60 Days Until Election 2024

Election Security Update as of Early September 2024

Foreign actors are increasing their election influence activities as we approach November. In particular, Russia, Iran, and China are trying by some measure to exacerbate divisions in U.S. society for their own benefit, and see election periods as moments of vulnerability. These actors most likely judge that amplifying controversial issues and divisive rhetoric can serve their interests by making the United States and its democratic system appear weak and by keeping the U.S. Government distracted with internal issues instead of pushing back on their hostile behavior in other parts of the world.

No Efforts To Interfere in Conduct of Elections

To date, the IC has not observed any foreign actor seeking to interfere in the conduct of the 2024 elections. The IC and our partners, however, continue to monitor foreign actors' influence efforts, seeking to uncover any activities that could enable election interference, especially cyber or physical disruptions of election infrastructure. The interagency election security community assesses that it would be very difficult for a foreign actor to manipulate election processes at a large enough scale to impact the outcome of a federal election without detection by intelligence collection, post-election audits, or physical and cybersecurity monitoring of the decentralized and diverse election infrastructure across the country.

Instead of interference, the IC assesses adversaries so far are focused on using information operations and propaganda to try to shape voter preferences or undermine confidence in the election. We continue to monitor adversaries' efforts to cast doubt on the electoral process or claim that they have interfered in the process when they have not actually done so, a tactic known as "perception hacking."

- In addition, reports of cyber espionage against election or campaign infrastructure do not necessarily mean that an actor is trying to affect the conduct of an election. Foreign adversaries sometimes use cyber tools to collect information that helps them tailor their influence messages to certain U.S. audiences or embarrass or denigrate particular candidates through leaks. For example, we have seen foreign actors work to compromise political entities. We have seen all key foreign actors engage in such efforts during this election cycle.

Foreign Actors

The IC continues to assess that **Russia** poses the most active foreign influence threat to this year's U.S. elections. Russia is looking to amplify divisive rhetoric and influence election outcomes, which is consistent with Moscow's broader foreign policy goals of weakening the United States and undermining Washington's support for Ukraine.

- As this week's U.S. Government actions further demonstrate, Russia is using entities such as the U.S.-sanctioned organizations Social Design Agency (SDA) and ANO Dialog and the state media outlet RT to covertly amplify and stoke domestic divisions and push for Russia's preferred election outcomes. RT has built and used networks of U.S. and other Western personalities to create and disseminate Russia-friendly narratives, while trying to mask the content in authentic Americans' free speech.
- These actors, among others, are supporting Moscow's efforts to influence voter preferences in favor of the former President and diminish the prospects of the Vice President through methods such as targeted online influence operations on social media and websites that portray themselves as legitimate news sites.

60 Days Until Election 2024 *(continued)*

Foreign Actors *(continued)*

The IC assesses that **Iran** is making a greater effort than in the past to influence this year's elections, even as its tactics and approaches are similar to prior cycles. Like Russia, Iran has a multi-pronged approach that seeks to stoke discord and undermine confidence in our electoral process. Tehran also has sought cyber access to individuals with direct ties to the presidential campaigns of both political parties while elements have also denigrated the former President.

- Iran has a suite of tools at its disposal, as demonstrated in recent reports outlining Iran's cyber operations, including the hack and leak operation against the former President's campaign. Beyond attempts to hack and leak information, Iran is conducting covert social media operations using fake personas and using AI to help publish inauthentic news articles.

China, for its part, is focused on influencing down-ballot races and is still not attempting to influence the presidential race. China is also continuing its longstanding efforts to build relationships with U.S. officials and entities at state and local levels because it perceives Washington as largely opposed to China. This view likely informs Beijing's greater interest in some non-presidential races.

- The IC is aware of PRC attempts to influence U.S. down-ballot races by focusing on candidates it views as particularly threatening to core PRC security interests.
- PRC online influence actors have also continued small-scale efforts on social media to engage U.S. audiences on divisive political issues, including protests about the Israel-Gaza conflict, and promote negative stories about both political parties.

We are seeing a number of countries considering activities that, at a minimum, test the boundaries of election influence. Such activities include lobbying political figures to try to curry favor with them in the event they are elected to office.