asd
G|M|F

Iran's Authoritarian Playbook

The Tactics, Doctrine, and Objectives behind Iran's Influence Operations

Ariane M. Tabatabai

Please direct inquiries to
The Alliance for Securing Democracy at
The German Marshall Fund of the United States
1700 18th Street, NW Washington, DC 20009
T 1 202 683 2650
E info@securingdemocracy.org

The full report can be downloaded for free at https://securingdemocracy.gmfus.org/irans-authoritarian-playbook/

Alliance for Securing Democracy

The Alliance for Securing Democracy (ASD), a bipartisan initiative housed at the German Marshall Fund of the United States, develops comprehensive strategies to deter, defend against, and raise the costs on authoritarian efforts to undermine and interfere in democratic institutions. ASD brings together experts on disinformation, malign finance, emerging technologies, elections integrity, economic coercion, and cybersecurity, as well as regional experts, to collaborate across traditional stovepipes and develop cross-cutting frameworks.

Author

Dr. Ariane M. Tabatabai is the Middle East Fellow at the Alliance for Securing Democracy at the German Marshall Fund of the United States and an adjunct senior research scholar at the Columbia University School of International and Public Affairs (SIPA). She is also a Truman national security fellow and a Council on Foreign Relations (CFR) term member. Prior to joining GMF, Tabatabai served as an associate political scientist at the RAND Corporation, the director of curriculum and a visiting assistant professor of security studies at the Georgetown University Edmund A. Walsh School of Foreign Service, and an international civilian consultant for NATO. Previously, Tabatabai was a post-doctoral fellow in the International Security Program and a Stanton nuclear security fellow in the International Security Program and the Project on Managing the Atom at the Harvard Kennedy School's Belfer Center for Science and International Affairs where she was also an associate. She is the author of No Conquest, No Defeat — Iran's National Security Strategy (Oxford University Press) and the co-author of Triple Axis: Iran's Relations With Russia and China (I.B.Tauris). She has published widely in academic, policy, and mainstream outlets, including International Security, the Journal of Strategic Studies, The New York Times, The Washington Post, The Atlantic, Foreign Affairs, and Foreign Policy. Tabatabai holds a Ph.D. in war studies from King's College London and is a native French and Persian speaker.

Introduction

According to a 2013 indictment by the U.S. Department of Justice, hackers backed by a foreign power gained access to the controls of the Bowman Avenue Dam, a small dam in the New York City suburb of Rye, New York. Cyberattacks on infrastructure have long been a concern in the United States: Russia has targeted the U.S. power grid and other critical infrastructure in the past—at times successfully.[1] Hackers backed by the People's Republic of China have targeted U.S. utilities companies.[2] However, neither of these strategic adversaries was behind this bold foray into U.S. suburbia: the culprit, according to the indictment, was the Islamic Republic of Iran.[3]

Over the past decade, Iran has emerged as an important national security challenge for the United States. A novel part of the regime's effort—facilitated by the advent of the information age and new technology—is its development of a playbook and toolkit designed to undermine the United States at home just as, in the eyes of Tehran, Washington does in Iran. This makes the current Iranian challenge more subtle and nuanced than has been the case for most of the Islamic Republic's existence. Iran has gradually expanded its capabilities to compete against the United States for influence within the region, and it is now also taking this competition into the United States and even Europe.

One hundred days before the 2020 U.S. elections, the Office of the Director of National Intelligence put a fine point on this threat when National Counterintelligence and Security Center Director William Evanina released a statement noting that, "at this time, we're primarily concerned with China, Russia and Iran," who are all looking to "use influence measures in social and traditional media in an effort to sway U.S. voters' preferences and perspectives, to shift U.S. policies, to increase discord and to undermine confidence in our democratic process."[4] The statement characterized the Iranian threat as follows: "Iran seeks to undermine U.S. democratic institutions and divide the country in advance of the elections. Iran's efforts center around online influence, such as spreading disinformation on social media and recirculating anti-U.S. content."[5]

The Islamic Republic's authoritarian toolkit is unlikely to become as sophisticated as that of China or Russia in the near-term. After all, Iran's economy is in shambles, its capacity restrained, and the model of society and governance it tries to offer profoundly limited in its appeal. And even the flagship tool used by Iran to interfere in democracies, namely its online influence operations, continues to suffer from such basic shortcomings as misspelled names, the repeated use of the same tactics and techniques, and a lack of proper research into the target and familiarity with its behavior.[6] However, a perceived existential threat posed by the United States, an inability to match the conventional capabilities of the United States and its allies, and a strong desire to compete with the same, have encouraged Iran to double down on efforts to develop a set of asymmetric tools allowing it to overcome its shortcomings. In this sense, Iran is not dissimilar to Russia. "Authoritarian learning" (including partnerships with both Beijing and Moscow) has likely helped Tehran to overcome challenges and to develop its toolkit quickly and effectively.

The result is that Iran is becoming a significant authoritarian actor challenging democracy in the United States and Europe. Tehran's influence operations span traditional and digital media. The regime has built a sprawling web of traditional media outlets, as well as networks of accounts on all major social media platforms (even as it bans and limits access to these websites at home), allowing it to reach millions of users abroad. The content Iran creates, distributes, and amplifies is multilingual and seeks to adapt to democracies' social, cultural, and political contexts—with fairly mixed results. Among the objectives of Iran's information manipulation efforts are sowing tensions in democracies, dividing democratic nations internally and from each other, and alleging hypocrisy in democratic states' foreign policies, undermining democratization in Iran and elsewhere. Iranian hackers routinely target U.S. persons, academic institutions, companies, non-profit organizations, and government agencies and departments. And Iran's illicit finance schemes are considerable; although, they are currently focused on

sanctions evasion and support of information operations, rather than used as a standalone vector to undermine democracies.

Some of these tools and the tactics used by Iran are similar to those employed by both Russia and China—and both Beijing and Moscow have lent Tehran a hand in developing some of its capabilities,[7] particularly in the realm of information manipulation. Iranian, Russian, and Chinese state media and associated social media accounts echo and amplify each other's messaging. But there are also some differences in how Tehran deploys these tactics. This is in part due to differences in the political culture and structure of the country, the Islamic Republic's own ideology and worldview, and the country's status in the international system. Another significant set of differences arises from Iran's shortcomings vis-à-vis both its adversaries (including the United States) and its authoritarian partners in Russia and China. For example, Russia and China can leverage their vast nuclear arsenal and enormous economic weight, respectively, to compete directly with the United States. Iran is ill-equipped to compete with the United States in either of those domains and, as such, sees this set of tools and efforts to undermine democracy as a means to elevate its level of competition rather than an end in itself. Hence, Tehran's toolkit is more limited than those of Beijing or Moscow, leading the Islamic Republic to be more deliberate and selective in the programs it develops and, perhaps, more forceful in how it deploys them. As a result, though Iran's growing efforts to undermine democracy should not be ignored and should be addressed adequately, for now, the Islamic Republic remains a lesser threat than China and Russia.

This report tries to make sense of these activities and provide a framework for understanding Iran's intentions and capabilities. It provides one of the first comprehensive discussions of Iran's authoritarian toolkit, doctrine, and objectives. It must be noted that unlike other key Iranian initiatives—such as its nuclear program, missile activities, support for non-state actors, and regional interventions—Iran's authoritarian toolkit remains scarcely studied in the academic literature. Understanding Tehran's objectives in undermining democracy and the means it leverages to do so is important for a few reasons. First, Iranian activities over the past few years have shown that the regime is increasingly active in this space. And as Iran's objectives and the tools it employs are different from those of other key malign actors, understanding their strengths and weaknesses and developing specific responses to them is a worthy exercise. Second, authoritarians learn from each other, and observing the Iranian case allows us to better identify the trends and comprehend the ways in which less powerful malign actors (as opposed to Russia and China, for example) may engage in similar activities designed to unde rmine democracy.

Methodology

This report cites primary and secondary sources from the U.S. government, including unclassified and declassified U.S. intelligence reports and other publications, and uses the existing literature on the topic and news articles as sources. Moreover, this report leverages the Alliance for Securing Democracy's (ASD) Hamilton 2.0 dashboard, which tracks Iranian, Russian, and Chinese information manipulation efforts, equipping researchers with the tools to study the three countries' official statements, state media reporting, and social media activities.

At present, the academic literature on Iran's efforts to undermine democracy is limited, as are primary Iranian sources on the topic. Given their often covert and sensitive nature, the regime rarely makes its white papers, memos, and other products available to the public. Much of the open source reporting and analysis is produced by journalists, think tanks, and technology companies. As such, although we consult the academic literature to make sense of broader Iranian objectives and doctrine and to situate the country's efforts in the context of broader authoritarian learning and resilience, we rely heavily on news articles, as well as research and analysis conducted by news organizations, think tanks, and tech companies. We also use Iranian media and social media activities.

The report proceeds as follows. First, it will provide an overview of Iranian objectives to make sense of its intentions before analyzing the Iranian toolkit. Next, it assesses the strengths and weaknesses of Iran's approach.

Finally, it closes by contextualizing the findings in terms of authoritarian learning and resilience, surveying U.S. vulnerabilities, and offering recommendations for addressing the gaps in democracies' capabilities. The appendix identifies the key actors involved in developing and implementing Iran's strategy.

Iranian Objectives

Although U.S.-Iran dynamics since the 1979 establishment of the Islamic Republic have been punctuated by a few moments of tacit cooperation, the two countries' relationship has predominantly been marked by deep distrust and hostility. The nascent regime was in its infancy when a group of hardline revolutionaries took over the U.S. embassy in Tehran and held its personnel hostage for 444 days. For Americans, the image of this new Iran was formed during that period: the U.S.-aligned forward-looking government was gone and replaced by a reactionary theocracy. Later, Tehran's support for various terrorist groups, including elements who perpetrated the 1983 Marine barracks in Lebanon, as well as the Iraqi Shia militias whose road-side bombs and improvised explosive devices killed some 600 Americans in the 2000s, further fueled U.S. distrust of Iran, as did the country's pursuit of nuclear capabilities (in violation of its international obligations under the Nuclear Nonproliferation Treaty).

