# How to Understand Iranian Information Operations

lawfareblog.com/how-understand-iranian-information-operations

February 19, 2021

Street art in Tehran showing rotary phones with protruding wires. (Flickr/Paul Kellar, https://flic.kr/p/49cnTB; CC BY 2.0, https://creativecommons.org/licenses/by/2.0/)

On Oct. 20 and 21, 2020, just two weeks before Election Day, Iranian actors sent out spoofed emails to thousands of American voters in Florida, Alaska and Arizona. The emails were designed to appear as though they were sent by the Proud Boys, a far-right extremist group, and threatened “we will come after you” if recipients did not vote for Donald Trump. Some of the emails were also accompanied by a link to a video depicting Trump calling vote-by-mail “a terrible thing” and followed by what was made to look like a demonstration of how to fraudulently produce a mail-in ballot. Government officials and cybersecurity experts debunked the video’s demonstration, but the video continued to circulate on social media. Within 48 hours, then-Director of National Intelligence (DNI) John Ratcliffe attributed this disinformation campaign to Iran, alleging that Iran’s purpose was to undermine Trump’s presidential campaign.

In the past few years, Iran has become increasingly sophisticated and active in online communities targeting the American public. And its brazen tactics leading up to the election could mark a shift in the country's influence strategy toward the United States. According to the public record, this is the first time that Iranian actors have engaged in an election interference campaign targeting the United States utilizing stolen voter information in influence operations.

But to the extent that Iran targets U.S. audiences in sustained disinformation campaigns, it still typically aims to broadly promote Iranian interests—such as denigrating sanctions against the country and bolstering their moral standing compared to the U.S.—rather than attempting to induce a specific result in American domestic affairs. More importantly, Iran is almost certainly expending far more of its resources on its geopolitical sphere of influence in the Middle East and North Africa.

As the Atlantic Council's Thomas Warrick notes, Iran's influence activities may not be as much of a shift in strategy as a shift toward using disinformation as a retaliation tactic. Iran has often engaged in symmetric cyber retaliation, responding to both kinetic and cyberattacks with cyberattacks on private and public industry. With this strategy, Iran is able to assert its national power without directly escalating and provoking a military confrontation.

Notably, about a week before the first Proud Boys emails hit Americans' inboxes, Iranian infrastructure suffered two major cyberattacks—one on the electronic infrastructure of its ports and one against an undisclosed target. Regardless of whether the U.S. was behind the attacks, Iran tends to assume some level of U.S. involvement in cyberattacks on its infrastructure. So the spoofed emails that Iranian actors sent a week later may well have been a familiar reflexive response—albeit using cyber-enabled disinformation rather than a more traditional cyberattack.

Alternatively, Iran's brash foray into U.S election interference may have been a sign of Iran's increasing desperation to escape the maximum pressure campaign mounted by the Trump administration by supporting an opposing candidate it believed would be a less aggressive and more predictable adversary. Just days prior to the email scam, the Trump administration reimposed severe sanctions on Iran, including on its financial sector. Cybersecurity experts and Trump administration officials disagreed over the ultimate goal of the Proud Boys email and video, but one aim may have been to target potential voters with a message emphasizing the connection between Trump and right-wing extremism, a narrative Trump himself promulgated when he told the Proud Boys to "stand back and stand by" during one of the presidential debates.

Ahead of the 2020 presidential elections, the Office of the Director of National Intelligence (ODNI) highlighted the threat of election interference by Iran. During and shortly after the 2016 presidential campaign, the ODNI—and a consensus of cybersecurity experts—were concerned primarily with disinformation by Russian actors. But under the Trump administration, the ODNI shifted its public focus toward election interference operations by Iran—and, to a lesser extent, China.

Under Trump, the ODNI's analysis tended to attribute to Iran long-term objectives that most experts see as closer to Russia's. For instance, in a widely covered August 2020 press release, the ODNI announced that China, Russia and Iran were all engaged in influence efforts related to the 2020 election. According to the report, Iran was seeking to "undermine U.S. democratic institutions … and divide the country" whereas Russia was reportedly "using a range of measures to primarily denigrate former Vice President Biden." However, the cumulative evidence of Iran's influence operations indicates that Iran's aim is persuasion in the hopes of achieving a friendlier foreign policy posture from the U.S. and the rest of the world—while Russia's disinformation campaigns are directed more broadly at weakening democratic institutions and dividing the American public.

Indeed, just this past October in its Homeland Threat Assessment, the Department of Homeland Security named Russia the greatest "purveyor of disinformation and misinformation" within the U.S., assessing that Russia's primary objective is to weaken the U.S. by "sow[ing] discord" and "undermin[ing] trust in Western democratic institutions and processes." Some former high-ranking intelligence officials have also indicated that the focus on Iran as opposed to Russia is misplaced. Former DNI Dan Coats's warnings about the threat Russia posed were reportedly watered down by the White House multiple times. And in an interview with NPR this past September, Sue Gordon, the former principal deputy director of national intelligence—the second highest ranking official at the ODNI—remarked that she would have put Russia "first on the list" of election interference threats because of the country's demonstrated interest and capability.

Particularly illuminating about Iran's true influence priorities are a series of investigative reports from Reuters, FireEye and ClearSky Cybersecurity, which uncovered a vast network of inauthentic news outlets and associated social media accounts pushing out Iranian propaganda around the globe. Most of the sites in this particular network were taken offline in October 2020 when the FBI seized 92 domains, which had relied on U.S.-based web hosting services. However, many of the sites operated for several years before then, and their structure and operation still reveal clues about Iran's strategy in the information space and its tactics for promulgating influence worldwide.

