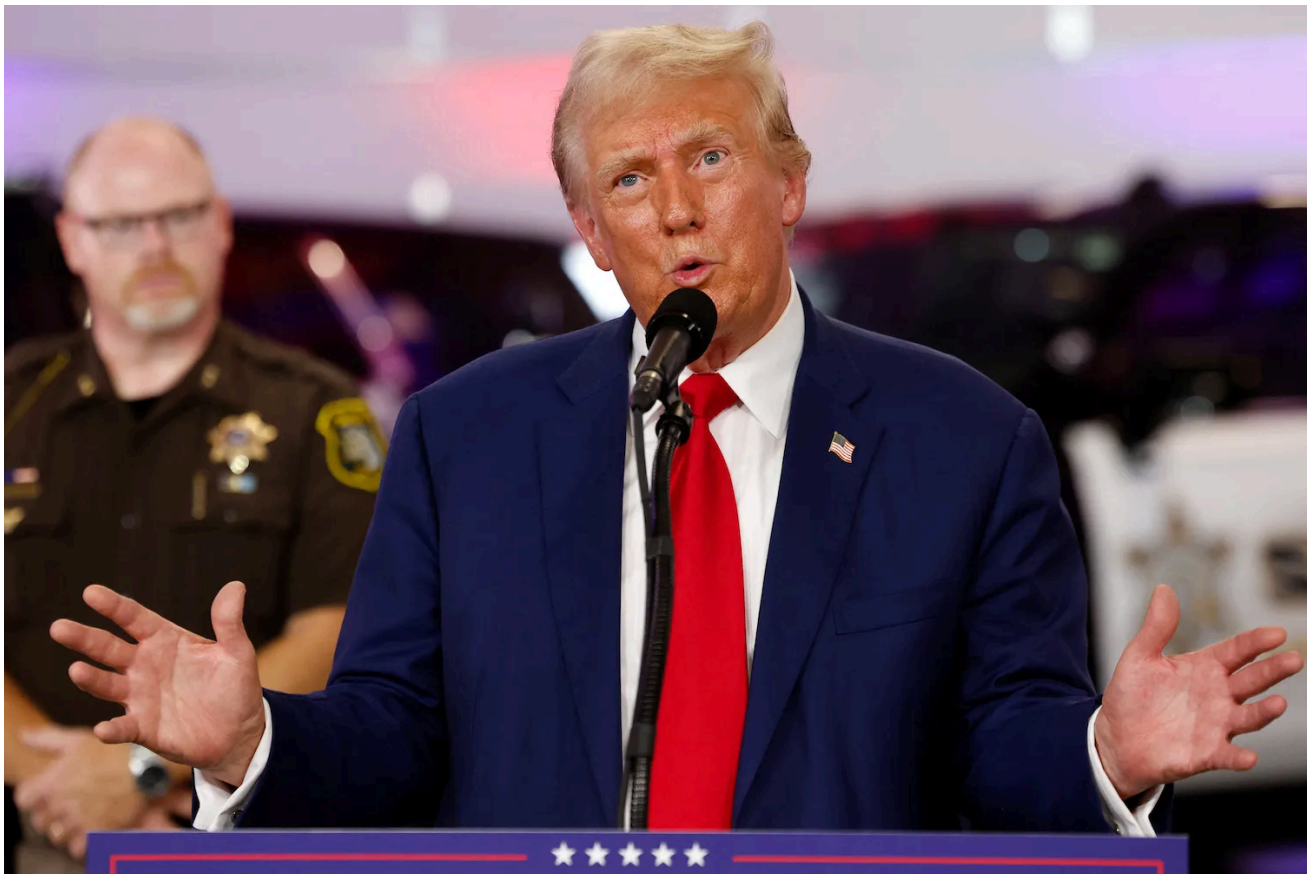
REPORT

Why Everyone's Suddenly Talking About Iranian Election Hacking

America's Middle Eastern adversary is occupying an arena typically dominated by Russia and China.

By Rishi Iyengar



Former U.S. President Donald Trump, the Republican presidential nominee, delivers remarks on crime and safety at the Livingston County Sheriff's Office in Howell, Michigan, on Aug. 20. U.S. agencies on Monday officially blamed Iran for the recent hack-and-leak operation against Trump's campaign. JEFF KOWALSKY/AFP VIA GETTY IMAGES

My FP: Follow topics and authors to get straight to what you like. Exclusively for FP subscribers. Subscribe Now | Log In

AUGUST 21, 2024, 2:15 PM

View Comments (1)

As November's U.S. presidential election draws closer and the campaigns of former President Donald Trump and Vice President Kamala Harris kick into high gear, so have efforts by hackers from Washington's adversaries aimed at disrupting or influencing the vote. One adversary in particular is playing an increasingly prominent role: Iran.

Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA)—warned in a joint statement on Monday.

Stay informed with FP's news and analysis as the United States prepares to vote.

They're not the only ones sounding the alarm. In the past three weeks alone, current and former intelligence officials as well as cyber threat researchers from Microsoft and Google have shared a growing body of evidence of Iran's hacking efforts. As several of them have pointed out, Iran's targeting of U.S. elections isn't new—hackers linked to Iranian security services have attempted to interfere with presidential and midterm races dating back to at least 2018.

However, "Iran perceives this year's elections to be particularly consequential in terms of the impact they could have on its national security interests, increasing Tehran's inclination to try to shape the outcome," the U.S. agencies wrote in their statement. "We have observed increasingly aggressive Iranian activity during this election cycle."

Trump and his acolytes have been particular targets of Iranian hacking, with some former intelligence officials speculating to Politico that efforts to compromise their email accounts could be part of an effort to assassinate U.S. officials in retaliation for the 2020 killing of Iranian Gen. Qassem Suleimani during Trump's presidency.

In their statement on Monday, the FBI, ODNI, and CISA officially blamed Iran for the so-called hack-and-leak operation against Trump's campaign that the campaign made public earlier this month. Those tactics, mirroring Russia's breach of the Democratic National Committee during the 2016 election, are only one part of Iran's election interference efforts along with broader disinformation campaigns aimed at sowing discord among the American electorate.

"Iran, especially because of the past events with Suleimani, they have a marked interest in this election," said retired U.S. Army Col. Candice Frost, the former commander of the Joint Intelligence Operations Center at U.S. Cyber Command. "They have attempted to message on past elections," she said, but "I think this one is almost personal to them."

Iran's relatively elevated profile and more brazen cyber efforts may also be spurred by the ongoing conflict

confrontation with Israel and the U.S. elections," he said. "This made them more proactive in attacking high-value targets that have brought massive visibility to their work."

Iran is not the only adversary officials in Washington are concerned with—election interference efforts by Russia have been extensively documented, and U.S. officials have increasingly warned about China's shift in cyber tactics from espionage to more disinformation and disruptive campaigns. Those two countries remain the prime threats, in large part because their capabilities are relatively more sophisticated.

"Russia and China are really a league of their own," said Frost, currently an assistant professor at Georgetown University's Center for Security Studies. "We oftentimes discount Iran and North Korea, and then you'll have something like the Sony hack or this hack [of the Trump campaign]. So it's not necessarily the level of advancement or competency that they have, but the fact that they kind of found a vulnerability and have been able to exploit that."

"Any nation that has an interest or perceived stakes in the outcome of a U.S. presidential election is going to be thinking about how to influence that outcome," said Gavin Wilde, a senior fellow in the technology and international affairs program at the Carnegie Endowment for International Peace and a former U.S. national security official. "It's easy to point to Russia and China as the most adversarial and the most sophisticated, but every nation around the world has some perceived interest in the outcome, and so I think we need to calibrate along those lines."

Officials and experts say the U.S. government has learned from the missteps of previous elections, particularly 2016, and is better prepared to defend this November's election from cyber threats than it has ever been. Part of that is the shift to publicly calling out adversaries and their activities much earlier in the process and adopting a form of sunlight-as-best-disinfectant strategy, like the ODNI, FBI, and CISA did this week with Iran.

"It's very hard to counter that narrative once it gets into the American psyche and our citizens' spheres of influence," Frost said. "But I do see the focus and calling out [of] this behavior. … That is what we're seeing at a much faster pace, and I give the current intel community a lot of props for doing that early."

But Wilde warned that while U.S. officials are "unquestionably" more prepared this time around, they also now need to be careful about showing their work without inciting panic about elections being compromised. "The tightrope they now have to walk is [being] helpful without creating the very kind of panic that might itself undermine confidence in the election," he said, adding that it's also important to draw distinctions among hack-and-leak operations that have become "a new normal" for political campaigns, election influence efforts that can sometimes be hard to legally define, and actual efforts to interfere with the ballot box itself.

"I think the most consistent thing from all of them is how much it's been a lot of just entrepreneurialism

Rishi Iyengar is a reporter at *Foreign Policy*. Twitter: @Iyengarish