From Iran's perspective, the hostilities did not start in 1979. They simply began to play out on Tehran's terms then. Iranians point to the 1953 coup toppling then-Prime Minister Mohammad Mossadeq, aided by the U.S. Central Intelligence Agency (CIA), as the onset of hostilities. In fact, as some Iranians see it, the hostage crisis was their response to the United States' history of meddling in their country's internal affairs. Next, Iranians point to U.S. support for Saddam Hussein's war effort against Iran—a war initiated by Baghdad and which lasted from 1980 until 1988, killing several hundred thousand combatants and civilians on both sides. Most recently, Iranians argue that decades of U.S. sanctions have hurt the country's economy and civilian population, and that several U.S. administrations have sought to topple the Iranian regime, as the Iranian Ambassador to the UN Gholamali Khoshroo accused the United States of doing in a letter to the UN Secretary General in 2017[8].

This perception is particularly salient within the conservative elements of the regime even though it does not accurately reflect the changes in U.S. policy toward within the past four decades. And, as with other authoritarian regimes, Iran's leaders see the United States' soft power as a major threat dividing the regime from the population. The regime's response is to censor U.S. media outlets, books, movies, music, and other artistic products, ban key social media platforms, and generally deny the population the ability to access U.S. cultural exports that are viewed as "corrupting" and, therefore, dangerous to regime survival. The country's highest authority, Supreme Leader Ayatollah Ali Khamenei, has, for example, warned against the importation of U.S. goods,[9] and authorities in Tehran have gone so far as to shutter a counterfeit Kentucky Fried Chicken for fears of U.S. influence.[10]

Many Americans may view the history of U.S.-Iran tensions and the narratives thereof as an esoteric academic exercise. However, they are relevant in shaping Iran's efforts to deploy its authoritarian toolkit against the United States and like-minded democracies. From the U.S. perspective, Iran is not considered a near-peer competitor like Russia and China in terms of the challenge it presents to national security. But from Iran's viewpoint, the United States is a critical national security threat.[11] The United States' nuclear arsenal, conventional military capabilities (including in Iran's own immediate neighborhood), political stature (encompassing a vast network of allies and partners), and economic prowess (entailing the ability to sanction countries and heavily enforce these sanctions) make Washington an impressive—and perhaps even existential—foe.

To respond to this challenge, and having largely depleted its pre-revolution conventional capabilities (acquired by the Shah with significant U.S. help), Tehran has invested in asymmetric tools that it can leverage to deter, defend against, compete with, and counter its adversaries. Iran seeks to respond to what it perceives as adversarial threats and actions in kind—thus frequently opting for a calculated and calibrated strategy. As is the case with asymmetric operations conducted by authoritarian regimes like Russia, leveraging such means and tactics also allows Iran to maintain its operations below the threshold of conventional conflict and, often, to execute them with plausible deniability, thus making it more difficult for the United States to respond in conventional terms.

In that context, the Islamic Republic has developed a toolkit that affords it the ability to counter U.S. policy aimed against Iranian interests at low cost and low risk. Indeed, Iranian decision-makers and military planners believe that their country is currently at war with the United States, a conflict they describe as "war by other means" (playing on the Clausewitzian definition of war as the continuation of politics "by other means").[12] From their perspective, these U.S. means include:

- Economic and financial tools—predominantly economic sanctions;
- Political and information warfare—such as public diplomacy and official U.S. government messaging designed to demoralize Iranians and support citizen journalism; isolate Iran and galvanize the international community to exercise pressure on the regime; heighten gender, ethnic, religious, and political divisions within the country; and support civil society and protests in the country, such as the 2009 Green Movement;[13]
- Cyber warfare—through such efforts aiming to stymie Iran's nuclear progress as exemplified by Stuxnet;
- Covert intelligence operations—including efforts to gain access to sensitive national security material, as well as the targeted killings of Iranian and allied figures (most notably the January 2020 killing of Maj. Gen. Qassem Soleimani and a significant Iraqi Shia militia leader and close friend of Iran, Abu Mehdi al-Muhandis).

In response, Iran has developed its own toolbox—elements of which it also shares with its proxies to serve as force multipliers and to add a layer of plausible deniability when needed.[14] Although from Iran's perspective the responses it formulates to these U.S. actions can be equated, in reality, there are significant differences between the two. It is important to distinguish Iran's asymmetric toolbox from the realm of accepted nation-state behaviors described above. Overt public messaging attributed to democratic governments, economic policy transparently implemented by democratic governments, and the traditional methods of intelligence collection and use of cyber tools for military purposes conducted by nation-states are often considered within the bounds of traditional statecraft. The asymmetric activity conducted by Iran—and other authoritarian states like Russia and China—are, as described earlier, often obfuscated to avoid attribution in order to undermine and destabilize the functioning of democratic institutions.

As former deputy commander of U.S. Cyber Command Vincent Stewart aptly characterized when he testified before Congress shortly after Soleimani's death, "Iran's asymmetric warfare can be viewed as a three-legged stool comprising support to malign actors and terrorists, information operations, and a range of cyber activities. All of these components are part of a long-term campaign to make the U.S. cost of staying in the region untenable while eroding support for the U.S. and avoiding the threshold for an overt U.S. military response."[15]

This paper focuses on specific Iranian actions designed to weaken the United States and like-minded democracies in order to level the playing field between a conventionally and economically weak Iran and what it views as one of the greatest threats to its own national security. In part, what Iran tries to achieve is to expose what it characterizes as democracies' hypocrisy in their treatment of international affairs, thus undermining their efforts to encourage democratization beyond their borders. By exposing its flaws and undermining democracy in general, authoritarian regimes like Iran are also able to dissuade their own populations from seeking alternatives to their systems. Hence, competing with and undermining democracy are not simply geopolitical considerations for actors like Iran, but also a means to prevent dissent at home and to ensure regime survival. As we will see later, whataboutist narratives are a core pillar of Iran's messaging and disinformation.

In addition to this more long-term objective, Iran (like Russia and China) also has a number of short- to medium-term proximate interests it pursues, which include directly deterring, defending against, responding to, and countering policies it views as damaging to its own national and regime interests, including U.S. and European political pressure and economic sanctions. The following sections offer an overview of Iran's doctrine.

Doctrine

Although it is often grouped with Russia and China (and it certainly learns from and cooperates with them), Iran is in somewhat of a different category from the two powers.[16] Russia and China are considered near-peer competitors for the United States—albeit in different terms. (For example, Russia is a near-peer competitor in the nuclear realm though its economy is no match for that of the United States, while China is an economic challenger whose nuclear forces and military capabilities are significantly less substantial than those of United States). Iran, however, is squarely outside this category. Tehran is well aware of its shortcomings vis-à-vis the United States and other U.S.-aligned democracies.

Iran has calibrated its objectives and efforts accordingly. Hence, Russia and China may have grander ambitions when meddling in democracies' politics and societies, and the scale of their operations is larger than those of Iran. Conversely, Iran appears to have more modest objectives, and though its capabilities appear to be growing, they remain more limited than those of Russia and China. For example, as discussed further, Iran's online influence operations are more circumscribed than those of the two major authoritarian players. The drivers behind Iran's efforts pertain more directly to the regime securing its interests as it sees them rather than offering a viable alternative model for outside consumption. Nevertheless, many of these interests also overlap with those pursued by Russia and China. The following are Iran's key interests, which shape the contours of its efforts to undermine democracy in the United States and Europe:

- Undermining the U.S. narrative on Iran internationally and presenting itself as a responsible member of the international community wrongfully targeted by the United States. By doing so, Tehran hopes to undermine U.S. efforts to isolate it politically and economically, preserve political and trade partners even as Washington seeks to disrupt Iranian engagement with other countries, prevent the United States from using international fora, chiefly the United Nations, as venues where it can hold Iran accountable.
- Promoting Iran's revolutionary ideology.
- Sowing discontent and creating and exacerbating tensions between the United States and its allies and partners. This makes it harder to create consensus on or build coalitions to counter Iran (Iran implemented this tactic in the aftermath of the U.S. withdrawal from the nuclear agreement[17] to further widen the gulf between the United States and its European allies and to raise the costs of the reimposition of sanctions by Washington).

Unlike China and Russia, Iran does not make most of its doctrinal and strategy documents publicly available. Hence, our ability to access such material in the open source is limited. To the extent that Iran publicizes such documents, it does so in short excerpts as part of reporting by media organizations close to key power centers (such as the Islamic Revolutionary Guards Corps (IRGC)) and in the statements made by political figures and military commanders. Generally, these pertain to Iran's overt military programs and activities, such as missile defense. Broadly speaking, Iran's military doctrine emphasizes deterrence and defense over offense. However, as Iranian military commanders have long noted in terms of the country's military activities, "the best defense is a good offense"—a mantra that the regime in general and the IRGC in particular appear to have embraced when it comes to undermining democracy.[18] Given its limited conventional capabilities, the regime sees its asymmetric toolkit as operating in lieu of conventional military power, serving to deny the adversary (in this case, chiefly the United States) the ability to impose costs on Iran for its actions and foment dissent within the country.

The regime has clearly placed cyber activities and information manipulation as top priorities in its doctrine. As a report published by the IRGC-linked news website Mashregh News explains, diplomacy is no longer limited to government-to-government relations.[19] Instead, the public is now a battleground for states' diplomatic outreach efforts, and a significant part of the state's diplomatic efforts are conducted by the government of a given country with the population of another country as the target audience.[20] On the surface, the report merely describes how

states conduct "public and cyber diplomacy," as it calls them (the latter is a term used to refer to what we consider to be information manipulation). However, the report is significant in that it both provides an overview of what IRGC affiliates see as adversarial efforts against Iran, as well as possibly providing a blueprint for Iran's own efforts in this space by pointing to the threats the organization believes it has to counter. The report lays out the different ways in which public diplomacy and cyber diplomacy are conducted, including:

- Influencing the thinking of political leaders;
- "Controlling the social behavior" of the populace by affecting public opinion (including by "directing public opinion via [the use of] international media," which can be leveraged to legitimize the state's worldview and actions in other societies, and in the cyber realm);
- Using cyber tools to make contact with the nationals and residents of a given country directly in an organized manner, or indirectly via channels operating under the guise of civil society activism;
- Creating movements and organizations that lack transparency and accountability and which can spread disinformation;
- Eroding self-determination through the establishment of new entities providing a cover for governments involved in other states' political ecosystems.

