Protecting Election 2024 from foreign malign influence: lessons learned help us anticipate the future

MTAC REPORT

Date: November 8, 2023

Today's era of digital competition necessitates a constant commitment from democracies to defend their institutions and elections. As dozens of major democratic elections take place around the globe in 2024, authoritarian regimes continue to routinely leverage cyber and influence operations to target election infrastructure, campaigns, and voters.

Last year, the 2022 US midterm elections came and went without impactful cyber or influence operations from Russia, Iran, or China — a welcome change, and likely the result of policy measures and mitigation methods undertaken by US institutions and technology companies. US midterm elections, however, offer limited gains for authoritarian regimes seeking to advance geopolitical goals. Distributed candidates and electoral systems make US congressional contests particularly difficult to influence, as understanding local voters and candidates in hundreds of districts proves far more challenging than a presidential contest.

US election defenders should not believe that the trends of 2022 will extend to 2024. Presidential elections determine the course of foreign policy and for authoritarian nation states — principally Russia, Iran, and China — next year's presidential contest will be critical for each of these countries seeking to advance their strategic goals. Election 2024 may be the first presidential election during which multiple authoritarian actors simultaneously attempt to interfere with and influence an election outcome. This report principally discusses Russia, Iran, and China, the three nation state actors whose cyber-enabled influence operations we most closely track throughout the year. Lessons from past election defense and early indicators of election influence efforts can inform how we should collectively prepare to protect next year's US presidential election from foreign interference and influence.

A short history of authoritarian interference in US elections (2016-2022)

Russia's cyber and influence operations targeting several Western elections from 2015-16 opened a new era of digital competition. Government and academic communities have devoted significant resources to the discipline since and dissected these activities into two categories: influence and interference. The Microsoft Threat Analysis Center (MTAC), in our analysis and reporting, utilize the framework as described in the 2021 Office of the Director of National Intelligence (ODNI) report "Foreign Threats to the U.S. 2020 Federal Election." ODNI defines election influence as "overt and covert efforts by foreign governments or actors acting as agents of, or on behalf of, foreign governments intended to affect directly or indirectly a US election — including candidates, political parties, voters or their preferences, or political processes." Election interference, comparatively, refers to a "subset of election influence activities targeted at the technical aspects of the election, including voter registration." Our analysis over the next year will inform this framework, and based on past elections, we expect the proportion of foreign influence to foreign interference in election 2024 to shift from the former to the latter as Election Day gets closer.

Russia has long undertaken influence and interference efforts in elections around the world, using a multifaceted approach that relies on cyberattacks, hack-and-leak operations, state-sponsored media outlets, and covert social media personas, among other tactics. Russia's distinct political warfare approach, known as "active measures," seeks to use such cyber-enabled influence operations to infiltrate foreign audiences and elevate political candidates sympathetic to the Kremlin's foreign policy objectives. The 2015 Brexit vote in the United Kingdom, the 2017 French and German elections, and the 2016, 2018, and 2020 US elections represent just a few examples of contests in which the Kremlin attempted to influence the outcome with the hopes of shaping their foreign policy objectives.

Russia is not alone in its influence and interference targeting elections around the world. Iran, for its part, routinely targets regional elections. During the 2020 US presidential election, Iran launched several cyber-enabled influence operations that impersonated American extremists, and attempted to sow discord among US voters and incite violence against US government officials. Since 2020, Iran extended its track record of election meddling, amplifying cyberattacks with parallel online influence operations in Bahrain and Israel.

Historically, China's Chinese Communist Party (CCP) largely focused its propaganda and social media disinformation on Taiwan, a relevant example being the 2020 Taiwanese presidential election. But in the last three years, the CCP has dramatically scaled up the scope and sophistication of its overt and covert influence activity around the world and expanded its covert social media operations, undertaking light influence activity during the 2022 US midterm elections.