All but a few of the inauthentic news outlets concealed their ties to Iran and portrayed their operations as originating in other countries. To help create an appearance of authenticity, fake social media accounts posing as journalists or political figures from a targeted country pushed out content from a news website to audiences in that country. However, all of the sites published stories generated by the International Union of Virtual Media (IUVM) and the Islamic Radios and Televisions Union (IRTVU)—two media operations sanctioned by the

Treasury Department in October for being controlled by the Islamic Revolutionary Guard Corps—which was itself controversially designated as a foreign terrorist organization by the State Department in April 2019.

Many of the sites also stole articles from legitimate news outlets, including Reuters and the Associated Press, as filler to make the news sites appear genuine. Some of these stolen articles were altered slightly to portray Iran's adversaries in a poor light. Other content was copied from Iranian state media and used as propaganda to bolster Iran's profile on the national stage. Of the 70 websites that Reuters uncovered and the 98 identified by ClearSky, the greatest number targeted Yemen, Syria and Afghanistan. Dozens of others targeted the Middle East and North Africa (MENA) region more generally, where Iran is locked in a struggle for influence with Saudi Arabia.

This campaign seems to have been broadly aimed at spreading stories around the world that uplift Iranian culture and the Iranian regime and generally denigrate Saudi Arabia, Israel and the United States. For example, Nile Net Online, which purported to be an Egyptian news outlet operating out of Tahrir Square, published several stories criticizing Cairo's relationship with the Trump administration. Other sites targeting Muslim majorities in northern African countries, where Iran and Saudi Arabia are fighting for influence, highlighted Saudi Arabia's killing of the journalist Jamal Khashoggi and criticized its military intervention in Yemen's civil war. Unlike Russian disinformation, which often aims to create confusion and chaos, this massive Iranian influence campaign demonstrates that Iran's propaganda is aimed at strategic persuasion.

Iran also invests heavily in projecting its traditional state media into other Middle Eastern countries, where many audiences are more likely to watch television than access the internet. For example, Iran broadcasts to Arabic speakers across the MENA region with its Al-Alam station, to Spanish speakers in Latin America with HispanTV, and to English speakers around the world with Press TV. These outlets are openly run by the Iranian government and could be properly classified as public diplomacy, in the vein of the U.S. government outlets Voice of America and Radio Free Europe. However, these outlets have also been found to intertwine false stories with real ones, mixing misinformation with its public diplomacy.

Even though many countries and regions where these stations are broadcast hold little immediate strategic value to Iran, the regime continues to invest in maintaining a media presence in order to promote Iran on the world stage and combat negative media broadcasts by Iran's adversaries. However, Al-Alam, HispanTV, and Press TV are all overtly tied to Iran and are therefore vulnerable to U.S. measures to diminish their reach, including designations and sanctions.

More covertly, Iran also spends significant resources funding pro-Iranian television stations in other countries that are nominally independent. For example, Iran provides funding to at least four Afghan television stations that create pro-Iranian content, according to one Rand

Corp. report. Iranian influence over these stations is so prominent that Persian words and Iranian expressions are used even in otherwise Pashto-language programming. Two stations in particular—Tamadon TV and Noor TV—have been criticized by Afghan officials and citizens for their entanglement with Iran. Although both have denied any association with the Iranian government, Afghan intelligence publicly accused both of receiving Iranian support. Additionally, both Noor and Tamadon are members of the IRTVU—one of the entities sanctioned by the Treasury Department in October—according to IRTVU's website. Although IRTVU does not discuss direct funding on its website, privileges of membership include benefiting from unspecified IRTVU services and participation in media training and news exchanges.

Iran's on- and offline influence operations and propaganda suggest that its global information strategy had little to do with dividing the American public to electioneer in the November U.S. presidential race as the ODNI suggested, despite the apparent attempt to scare Americans with the Proud Boys email scam. Of course, Iran has also leveraged narratives that are politically divisive in the U.S., but the purpose is almost always to impugn the reputation of the country's greatest adversary before a global audience. Unlike Russia, which often creates fake personas taking both sides of an issue to amplify discord and distrust among Americans to undermine democratic institutions, Iranian personas tend to take one side of an argument and attempt to persuade a global target audience from that position.

During the summer of 2020, for example, Supreme Leader Ali Khamenei publicly supported Black Lives Matter in the wake of George Floyd's killing by Minneapolis police officers. Iran's purpose in supporting this movement was not to turn Americans against each other but, rather, to denigrate the U.S. government before the American people and the world by accusing it of interfering with other nations around the world while perpetuating injustice at home. This narrative was apparent from Ali Khamenei's tweets saying, for example, that domestic protests represent "all nations against which the US has committed many atrocities" and "[t]he people of the United States have every right to feel embarrassed and ashamed by their govts, particularly the current govt." Iran's adoption of a single narrative that directly attacked the U.S. government and U.S. authorities rather than attacking groups of U.S. citizens or taking multiple sides on the issue suggests that its purpose was persuasion rather than division.

What approach might the ODNI take to Iranian information operations under the Biden administration? Senators on the Intelligence Committee have indicated they are eager to work with the current DNI, Avril Haines, to establish more neutral reporting led by rigorous tradecraft. A report by the ODNI's analytic ombudsman from early January gives some indication of how the agency could publicly report on election interference and reform its internal leadership and tradecraft processes. The report, requested by the Senate Intelligence Committee leadership and delivered on Jan. 6, found that internal politicization of the agency's election interference intelligence led to biased public reporting on Russian and

Chinese interference efforts. Although reporting on Iran was not specifically addressed, the report’s broad recommendations for reforms from senior agency leadership to line analyst tradecraft policies would likely improve the agency’s public reporting on Iran as well.

Tags:

- Information Operations