The report offers several recommendations designed to both help Iran prevent adversaries from successfully undertaking these actions while also becoming more competitive in this realm. These include increased government control over the Internet and the creation of a national Intranet (or "Halal Internet")—a project initiated in 2011 by the Iranian government; cooperation with academia and private tech companies; and increasing Iran's presence in the cyber space, including in terms of its official presence. It highlights the importance of Tehran adopting an offensive posture to both deter adversaries and to weaken them. It suggests that Iran's best options are to create cyber channels on every level—tribal and ethnic, regional, and international—to be able to "direct social movements against the adversary and to prevent it from attacking."[21] The document points to the need for some centralization: it suggests that centralization is critical in terms of command and coordination, but crucially (and in line with Iran's general doctrine) it allows for flexibility and a degree of decentralization in the control and implementation.[22]

Particular attention appears to have been paid to social media engagement; in particular in the 2017-18 timeframe, Iran appeared to be considering how to increase its information manipulation efforts. As discussed further in the following sections, 2018 saw the highest number of Iranian official accounts created on Twitter. Half of Iran's current official accounts operating on the platform were created that year. Prior to that uptick, Mashregh published a report considering the diplomatic presence of other countries on social media platforms, pointing to Facebook and Twitter as the most popular such websites for foreign diplomats; although, a number of key Iranian officials and organizations also have an active presence on platforms such as Instagram, WhatsApp, Telegram, and YouTube to name a few.[23] Social media platforms are preferred tools for Iran given their "simplicity and flexibility" in terms of the lack of specific time and space limits, as well as the low cost.[24] Another appeal of social media platforms is that Iran is able to reach several audiences in a much more effective way.[25] Given the state of the country's economy under sanctions, Iran privileges the use of low-cost means that provide it with the maximum outcome. Beyond information operations (starting in the 2012 presidential elections), Iran's attempts at interfering in U.S. elections have remained more modest; although, on at least several occasions Iran-linked actors have sought to hack U.S. campaigns.[26] To the extent that Iran has sought to interfere in U.S. elections, it has done so with the aim of sowing divisions between Americans and exacerbating partisanship in the United States, increasing racial and other tensions within the country, and elevating candidates deemed more "friendly" toward Iran at the expense of those perceived more hostile.

Iran's willingness and ability to be more active in election interference in the United States may change as its capabilities grow and its interests appear more directly at stake. In 2016, the Islamic Republic seemed more ag-

nostic about the outcome of the U.S. presidential election. Democratic candidate Hillary Clinton was known to the Iranians given her long track records in U.S. politics, in particular for her role as the former secretary of state whose team had initiated negotiations over the Iranian nuclear program in 2012. Clinton was seen as "tough" on Iran.[27] During that cycle's Democratic primary elections, Iranian-linked accounts briefly sought to boost Sen. Bernie Sanders' campaign.[28] Clinton's rival, the Republican nominee Donald Trump, did not have a history in politics to indicate how he would position himself on Iran policy. And although he often denounced the Joint Comprehensive Plan of Action (JCPOA) on the campaign trail, pledging to withdraw the United States from the agreement, Iran viewed the future U.S. president as a businessman who would act pragmatically—more so than Clinton, whom the regime the regime saw as an ideologue.[29] For example, some regime-linked analysis went as far as playing down Trump's threats to withdraw from the JCPOA.[30] Hence, Tehran was likely more agnostic about the fate of the 2016 elections.

In 2018, Tehran was among the foreign actors seeking to interfere in the U.S. midterm elections.[31] Iran's activity during that period appears narrowly focused on online influence operations, which remained less sophisticated than those of Russia and tended to focus on the regime's immediate policy concerns and objectives, with its messaging concentrated on one side of a given policy debate and issue—in contrast to the Russian efforts, which attempt to reach all sides of the debates.[32] Twitter alone shut down over 7,000 fake accounts and sock puppets linked to Iran that year, and some, such as "@AliciaHernan3," tweeted content related to the 2018 elections, as reported by The Washington Post.[33] Iranian actors did not limit their social media activity to impersonating American voters, however. They also created spoof accounts impersonating American political candidates, including a Republican from California running for Congress.[34]

Since then, Iranian operatives have created fake accounts posing as political figures in Europe as well as the United States. On two occasions in 2019, Twitter took down fake accounts impersonating high-level French officials. One case involved President Emmanuel Macron's Chief of Staff Alexis Kohler. The fake account had posted material about Iran—particularly content pertaining to the Mujahedin-e Khalq (MeK).[35] The tweets had falsely claimed that France would expel MeK members from its territory—a move that Iran would welcome. Iranian state media also amplified the fake news.[36] The second case involved the French consul general to Israel, Pierre Cochard. The fake Twitter account had claimed that the MeK's leader, Maryam Rajavi, was set to visit Israel on a trip facilitated by President Trump's personal lawyer, Rudy Giuliani.[37] Rajavi, the tweets further alleged, would be meeting with Israeli Prime Minister Benjamin Netanyahu and Yossi Cohen, the director of the country's intelligence service, Mossad.[38]

In addition to social media activity, Iran-linked actors also reportedly targeted traditional media outlets. Newspapers in Virginia and Texas appear to have published letters that were part of Iran's influence operations.[39] Looking ahead to the 2020 presidential elections in the United States, the intelligence community included Iran (along with Russia and China) would potentially interfere in the elections either through "the voting process or [by] influenc[ing] voter perceptions."[40] It is not clear whether Iran's efforts will follow the same pattern as that of previous elections, in which they mostly focused on information manipulation rather than attempting to use cyber tools to manipulate the voting process itself. In 2018, Iran's efforts may have been limited to the information realm due to the fact that the elections were midterms and not presidential and, therefore, less consequential from the perspective of Iran's leaders.

Nevertheless, Iran's influence operations are likely to grow in their sophistication and, perhaps, even their scope. For example, as technology companies discover and take down Iranian accounts, the operatives behind these efforts also learn from their shortfalls and mistakes and rectify them as they create new accounts and undertake new efforts—though, as noted previously, Iran has been slow to implement these lessons learned, creating a key vulnerability in its operations. Moreover, Iran appears eager to diversify its means of interfering in elections. So far, in the 2020 election cycle, the regime has adopted a third mean of interfering in the elections by attempting

to hack U.S. presidential campaigns—in this case, President Trump's campaign (though it is not clear yet whether Iran's intentions were traditional espionage or to gather and leak information in an attempt to interfere in the elections). In 2019, Microsoft revealed that Iran was tied to an attempt to breach email accounts belonging to President Trump's reelection campaign.[41] In 2020, Google also reported that Iran-linked hackers had made similar attempts to hack the Trump campaign.[42]

Like Russia, Iran is able to break and enter into computer systems to find and leak sensitive information. Moreover, although much of Iran's 2019-2020 kinetic efforts in Iraq, the Persian Gulf, and the Arabian Peninsula (as well as the timing and intensity of peaks and lulls in these activities) can be attributed to the Trump administration's killing of Soleimani and a maximum pressure campaign against the regime, they may also be attributed in part to a desire to influence the outcome of the 2020 elections.[43] As was the case during the 1979-81 hostage crisis, foreign affairs can directly or indirectly shape the outcome of U.S. elections. Understanding this, Tehran may be using violent tactics (or a pause in such activities) in the Middle East and elsewhere to further divide Americans and potentially sway their votes (as it did when the regime took American hostages and targeted Americans in the region). Nevertheless, the most significant element of Iran's election meddling efforts continues to lie in its information operations.

The Toolkit

Cyber Activities

Cyberattacks have emerged as one of both Washington and Tehran's preferred tools throughout the past decade—although U.S. targets are military in nature and much more limited in scope. U.S. cyberattacks against Iranian targets tend to fall in the accepted realm of those permissible in state-to-state competition in the context of intelligence and military activities while Iran, as will be discussed throughout this section, has adopted a wide range of targets. Perhaps the most significant such action attributed to the United States was Stuxnet, which targeted Iran's uranium enrichment program in the late 2000s and early 2010s. More recently, the United States opted for a cyber response to the Iranian attacks on Saudi oil facilities in 2019.[44]

For its part, Iran (like other authoritarian actors) also sees cyberattacks as a low-cost way to take action against the United States and other countries deemed significant to Iranian interests, including in Europe, as they are less likely to provoke a response.[45] Historically, Iran's cyber activities have been largely focused on intelligence operations, as well as defensive and offensive actions against U.S. government targets, rather than on undermining U.S. democracy—though, as discussed throughout this section, that has started to change. As noted previously, Iran's military doctrine in general and its authoritarian playbook in particular are flexible and adaptive, and cyber space is no exception. Iran has expanded its cyber capabilities over the past decade. Two key events drove Tehran's decision to invest heavily in this domain. In addition to the aforementioned Stuxnet incident, the 2009 contested and fraudulent presidential elections (leading to a second term for the controversial hardliner President Mahmoud Ahmadinejad) shaped the regime's thinking in the cyber realm. Since then, key power centers (the IRGC chief among them) have developed the country's capabilities, making it one of the most important state actors presenting cyber challenges for the United States. To maintain its edge, Iran switches up its methods, rotates members of its groups, and retires malware as it becomes identifiable.[46]

As then-Director of National Intelligence Dan Coats noted in 2019, "Iran uses increasingly sophisticated cyber techniques to conduct espionage; it is also attempting to deploy cyber attack capabilities that would enable attacks against critical infrastructure in the United States and allied countries."[47] Moreover, the intelligence community assessed, "Iran has been preparing for cyberattacks against the United States and our allies. It is capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017."[48] This assessment may change as Iran's capabilities grow and its intentions shift. For example, Iran may now be able to inflict more long-term harm to democratic institutions than it was able to do previously.