High stakes for authoritarians with 2024 US election outcome

The 2024 US presidential election cycle will define the foreign policy future of the US in several major conflicts. For the Kremlin, disrupting American support for Ukrainian President Volodymyr Zelensky is of critical importance. Today, US support to Israel amid the Israel-Gaza War acts as a buffer to Iran's potential escalation of a wider regional conflict. Meanwhile, China's increasing aggressiveness in the Taiwan Strait could potentially escalate a future conflict in East Asia, which would in part be shaped by US commitments to preserve stability in the Strait.

For Russia, Iran, and China, the next US president will define the direction of conflict — whether wars might occur, or peace might prevail. MTAC expects Russia, China, and Iran are unlikely to sit out next year's contest — the stakes are simply too high.

Anticipating what these three authoritarian nation states might do during the 2024 US election cycle requires some reflection on a dynamic US digital information environment. Foreign manipulators seek out the audiences they hope to influence, and American audiences continue migrating to more and different online platforms. Those targeting US

elections in previous years will encounter a far different online information landscape in 2024 compared to 2016.

America's social media ecosystem today is far more visual than in previous years. Memes, gifs, podcasts, video clips, and influencers are the means of today's influence operations — not bots and pithy text posts. The sale of the world's largest micro-blogging platform a year ago spurred the development of and migration to many similar competing micro-blogging platforms with audiences and nation-state actors transiting between them. MTAC has detected new, inauthentic personas and networks emerging on traditional social media platforms, but their followings appear small, or if large, mostly inauthentic. The lack of centrality among social media users — with different platforms catering to different audiences via different mediums — presents a tougher challenge for all foreign manipulators seeking to shift votes to their preferred candidates from afar.

Russia, though, remains the most committed and capable threat to the 2024 election. The Kremlin likely sees next year's contest a must-win political warfare battle determining the trajectory of support to Kyiv and the outcome of the Ukraine War.

In the year prior to election 2016 and election 2020, 2015 and 2019 respectively, our team observed account positioning and messaging designed to sway audiences across the political spectrum in hopes of influencing the nominee result in each political party before the general election. In 2023, we've observed limited Kremlin activity to influence the outcome of the US primary season and nearly all account placement and infiltration appears tailored for the same audiences and themes as the 2020 presidential contest. However, in recent weeks, MTAC has observed Russia's influence ecosystem slowly accelerating their operations mimicking current news trends with political narratives. Overt Russian media outlets and covert Russia-affiliated social media networks have aligned, focusing their propaganda and disinformation on Western military aid to Ukraine and messaging against candidates committed to it. Based on the limited amount of Kremlin influence activity to date, MTAC observes three key trends during this year's election cycle.

First, Kremlin-aligned actors likely will reuse existing assets to infiltrate and influence US voters. The Kremlin and sympathetic influential public figures have long developed outlets and associated social media networks to target US voters. While some entities, like the overt Russian state-backed outlet RT and the SVR-directed Strategic Culture Foundation operate continuously, other actors launch campaigns in distinct patterns around election cycles, often utilizing accounts with well-developed audiences. One Russia-affiliated social media network has repositioned to focus on the 2024 election, including a focus on at least one specific swing state, within two weeks of the first primary debate in August 2023. This network previously participated in social media operations for the Russian outlet North American and European Based Citizens (NAEBC), a 2020 election influence operation reportedly assessed by the FBI as "run by people associated with [Yevgeny Prigozhin's Internet Research Agency troll farm]," which also launched campaigns targeting US voters before the 2022 midterm

elections. While some new account batches will seed new content for campaigns and others will emerge for amplification and engagement, existing influence assets will continue to provide the easiest broadcasting platforms for new campaigns.

