likely | Very Likely | Almost Certain |
|------------------|---------------|----------|---------------------|--------|-------------|----------------|
| 1-5%             | 5-20%         | 20-45%   | 45-55%              | 55-80% | 80-95%      | 95-99%         |