As Michael Eisenstad has written, Iran's interest in cyber tools is not surprising as they fit neatly into its strategic culture. This entails:

> A preference for ambiguity, standoff, and indirection when conducting potentially high-risk activities—enabling it to better manage this risk. Second, international cyber norms remain inchoate, providing Iran with margin for maneuver in this domain. Third, Iran hopes to shape these emerging cyber norms, so that its cyberspying and offensive cyber operations become a tolerated form of behavior, much as its use of terrorism is tolerated by many members of the international community. Iran also uses cyber to demonstrate U.S. impotence in the face of Tehran's defiance of Washington.[49]

Iran's cyber activities can be separated into two categories: 1) those activities that fall in the traditional realm of intelligence and military operations, and 2) those malign activities designed to undermine democracy that fall outside the realm of broadly accepted intelligence and military practice. Actions in the first category are designed

to infiltrate U.S. government agencies and departments, obtain classified information and sensitive material pertaining to U.S. national security, and cultivate and recruit Americans viewed as willing and able to cooperate with Iran to counter the United States.

Examples of successful Iranian operations include hacking the U.S. Navy email server in 2013.[50] Iran reportedly targeted the U.S. military, hacking an unclassified Navy computer network, as nuclear negotiations between the two countries (as well as six other parties: China, Russia, France, Germany, the United Kingdom, and the European Union as a separate entity) were ongoing. As a Wall Street Journal report noted, though the United States did not "believe Iranian agents stole information of significant value, [...] the incident sparked concerns within the Pentagon because it showed a more potent Iranian hacking capability than previously believed and suggested the Iranians have the ability to access military data."[51] Just a year prior, the United States "considered Iran's capabilities unimpressive."[52]

Although the initial contact and grooming of former U.S. Air Force intelligence specialist Monica E. Witt appear to have been largely done with more traditional means, cyber tools were instrumental to Iran's project once it had successful recruited Witt.[53] The intelligence provided by Witt helped Iran target other U.S. intelligence officials for surveillance purposes—including by creating fake Facebook profiles and emails with malware. The operations were allegedly conducted by Behzad Mesri and a group of hackers. Mesri has also been accused of breaking into HBO's computer system to steal unreleased episodes and material for the network's flagship show "Game of Thrones." Mesri demanded $6 million to refrain from releasing the material; although, he does not appear to have undertaken this effort on behalf of the Iranian government but rather as a free agent.[54]

The second category involves operations that target U.S. government agencies, as well as academia, think tanks and other NGOs, companies, and international organizations.[55] In 2018, media reports revealed that Iranian hackers had stolen research from some 320 universities, companies, and government agencies (including five U.S. government agencies and 30 U.S. companies) over the course of five years. Among these institutions were a biotechnology company, 11 technology firms, and a number of academic publishers, while the government agencies affected were the Federal Energy Regulatory Commission and the Department of Labor, along with the states of Hawaii and Indiana.[56] The monetary impact of these efforts was reportedly a $3.4 billion cost to these institutions in terms of "procedure and access."[57] In 2020, amid the race to develop treatment for the coronavirus, Iran-linked hackers targeted the U.S. drug making company Gilead Sciences Inc.[58] Just as the regime attempts to leverage a large Iranian diaspora within democracies (discussed further below), it also sees members of this group as threats. Hence, the regime has a history of targeting Iranian dissidents, expatriates, and Americans and Europeans of Iranian descent.[59]

Iran also has a track record of targeting U.S. critical infrastructure. In 2011-13 (at the height of U.S. sanctions against Iran as the two countries were beginning secret talks on the Iranian nuclear program), Tehran undertook a series of Distributed Denial of Service (DDoS) attacks (codenamed Operation Ababil), which forced U.S. banks offline when it overwhelmed network traffic in 2012.[60] Though relatively unsophisticated, these attacks, described as "unprecedented" in their "scale," "scope," and "effectiveness," met their objective of disrupting the banks' operations.[61] In 2013, as mentioned previously, Iran hacked a New York dam's control systems.[62] In 2020, an Iranian-linked group known as Magnallium targeted U.S. electric utilities and oil and gas firms.[63] Counterintuitively, Iran's relatively inferior cyber capabilities may make it more willing to take more destructive action. As Annie Fixler put it in a *CTC Sentinel* article, "A common view held by researchers who follow the activity of Iranian hackers is that they are more likely to engage in destructive or disruptive attacks whereas their counterparts in other countries might be more inclined to quietly collect valuable data and intelligence."[64]

A 2018 Reuters report looking into Iran's influence operations found that many U.S. companies had unwittingly facilitated Tehran's efforts. As the report found, by normalizing concealed ownerships, U.S. firms had made it

harder to identify Iranian operations: "More than 50 of the sites use U.S. web service providers Cloudflare and OnlineNIC - firms that provide website owners with tools to shield themselves from spam and hackers. Frequently, such services also effectively conceal who owns the sites or where they are hosted."

Information Manipulation

In recent years, Iran has stepped up its efforts to create, disseminate, and amplify content it deems favorable to its interests in the United States and Europe, as well as in Latin America, the Middle East, and Africa.[65] According to the U.S. intelligence community, "Iran, which has used social media campaigns to target audiences in both the United States and allied nations with messages aligned with Iranian interests, will continue to use online influence operations to try to advance its interests."[66] Significant events helping Iran develop its information manipulation capabilities lie in the 2009 Green Movement, which drove the regime to become much more active in cyber space, as well as a robust propaganda campaign around the country's operations against the Islamic State in Iraq and Syria (ISIS) following the group's rise in neighboring Iraq in 2014. This campaign was designed to reassure fearful Iranians that their country was not succumbing to the fast-growing threat posed by ISIS, while also targeting other audiences, including in the United States and European nations whose forces joined the U.S.-led coalition fighting ISIS.

As a study by the Atlantic Council found:

> As of January 2020, Facebook has publicly identified: 766 pages followed by 5.4 million users; 55 groups joined by 143,000 users; 1,114 Facebook accounts; and 344 Instagram accounts followed by 438,000 users. Facebook has further attributed 43 Facebook events and $57,000 in advertising to Iranian actors. Twitter has identified 7,896 accounts responsible for approximately 8.5 million messages. Reddit has identified 43 accounts. There can be no guarantee that this represents the sum of Iranian efforts on these platforms.[67]

These are accounts linked directly to the Iranian state or backed by it.[68] Social media companies subsequently identified a number of new accounts with links to Iran.[69] Elsewhere, Iran has created spoof websites and pages to promote misinformation—including impersonating the U.S. think tank Foreign Policy Research Institute in early 2020.[70]

One of Iran's most far-reaching and well-documented efforts to spread false information was its "Endless Mayfly" campaign, which comprised dozens of websites imitating legitime news sources that were then disseminated by fictitious or stolen online identities. Most of the promoted stories contained false or misleading information aimed at disparaging Saudi Arabia, the U.S. or Israel. In many cases, once the imposter website was noticed, the hackers took it down and began redirecting to the authentic website, creating an "ephemerality" that made the operation harder to track.[71]

This digital manipulation campaign is the cornerstone of Iran's influence operations and is designed to counter and undermine the U.S. narrative on Iran and to "expose" the United States' shortcomings. These accounts targeted domestic Iranian audiences (despite the aforementioned ban on key social media platforms), the Iranian diaspora, and other Americans and Europeans. Official Iranian state-linked accounts and inauthentic accounts spread and amplified this content. As noted previously, Iran's official social media presence and activity are growing but remain well below those of China and Russia. And while the depth and breadth of Iranian covert information manipulation has not been fully exposed, data released by tech companies in recent years points to a growing trend. Moreover, compared to Russia and China, Iran's official presence on social media is much more fragmented and decentralized. For example, a number of individuals, including former President Mahmoud Ahmadinejad, who can be considered part of the broader Islamic Republic's system but who no longer hold offi-

cial positions within it, are active on social media—unlike in Russia and China. Platforms privileged by Iranian operatives include Twitter, Facebook, Instagram, and Telegram.

Iran's information manipulation efforts in the United States can be separated into several categories—although many overlap, and Iran's campaigns increasingly weave these themes together to create a more intricate narrative that can reach several audiences.

Theme 1: Fomenting Internal Division

The first strand of the Iranian narrative is geared toward leveraging U.S. domestic political and social themes to sow divisions within the U.S. political context. Like other online authoritarian information operations, Iranian-linked accounts aim to leverage existing divisions within the United States rather than to create new ones. This allows Iran to adapt to the social and political context rather than manufacture themes that do not gain traction. These tensions are typically along racial, social, economic, and political lines. For example, Iran's leadership has long sought to weaponize existing racial tensions in the United States by highlighting gaps in the U.S. judicial system, issues pertaining to unequal treatment by law enforcement, the absence of economic opportunities, and the lack of political representation.[72]

In both 2014-15 and 2020, Iran saw the Black Lives Matter (BLM) movement in the United States as an opportunity to exacerbate these tensions—though it is important to note that it mostly did so by highlighting the events as reported by the United States' own press rather than engaging in disinformation efforts. Iran also often connects themes in U.S. domestic tensions to U.S. foreign policy vis-à-vis the Middle East, framing these events in the context of its own struggles with the United States and presenting them as the continuation of the American people's own oppression by their government. For example, referring to the brutal killing of George Floyd by a police officer, which triggered massive protests throughout the United States, President Rouhani stated in June 2020 that Washington has its knee on Iran's neck.[73]