Second, some assets affiliated with the late Yevgeny Prigozhin, previously the owner of the Wagner Group, Patriot Media Group and the Internet Research Agency (colloquially known as the Russian troll farm), remain active — but persistence and lasting impact remain to be determined. Two Prigozhin-affiliated assets remain persistently focused on the US election: the former NAEBC profile network and the Foundation to Battle Injustice outlet, which has platformed damaging personal claims around at least one 2024 candidate since at least January 2023. Both demonstrate indications of former Prigozhin assets remaining on course to utilize already-cultivated audiences in the US. Further, members of a Wagner Group affiliate youth group met in Russia with a US-based separatist influencer who has discouraged individuals within a specific US racial demographic from voting in 2024. A July 2023 blog post on a domain registered by this influencer explicitly claims the Russian group has developed a foothold within the US to lawfully campaign against the US government, although the reality around these claims warrants scrutiny.

Finally, Russia-affiliated actors will likely leverage newly observed tactics empowered by new technology — generative AI. Since at least July 2023, Russia-affiliated actors have utilized innovative methods to engage audiences in Russia and the west with inauthentic, but increasingly sophisticated, multimedia content. These actors publish videos spoofing legitimate media coverage of fake content espousing Kremlin-preferred narratives delegitimizing Ukraine and casting blame for the current Israel and Gaza conflict on the US and Ukraine. As the election cycle progresses, we expect these actors' tradecraft will improve while the underlying technology becomes more capable.

Iran will likely remain as a spoiler and, if Tehran does anything in 2024, it will seek to sow chaos later in the election cycle with equal focus on election interference as influence. With fewer resources to commit to persistent, sophisticated influence campaigns, Tehran will need to target those it seeks to denigrate more precisely, thus any operations — likely a hybrid campaign, blending cyber and influence activity — would likely occur much closer to Election Day. Thus far, we've not witnessed any significant election influence or interest from Iran-affiliated influence actors, but we expect that will change with increased tensions in the Middle East.

In 2020, China committed little effort to influence the US presidential election. But, as the CCP has scaled its propaganda and disinformation capabilities, China has grown more provocative pursuing election influence in the 2022 US midterms and Canada's federal elections. The next few months may offer a preview of CCP election influence and interference as Taiwan's national elections occur in January 2024. MTAC has observed some China-affiliated inauthentic social media personas and accounts infiltrating US audiences and posting divisive and inflammatory content about American candidates. The accounts and their content have

yet to gain much traction, but their presence indicates Beijing may be positioning for 2024 election influence or interference.

The most sophisticated actors influencing and interfering in elections likely will employ a combination of targeted hacking operations with strategically timed leaks to drive media coverage to elevate their preferred candidates. To date, MTAC has not observed cyberattacks we believe to be tied to next year's US presidential election. We assess it's too early in the election cycle for any nation state actor to know who and where to breach. Russian intelligence services have consistently attempted hacks to power their influence activity, and Iran, over the past two years, has prolifically used hack-and-leak operations against a range of Tehran's opponents. China, thus far, has not employed target hacks to power their election influence operations against the US, but that may change in the future.

The US should expand its detection of foreign influence campaigns beyond Russia, Iran, and China. One constant since 2016 has been ever more countries conducting cyber- enabled influence operations in pursuit of their foreign policy goals. Many countries have developed inauthentic and overt information capabilities and likely all may find interest in achieving foreign policy goals in election 2024.

Looking ahead

Nonetheless, election defense efforts — from both US government and the private sector — will likely be heavily tested this year and next as the election cycle begins. Microsoft remains committed to protecting democratic elections, and we've outlined our principles for safeguarding elections and democratic institutions in the era of AI in our recent blog, "Protecting Elections and Safeguarding Democracy in the Age of AI: How Microsoft is helping candidates, campaigns, election authorities, and voters navigate the challenges of AI and cybersecurity." This report offers the first of several assessments MTAC will provide throughout the next year leading up to Election Day. Threat activity documented in these assessments will inform Microsoft's Democracy Forward team's programs to protect candidates, campaigns, elections, and voters headed into 2024.