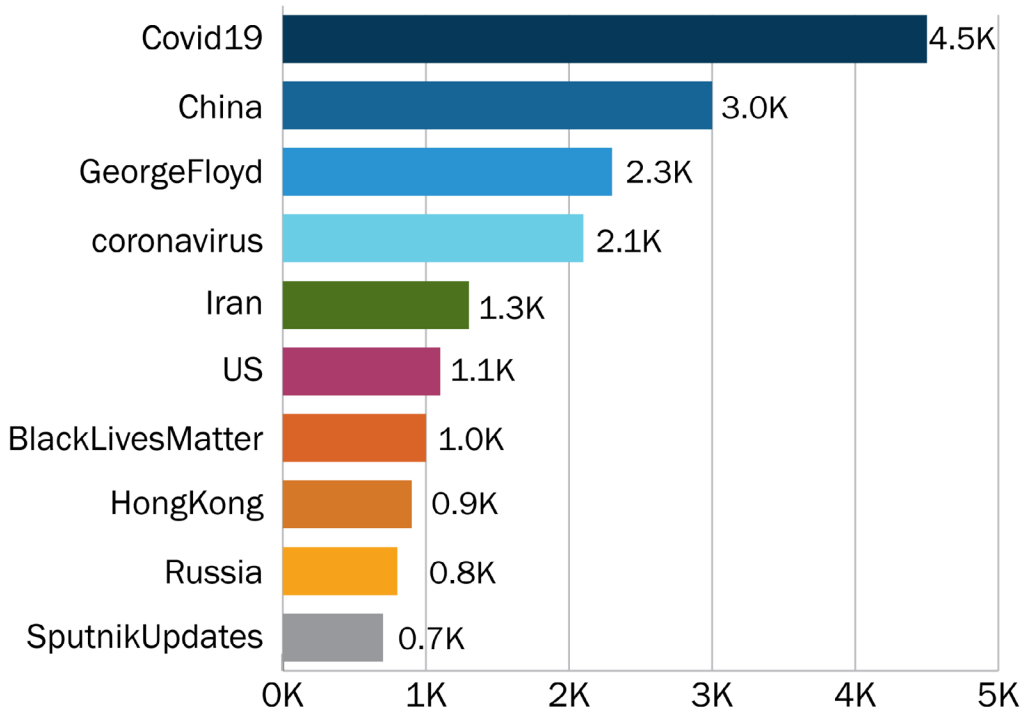
On both occasions, Khamenei took to Twitter repeatedly to frame familiar themes in Iranian propaganda, aligning himself with the BLM movement—not to express genuine concern for African Americans but to lend credence to Iran's own vision. According to this narrative, Iran and the American people are both victims of the U.S. government, and the animosity between the two countries is in fact the result of U.S. government policies. As Iranian officials often claim in vain, their chants of "death to America" are not directed toward the American people but toward their government and its policies.[74] By weaponizing BLM, Iran also sought to point out what it characterizes as U.S. hypocrisy. U.S. officials often decry the Islamic Republic's treatment of its own citizens and have taken action against the regime (chiefly through economic sanctions) for its human rights track record. Here, Iran saw an opportunity to turn the tables and point out that despite championing women's, religious minorities, and LGBT rights (among others), the United States, too, fails to keep its own house in order.

Using the Islamic Republic's traditional revolutionary language (dating back to prior to the revolution itself), Khamenei tweeted on August 17, 2014 that, "At events in #Ferguson US is fighting w its ppl. #BlackLivesMatter."[75] A week prior, Khamenei had taken to Twitter to frame his commentary in religious terms and in the context of Middle Eastern affairs, claiming, "#Jesus endured sufferings to oppose tyrants who had put humans in hell in this world& the hereafter while he backed the oppressed. #Ferguson."[76] A few months later, on Christmas Eve, December 24, 2014, Khamenei Tweeted an image of Jesus with several children with the caption, "If #Jesus were among us today he wouldn't spare a second to fight the arrogants&support the oppressed.#Ferguson #Gaza."[77] Here, Khamenei sought to cast Iran, Palestinians, and the American people as aligned in their respective struggles against the U.S. government (and, by extension, Israel).

Theme 2: Alleging Hypocrisy

When protests broke out throughout the United States (and in other democracies) in response to the killing of George Floyd by a police officer in May 2020, Iranian-linked media outlets and accounts resumed their activity around BLM. This time, Iran-linked accounts highlighted President Trump's decision to deploy U.S. military and other security forces on the streets of the nation's capital.[78] Key Iranian officials, including Foreign Minister Javad Zarif, took to Twitter to condemn the U.S. government's response and to call out European (and other democracies') silence on the matter. The message pushed in this context was that Europeans are often quick to condemn the human rights abuses in Iran, Russia, and China, but not when they are perpetrated by allies, including the United States. Chinese-linked accounts also pushed this narrative, pointing to double standards regarding U.S. support for protesters in Hong Kong when juxtaposed with the treatment of American protesters at home.[79] Iranian, Russian, and Chinese accounts engaged in circular amplification efforts, and #GeorgeFloyd and #BlackLivesMatter were in the top 10 hashtags pushed by the official accounts tracked by Hamilton 2.0. As the U.S. Department of State has noted, the convergence between the Chinese, Russian, and Iranian messaging has accelerated, and the three countries' messaging around the 2020 BLM protests in the United States illustrate this point.[80]

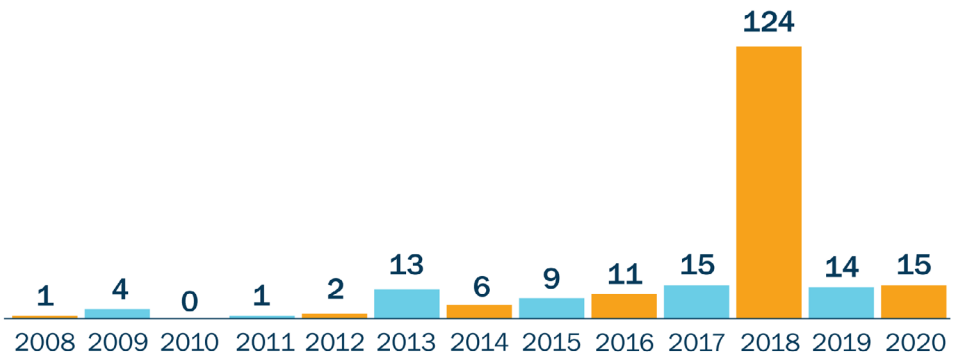
Top hashtags for Iran, Russia, and China for May 29-June 12, 2020 captured by Hamilton 2.0



Another example of the use of domestic political tensions and popular concerns in the United States lies in an April 2020 "digital flex" campaign by Iranian official and inauthentic accounts seeking to trend #Calexit.[81] California secessionist efforts have received a push by authoritarians in the past—so much so in fact that the California Independence Campaign's leader, Louis Marinelli, moved to Russia in 2017.[82] Miranelli had also publicly courted Chinese support.[83] In 2020, amid the domestic tensions regarding the response to the coronavirus and U.S.-Iran escalation in Iraq, Iranian activity around #Calexit resumed again. Former IRGC commander and presidential contender Mohsen Rezai was among those tweeting to make the hashtag trend. Framing the issue in the same familiar terms as Khamenei's engagement with #BlackLivesMatter, Rezai noted, "Californians are long-suffering victim of Washington's oppression, as so many other nations in the world. Stop spending their tax dollars to incite hatred around the world. They want to build bridges with their money, not walls. #Calexit."

Theme 3: Criticizing U.S. Foreign Policy

A third theme in Iran's disinformation and propaganda campaigns is using foreign affairs both to divide the U.S. public and advance Iranian interests. The nuclear deal with Iran is an important theme in Iranian social media activities. A key issue directly relating to Iran's core national interests, the JCPOA also had the specificity of being a particularly divisive foreign policy matter in the United States, providing Iran with more fodder in its campaign—which has spiked at least on two occasions, around the last stretch of the negotiations that led to the signing of the deal in Summer 2015 and following the subsequent U.S. withdrawal from it in Spring 2018.[84] 2018 also saw the creation of the most number of Iranian diplomatic accounts on Twitter; over 100 official Iranian accounts were created on the platform that year. As noted previously, one specific datapoint suggesting that Iran's overt use of social media to advance its narrative is mostly for external consumption lies in the fact our data shows correlation (though not causation) between major international and foreign policy events and an uptick in Iranian social media activity. Conversely, major domestic events, including elections and protests, do not lead to such upticks—though the 2009 Green Movement and late 2017-early 2018 protests that erupted throughout Iran are important exceptions.



Number of Iranian Diplomatic Accounts Added to Twitter

(Data accurate as of June 2020)

Iranian-linked accounts also promote anti-Saudi, anti-Israeli, and pro-Iranian content.[85] This content tends to favor the U.S. left, which may be predisposed to oppose Saudi and Israeli policies, and U.S. policies perceived to be aligned with those nations' interests.[86] In particular, a number of Iran-linked online influence operations appear to target the progressive wing of the Democratic party (a similar pattern is visible in the case of the Labour Party in the United Kingdom).[87] Staple themes in Iran's anti-Saudi and anti-Israeli online campaigns include pro-Palestinian narratives highlighting Israeli settlements and human rights abuses, as well the Saudi-led coalition's war in Yemen and the humanitarian crisis in that country. Despite the regime claiming to oppose Israel as a state and the policies pursued by its leadership rather than Jewish people, much of this content is outright anti-Semitic, and it uses Palestinian causes and narratives as a justification for its anti-Semitism.

The regime and key opposition groups (especially the pro-monarchy and MeK) clash on social media by siding with one side of the U.S. political spectrum over the other.[88] Indeed, many pro-monarchy and pro-MeK accounts embrace President Trump's "maximum pressure" campaign against Iran and baselessly denounce Democrats (especially those on the more progressive end of the spectrum) as pro-regime. Although these two movements have little in common in terms of ideology, values, and beliefs, they both wish to see the Islamic Republic collapse

(which would potentially usher them back into power). For segments of these groups, the Democrats' proposed approach to Iran (as symbolized by President Obama's nuclear deal) only serves to maintain the regime instead of forcing it to capitulate, thus helping create what they would consider the right environment for a new political system led by their leaders to emerge. Hence, both parts of the pro-monarchy and MeK opposition push for a more hawkish Iran policy which would leverage U.S. foreign policy in the pursuit of their own goals. For its part, the regime-linked accounts tend to amplify content by progressive politicians and groups which they view as less anti-Iran.

Elsewhere, Iran is also focused on building global support for its policies and countering the U.S. narrative. The regime has long invested in an intelligence and media apparatus targeting regional states and key co-ethnic and co-sectarian groups. In Afghanistan, Iraq, Lebanon, the Persian Gulf region, and Syria, Iran promotes narratives that seek to undercut those of the United States and its allies. There, Iran presents itself as a benevolent power, siding with those "oppressed" by the "oppressor" camp led by the United States and composed of Israel, adversarial and rival Gulf monarchies, and the United States' European allies.

Theme 4: Shifting Blame, Projecting Power

Another key thread in Iran's efforts is best summarized as "America can't do a damn thing."[89] Ayatollah Khomeini had tried to capture the United States' weakness in this quip during the hostage crisis, and the quote appears on many Iranian weapon systems, as well as at rallies and arms expos. Today, Iranian state media and affiliated accounts try to highlight U.S. incompetence or weakness, which they compare and contrast with Iran's own strength—a strength that in their narrative does not stem from economic or military power but faith, values, righteousness, self-confidence, and self-reliance. Though this strand is much more prominent in Iran's internal propaganda and disinformation efforts and is largely meant for domestic consumption, it is relevant to this discussion as it also targets populations in other democracies, especially those that may already be skeptical of or nonaligned with the United States, as well as members of the diaspora.

In the context of the global struggle to respond to the coronavirus (and eager to distract from its own botched response to the outbreak), the regime sought to highlight the United States' failure in managing the pandemic. Khamenei likened the environment created in the United States by the coronavirus to the "Wild West," though he attributed the statement to an unnamed "Western Senator."[90] According to Khamenei, the senator had noted that "the Wild West has been revived,"[91] lending credence to what Iranian officials say when they suggest that underneath the appearances, the West is wild. Iranian media outlets and affiliated social media accounts then began to push the Persian translation of "Wild West" as a hashtag on Twitter. Cartoons and articles mocked toilet paper shortages and reported on efforts by the U.S. government to outbid its allies in the process of acquiring masks, and were amplified by regime-backed social media accounts and in other state-run outlets.[92] Some state-linked outlets echoed themes present in Chinese and Russian propaganda efforts, including claiming the world order as shaped by the United States was on its last leg as a result of the coronavirus.[93]

Moreover, in an effort that met the objective of showcasing U.S. weakness in contrast to Iranian strength and of sowing divisions within the United States, Iranian-linked accounts capitalized on the internal struggle to resume economic life within the United States. When protests erupted in the several U.S. states opposing the lockdowns imposed and enforced by their governors, which in some instances culminated in tensions between healthcare professionals and armed protestors, Iranian-linked accounts published footage and photos using the hashtag "#Wild West." The message here was that while Americans were intimidating healthcare professionals with their guns, Iranians were thankful for healthcare workers' efforts.

Theme 5: Pushing Specific Iranian Interests and Opposing Sanctions

Finally, some of the Islamic Republic's information manipulation efforts are geared toward changing the dis-

course around specific policies directly affecting Iran in general and deliberations around sanctions policy in particular. Given the prominence of sanctions in the United States' approach toward Iran in recent years and the controversial nature of this pressure tool, the regime has undertaken a robust propaganda campaign aimed at discrediting them. Iranian officials often equate sanctions with economic warfare or terrorism (Iran-linked accounts often push #EconomicTerrorism on Twitter).[94] With the outbreak of the coronavirus, "#MedicalTerror" became another term and hashtag used by Iranian officials.[95] And Iranian officials, state media, and affiliated social media accounts promote the narrative that U.S. sanctions are purposefully targeting humanitarian trade, particularly medical devices and medicine.[96]

While there are legitimate questions about the side effects and unintended consequences of U.S. sanctions and their implications for humanitarian trade, it is false that they directly target such business; in fact, humanitarian goods, such as medical devices, medicine, and food are exempted from U.S. sanctions. Nonetheless, this narrative has gained traction both among the Iranian population and the Iranian diaspora. And this line of reasoning according to which U.S. sanctions directly target humanitarian trade is part of the domestic U.S. debates about Iran and sanctions policy. Another similar example lies in the efforts by the Iranian government to legitimize its actions in the Persian Gulf. The IRGC Navy routinely harasses the U.S. Navy vessels there. According to Iranian officials, the United States has no business in the Persian Gulf, which is, after all, named the Persian Gulf not the Gulf of Mexico, as they put it.[97] The issue of the Persian Gulf strikes a patriotic note for many within the Iranian diaspora, and this narrative resonates with many Iranian-Americans and other Americans critical of U.S. military interventions, thus gaining traction at a time when many in the United States question the desirability of U.S. operations and presence in that region.

The overarching objective of these strands of Iranian information manipulation efforts is the promotion of a U.S. foreign policy that favors Iran. This is achieved by leveraging existing tensions and divisions in U.S. society pertaining to both foreign and domestic policy issues. In that sense, Iran's objectives are not dissimilar to those pursued by Russia and China, both of which use this tool to advance their interests. But Iran's may be more modest than those of Russia and China (as are the means at Iran's disposal and the sophistication of its campaigns), which see themselves in a more holistic (and equal) competition with the United States. As Emerson T. Brooking and Suzanne Kianpour put it, "[t]he primary aim of these efforts is to simply 'tell Iran's story,' the same as any Western government broadcaster might strive to do. The difference is that, as an international pariah, Iran must pursue this work through more clandestine means. Global observers have long learned to doubt the truthfulness and sincerity of Iranian-branded media."[98]

Malign Finance

Despite a long track record in malign finance there is little evidence at present to suggest that this area is a major challenge in terms of foreign efforts to undermine democracies (certainly not on the scale of Russia's).[99] Iran's illicit financial activities appear to be mostly focused on achieving several key objectives: 1) Keeping the country's economy afloat and undercut sanctions; 2) Increasing Iranian influence and funding the regime's activities in the region (including by funding direct Iranian interventions and various proxies in the region); and 3) Supporting information manipulation operations aimed at Western audiences. This is not to say that Iranian malign financing efforts are not a challenge and should not be addressed by the United States and like-minded democracies. After all, these activities pose a threat to the "integrity and security of the international financial system."[100]

Iran has been under U.S. and international sanctions for the better part of the regime's existence. Lacking access to legitimate markets and the global financial infrastructure, Tehran has built a comprehensive illicit finance and procurement network.[101] The IRGC leads many such activities, and its sprawling business and financial networks have thrived despite (and, in some cases, thanks to) sanctions.[102] Following the signing of the JCPOA, the Iranian government attempted to address some of the challenges stymying its efforts geared toward economic recovery.

In particular, the absence of a proper regulatory landscape stood out and deterred risk-averse businesses and banks from entering or reentering the country's market. As a result, the government sought to push forward plans aimed at getting the country removed from the Financial Action Task Force (FATF) high-risk jurisdictions list—whose criteria include failing to comply with standards pertaining to money laundering, terrorist financing, and financing of proliferation.[103]

The issue was highly contested within the Iranian political system as the regime's security architecture is largely dependent on non-state allies and partners, including many designated terrorist organizations. After much domestic political bargaining, including a back and forth on a bill proposed by the parliament going all the way up to the Expediency Council—an advisory body to the supreme leader on policy matters, which also serves as a legislative body as it is tasked with arbitrating between the parliament and the Guardian Council when the latter offers amendments to a proposed bill by the former—Iran was placed on the list again with FATF noting that the country had not completed the action plan to address its strategic deficiencies.[104] In particular, Iran failed to ratify the Palermo and Terrorist Financing Conventions.[105] FATF also noted items lacking in terms of the Counter-Terrorist Financing Act and Anti-Money Laundering Act.

According to the U.S. government, Iranian practices include "front companies, fraudulent documents, exchange houses, seemingly legitimate businesses and government officials, to generate illicit revenues and finance their malign activities."[106] The creation of front companies also facilitates the intersection of malign finance and information manipulation. The regime establishes or supports media organizations that obfuscate their financial and operational ties to Tehran and promote Iranian interests in a manner that appears more legitimate to Tehran's audiences in the United States and Europe. As a result, a narrative that may be dismissed by Americans and Europeans if it is overtly pushed by an authoritarian actor or adversary can gain more traction if it appears to be advanced by independent organizations formed by concerned citizens. The effectiveness of these operations appears limited; although, it remains largely understudied. These news outlets employ Americans and Europeans who may share some of the Islamic Republic's beliefs or provide them with a platform to express such ideas. Iranian actors (likely tied to the Ministry of Intelligence and Security, the Islamic Republic of Iran Broadcasting (IRIB), and/or the IRGC) pay these individuals, some or all of whom may not be aware that they are part of an Iranian influence campaign.

For example, starting in 2015, The American Herald Tribune, a website reportedly originating in and run from Iran, paid Americans to publish English-language material.[107] "Unwitting" Americans were paid to write stories and articles that aligned with the views of the Islamic Republic in an effort that was designed to help bolster and lend credibility and legitimacy to Tehran's efforts. The website was used to reach several audiences both in Iran and abroad thanks to circular amplification. Circular amplification is a tactic often used by Iran (and other authoritarians) to maximize the number of targeted audiences a single campaign can reach. In this case, The American Herald Tribune served to target a primarily U.S. audience. Iran's state media would then reference or publish The American Herald Tribune's articles as an example of what it would falsely claim to be American reporting supporting the Islamic Republic's narrative, thus attempting to lend credibility to Iran's positions.[108]

In one such instance, the hardline Iranian website Shafqna translated a piece in 2019 that had originally been published in The American Herald Tribune, arguing that U.S. policy toward Iran had failed.[109] To an unsuspecting Iranian audience, this appeared to be a legitimate article published by a U.S. outlet supporting the regime's position.[110] Another such example lies in the public relations campaign around Khamenei's "Letter to Western Youths." In 2015, Khamenei wrote an open letter to the youth of Europe and North America inviting them to try to understand what he characterized as real Islam in an effort to change perceptions of the faith in the West following the rise of ISIS and the terrorist attacks perpetrated by the group's operatives in Europe.[111] The letter, which was promoted under "#Letter4U" on social media platforms,[112] was circulated by The American Herald Tribune and other Iran-linked media outlets and accounts. The letter went mostly unnoticed in the West. Having

failed to reach its desired objective internationally (and in the United States and Europe in particular), the regime sought to convince its domestic audience that the letter had gained traction by reproducing The American Herald Tribune's report about it.

The Strengths and Limitations of Iran's Authoritarian Toolkit

Like Russia and China's, Iran's influence operations have a number of strengths—although Tehran is not always able to use them to their full potential. First, the regime's fairly modest objectives (relative to Russia and China) make them attainable for a country with fewer resources at its disposal than the two other key authoritarian actors. Iran is not looking to fundamentally challenge the United States but to score points where it can. Hence, although its resources are limited, so too are its objectives. Iran also benefits from a fairly flexible and adaptive national security strategy and has demonstrated an ability to evolve and try to develop new tools to expand its toolkit—even though these tools may not always be easily attainable to the country as it has been under sanctions and largely cut off from international markets for the better part of the Islamic Republic's existence.

Second, a large Iranian diaspora provides Iran with a significant resource, especially in key countries of interest. Similarly to Beijing and Moscow's efforts to build bridges to the Russian and Chinese diasporas in key countries, Tehran also targets what it views as influential Americans, Canadians, and Europeans of Iranian heritage in business, academia, journalism, civil society, and government. Second and third-generation Americans and Europeans of Iranian descent are often well-assimilated and in tune with their cultural contexts, fluent in the language of their country, and some are the product of mixed families. However, several obstacles make it difficult for the regime to establish a connection with them.

Many in the diaspora, including those who may have more sympathetic views of Iran, reject its government and would not wish to adhere to its belief system and restrictions. Many are deeply loyal to their countries and indeed choose to serve in the U.S. or European militaries or governments over the Iranian regime and its armed forces. The Islamic Republic's efforts to spy on and intimidate dissidents and critics, as well as the arrests of dual nationals (particularly American nationals and EU citizens) further fuel the distrust between this group and the regime. And the regime's own suspicions, paranoia, and ideology are an obstacle preventing it from effectively recruiting and working with individuals within the diaspora. Tehran's messaging is also much less appealing and the means by which it tries to activate nationalism in the diaspora more constrained and less sophisticated than those employed by Russia and China. This is a weakness in Iranian operations the United States and Europe can leverage to undermine the regime's attempts at undermining democracy on both sides of the Atlantic.

Finally, perhaps the greatest strength playing in Iran's favor lies in its ability to effectively leverage and fuel existing tensions within U.S. society. Distrust of facts, the government, news media, and other institutions; divisions along socioeconomic and racial lines; and heightened partisanship are all weaknesses that Iran (like Russia and China) has been able to exploit. In essence, Tehran does not need to create new divisions when it can simply observe, identify, and weaponize existing ones. Using grievances to sow discord and fuel conflict is not a new tactic for the Islamic Republic, whose regional playbook has consisted of leveraging and exploiting existing and real concerns within a society in countries such as Iraq and Yemen. Thanks to the Internet in general and social media in particular, Iran can now deploy this tactic in the United States and in Europe more effectively, at a low cost, and with little risk in an attempt to undermine democracy.

Iran's influence operations also suffer from a number of shortcomings and weaknesses. First and foremost, despite being an authoritarian regime, Iran's system is not always unified, even though it does design and implement its national strategy as a unitary state. Hence, different power centers may push different, and at times even conflicting, narratives. For example, during the early stages of the coronavirus outbreak, several narratives were emerging from key Iranian power centers and outlets. As Khamenei and some IRGC commanders (falsely) claimed that the disease was perhaps created and spread by the United States to target its enemies in places like China and Iran, others (including state media outlets, such as Fars News and Tasnim) were focused on the theme

of Western helplessness, highlighting the number of deaths in the United States and Europe. This narrative used by Fars News and Tasnim aimed to point to mismanagement of coronavirus in the West (and was likely part of an effort to take the heat off of the regime's own abysmal response to the disease). China and Russia both undertook similar efforts and used comparable tactics. In fact, as noted previously, all three countries adopted similar themes in their disinformation campaigns and amplified each other's messaging.

Second, the regime's incompetence, mismanagement, and corruption have often provided real-life and real-time counterpoints to its carefully crafted messaging.[113] In January 2020, for example, shortly after the United States targeted and killed Soleimani, Tehran formulated what it hoped would be a high-profile and resolute response. The action and messaging around it were carefully designed and calibrated. The Iranian armed forces targeted two bases in Iraq housing U.S. personnel. The propaganda campaign that followed sought to show Iran's strength and telegraph to the United States that it would not be deterred or intimidated.

Iranian military commanders and IRGC-affiliated reporters claimed that their attack had led to many U.S. casualties—even as the U.S. Department of Defense denied the figures presented by the regime claiming dozens of casualties. Iran's propaganda campaign was quickly stymied by emerging reports that the regime had accidently shot down a Ukrainian airliner during its attacks on the Iraqi bases, killing all passengers and crew onboard. After a brief attempt at covering up the cause of the accident, the IRGC took responsibility for the incident and the more than 160 deaths. Accountability, however, remained limited, as virtually none of the prominent players involved in the debacle saw repercussions for their mismanagement of the episode. Though Iran clearly undercut its own response and messaging, it must be noted that the U.S. government's initial failure to acknowledge that a number of service members had indeed suffered severe brain injuries during the attack, before slowly unveiling the numbers of those diagnosed—a number well above 100—did play into Tehran's hand.[114]

Third, although they have been expanding over the past decades, Iran's capabilities remain fairly limited (even as they grow in certain realms, like cyberspace), and its ability to invest in developing its toolbox is restrained by sanctions, due to a lack of funding, resources, and access to open markets, as well as stymied by regime paranoia, infighting, and intra-system competition.[115] Iran has a fairly dynamic and active start-up sector, and the government has increasingly invested in the state-run tech sector as well—though, here, too, the regime's paranoia and emphasis on loyalty pose a challenge to improving ties and cooperation between the government and these sectors. Tehran likely acquires tools and know-how from Beijing and Moscow. Hence, a poor economy, lack of capacity, and sanctions have denied Iran some tools. They may, however, have led Tehran to use whatever capabilities it has at its disposal more aggressively.

Fourth, opposition within Iran and Persian news outlets based in the United States and Europe can provide powerful counternarratives exposing the regime's disinformation, misinformation, and propaganda. Some such outlets may also face a credibility challenge as sources of funding tied to these governments (the United States and Great Britain or regional states such as Israel and Saudi Arabia) raise questions about their neutrality. Hence, it is critical that democratic governments' efforts to ensure the free flow of information inside Iran and to undercut the regime's propaganda and disinformation are based on unbiased, truthful, and credible reporting.

Finally, the vision Iran tries to sell is inherently limited in its appeal. Given the religious undertones of the revolutionary ideology (one predominantly appealing to Shia Muslims), Iran is unable to offer a real competing vision to that sold by the United States and its democratic allies. Iran is aware of the limited reach of its vision and ideology, as well as the restrictions of its capabilities, and has, as a result, mostly focused its efforts on building a media infrastructure designed for its immediate region.

Implications, Vulnerabilities, and Recommendations

Implications for Authoritarian Learning and Resilience

Iran has certainly observed and learned from other authoritarian regimes, chiefly Russia and China. It has also cooperated with both to further develop its toolkit. Though the three authoritarian actors do not have a unified vision of what model they seek to promote, they all view democracy promotion as a threat to their regime survival and interests. Hence, the three states are more aligned in what they are fighting against than they are in the view of what they are fighting for. In fact, "[a]uthoritarian governments do not aim to promote authoritarianism per se as a mirror image to democracy promotion. Collaboration, particularly in crisis conditions, is more opportunistic than strategic."[116] There are some differences in the objectives pursued and methods employed by Iran, Russia, and China. Nevertheless, they all capitalize on existing vulnerabilities in democracies.

Recommendations

Build resilience to disinformation in democratic societies

Misinformation at home can help authoritarians' disinformation efforts. Democratic governments should build resilience through democratic institutions and invest in news literacy among their populations. They should also support the independent press. Likewise, coordination between national governments, technology companies, and civil society is key. Technology companies, in particular, should increase transparency by taking such actions as labeling outlets and accounts funded or operated by the Islamic Republic, as they have begun to do for other key actors, including Russia and China. Iran (like Russia and China) thrives on divisions within democracies, which it leverages to weaken the United States and like-minded democracies. By contesting facts domestically, democracies make it easier for authoritarian players to disarm them and to advance their own "alternative facts" and dubious narratives. Authoritarians weaponize misinformation and divisions in democracies to discredit any criticism directed at themselves and to advance their agendas. An example lies in the May 14, 2020 tweet by Zarif, where he leveraged inaccurate statements made by President Trump about the possibility of injecting disinfectants into the human body to fight coronavirus, noting, "Those who muse about injecting disinfectant to 'clean' the coronavirus, also argue that they are a 'participant' in a UN Security Council Resolution endorsing a deal that they long ago 'ceased participating' in. Their own words."

Don't respond to authoritarian efforts in kind

The United States and its democratic allies should not reciprocate Iran and other authoritarians' efforts. Democracies should not adopt the tactics used by authoritarians to undermine democracy. Instead, they should ensure that democratic principles guide their approach and responses to authoritarians such as Iran. Democracies should focus on leading by example and taking "the high road." For example, combating misinformation at home, facilitating free speech, and making it clear that the intimidation of individuals based on their beliefs (as the State Department-funded initiative, Iran Disinfo, aimed to do prior to being rightfully terminated by the department) are not just powerful tools in undermining authoritarian efforts aimed at weakening democracies; they are an end in themselves. Overall, the United States' soft power and its ability to lead by example are the most powerful tools in the U.S. toolkit.

Deepen understanding of Iran's activities that are designed to undermine democracy

Although the U.S. intelligence community has warned frequently and consistently for a number of years that Iran has joined Russia and China in undertaking activities designed to undermine democracy (including the Office of the Director of National Intelligence mentioned at the top of this report), our understanding of Tehran's

objectives, strategy, tactics, techniques, and procedures is still lacking. This report has attempted to shed light on Iran's activities, but more research is still needed to fully grasp how Tehran's objectives and operations compare to and differ from those of Beijing and Moscow, as well as Arab Gulf states. Moreover, as this report has shown, Iran's operations continue to develop and become more sophisticated, making it more important to monitor the threat's evolution and to identify new strengths and vulnerabilities.

Contextualize and depoliticize Iran's authoritarian efforts to undermine democracy

Iran presents numerous national and international security challenges. The regime is engaged in a host of nefarious activities ranging from human rights violations at home to military interventions and support for terrorism in the region, as well as nuclear and missile activities that pose a threat to the United States and its allies and partners. There are reasonable debates within the U.S. national security community regarding the level of the threat presented by Tehran and how best to tackle it, though these debates have become increasingly partisan in recent years, especially following the start of the nuclear talks during the Obama administration. However, Iran's authoritarian efforts to undermine democracy in the United States and elsewhere should be separated from the regime's other actions and considered in a nonpartisan and apolitical manner. For this reason, both sides of the aisle should make it clear that regardless of partisan differences on other key Iranian challenges, interference in U.S. elections by Iran would not be tolerated and will be addressed similarly regardless of which party, platform, or figure they target.

Formulate a clear and coherent declaratory policy about Iran's efforts—unilateral or coordinated with other authoritarian actors—to undermine democracy

Democracies should deter authoritarian actors such as Iran from undertaking actions designed to undermine democracy in the United States, Europe, and elsewhere. Additionally, democracies should also develop a strategy to respond to such efforts, including by building multilateral and unilateral mechanisms and tools (on a bipartisan basis) that raise the costs of and impose repercussions for authoritarian actions that undermine democracy.

Use a broader set of tools to counter Iranian activities

In recent years, the United States' Iran policy has mostly leveraged sanctions as a coercive tool. This overreliance on sanctions comes with significant drawbacks, including further dividing Washington and its European allies. In the long term, this overreliance on sanctions risks decreasing their efficacy—especially as Tehran's resilience to sanctions improves. When it comes to Iran's efforts to undermine democracy, the United States should adopt a multilayered approach, which leverages different tools in its toolkit. This would include but would not be limited to sanctions and consist of diplomacy and cyberattacks, among other option.

Promote multilateralism and work with allies and partners

As we have seen, among Iran's chief objectives is to widen the gap between the United States and its allies in Europe, which allows Iran to better advance its own interests. For example, with the Trump administration pursuing a series of unilateral actions against Iran—which affect Europe directly—with little regard for the security concerns of the United States' European allies, Iran is able to pit the two sides of the Atlantic against each other. This leads to neither the United States nor Europe securing their own objectives, and allows Iran to benefit from the division. A notable example of this dynamic lies in the U.S.-Iran tensions resulting from the U.S. withdrawal from the JCPOA, which have paralyzed Europe, brought the United States to the brink of war with Iran (and led to the deaths and injuries of a number of U.S. servicemembers), while allowing the regime to resume key elements of its nuclear program previously limited by the agreement, as well as to dial up violence in the region.

The United States and its European allies should elevate Iran's authoritarian efforts to undermine democracy on both sides of the Atlantic in discussions and processes designed to formulate a coherent policy to tackle the

challenges it poses. Generally, Washington and its European allies have worked in concert to advance interests pertaining to financial transparency, nuclear nonproliferation, counterterrorism, and human rights, including by coordinating on sanctions and establishing multilateral diplomatic processes. They would benefit from similarly adopting a more coordinated response to Iran's growing efforts to undermine democracy.

Similarly, in the Middle East and North Africa region, where Iran has often sought to undermine democratic efforts when it perceived them as going against its own interests, the United States would benefit from partner engagement on the issue. In particular, Iran has increased its influence operations in the region in recent years, investing in Arabic-language media outlets and the creation and amplification of social media content designed to advance Iranian interests at the expense of democratic movements in the region. Yet, the United States continues to see capacity-building with regard to regional partners through the prism of conventional military capabilities.

Develop cross-sector cooperation and information sharing to counter Iran's influence operations and cyber activities aimed at the private sector and civil society

A more robust public-private partnership is needed to identify and mitigate threats posed by Iran-linked actors, who are launching a growing number of cyberattacks on civil society and the private sector in democracies. In the United States as in Europe, the executive and legislative branches and the tech sector should share information and provide information to the public.

Adopt clear and coherent policies and expose the flaws in Iran's narrative

As noted previously, democracies should not be engaged in reciprocating or reproducing authoritarians' information manipulation efforts; however, adequate and clear messaging can help expose the flaws in these regimes' propaganda and disinformation. For example, the U.S. government would benefit from clear guidance on its sanctions on Iran. Not only would this serve broader U.S. objectives vis-a-vis the regime, it would also help undercut its disinformation efforts as exemplified by the activity around the coronavirus and the humanitarian exemptions in U.S. sanctions. Presenting clear evidence of what the U.S. government has done to facilitate humanitarian trade to undercut Iranian claims that such business is allowed would help combat Iranian propaganda efforts at home and disinformation campaigns abroad.

Conclusion

Over the past decade, Iran has joined two traditional authoritarian players, Russia and China, seeking not just to compete with but also to undermine democracy in the United States and Europe. To this end, Iran has likely been aided (both directly and indirectly) by Russia and China, becoming more sophisticated in the methods and tactics it deploys against the United States and like-minded democracies, particularly in Europe. However, the Iranian challenge must be contextualized, and it should not be overstated. Iran remains a lesser threat than Russia and China, whose intentions are broader, worldviews less limited in their appeal, and capabilities much more advanced. Nonetheless, Tehran's efforts to interfere in and undermine U.S. democracy must be taken seriously and addressed. But at present and for the foreseeable future, Iran is unlikely to rise to the level of Russia and China both due to its far inferior capabilities and awareness of the limitations shaping its intentions. Nevertheless, a growing toolkit and an evolving playbook make Iran an important source of concern in such areas as cyberspace in general and online information manipulation in particular, with malign finance and broader election interference remaining far less significant threats stemming from Tehran's authoritarian playbook.

Appendix

Key Players

The objectives and doctrine outlined throughout this report are decided and executed by key power centers within the Iranian system. The following sections provide a brief summary of the mandate of and role played by each in terms of decision-making and the deployment of the tactics considered later in the paper. The Iranian system does not allow for traditional political parties as in liberal democracies. Instead, several blocs vie for influence. Today, they are generally broken down along these lines:

- Principalists call for preserving the Islamic Republic as intended by its founder, Ruhollah Khomeini, and the revolutionaries who rallied around him. They privilege self-reliance and a foreign policy based on few concessions to the West (and tend to see negotiations through the prism of concessions made to the powers). Instead, they focus on building ties with similar-minded state and non-state partners. However, while most principalists leave some wiggle room to work with the West, a subset of them closes the door to any flexibility.
- Hardliners are the subset of principalists who demand the strictest adherence to the Islamic Republic's vision and values and tolerate little to no deviation from them. They are the most ardent opponents of engagement with the West in general and the United States in particular. Hardliners stress more self-sufficiency and less reliance on the West.
- Reformists are the camp most closely associated with change (within the confines of the system) in the Islamic Republic. The pro-reform movement has called for less strict enforcement of social constraints, more openness to the world, and greater engagement with the West. This bloc has been mostly sidelined and rendered irrelevant in the regime in recent years.
- Pragmatists tend to favor a middle-of-the-road approach. Under Rouhani's presidency, the pragmatist view of foreign and domestic issues has been characterized by a near exclusive focus on economic issues, the quest for improved relations with other countries (especially Europe and those in the Middle East), and very little movement on social issues, despite initial promises to the contrary. Pragmatists tend to identify areas of compromise between the reformist camp and the principalist bloc, and they try to build an agenda that they believe can be implemented within those constraints.

These blocs are rather fluid, and individuals tend to move from one camp to another depending on their interests, their beliefs, the issues at hand, and other considerations. For example, a notorious principalist for most of his career, Aliakbar Hashemi Rafsanjani, who occupied a number of key positions within the Iranian system, including the presidency, has also championed reformist causes and became known as one of that camp's chief leaders. The former speaker of the parliament, Ali Larijani, is another case in point. Although he is mostly a principalist, Larijani supported the JCPOA and was instrumental in securing buy-in for the agreement from other principalists. The following sections provide an overview of the formal power structure in Iran and the role of key power centers in shaping and deploying the regime's authoritarian toolkit.

The Supreme Leader

The Iranian toolkit is designed and deployed by several (often redundant) power centers and entities within the complex web of organizations in the Iranian system. The supreme leader sits on top of this apparatus and has veto power over all matters. Although the supreme leader is a single individual comprising the highest authority in the country, he receives support from a much larger apparatus. The Office of the Supreme Leader (known as *beyt-e rahbari* or the house of the leader) is composed of thousands of aides, advisors, and security forces. A number of redundant positions exist in the supreme leader's office and advise him on nearly all core issues ranging from domestic and foreign policy matters to religion. Since the early days of the Islamic Republic, the Office

of the Supreme Leader has served as one of the key players in the information operations domain.

Khamenei's predecessor, Ruhollah Khomeini, gained prominence as a religious scholar over the course of nearly three decades before becoming the leading voice of the revolution and, subsequently, the head of state. He emerged as a fairly junior cleric whose opposition to Mohammad Reza Pahlavi, commonly known as the Shah, (and especially the Shah's cooperation with the United States and Israel, and efforts to expand civil rights for women and religious minorities, particularly Jewish and Baha'i communities in Iran) afforded him a loyal and fanatical following. The Shah's own authoritarianism and his decision to send Khomeini into a 15-year exile coupled with his rapid top-down reforms brought about his downfall. From afar, Khomeini first helped shape the anti-shah narrative before completely dominating it. Khomeini and his followers were able to use the technology available to them at the time to spread disinformation (about the Shah and his security forces, as well as U.S. intentions and operations in Iran). These tools included cassette tapes, pamphlets and leaflets copied thanks to the newly available Xerox machines and distributed throughout the country.

Since his rise to supreme leadership, Khamenei has followed in Khomeini's footsteps, advocating for the use of new technology to secure regime survival and make the regime more competitive against its adversaries. His office has long championed the use of cyber capabilities and information manipulation to undermine democracies. As the chief guarantor of Khomeini's revolutionary legacy and the commander in chief of the armed forces (which include both the IRGC and the conventional military or Artesh), Khamenei plays a critical role in defining the framework within which decision-making on the development and implementation of Iran's strategy and toolkit take place. Khamenei is a principalist and even a hardliner on many issues and has generally expressed a deep distrust of Western-style democracy, particularly the United States.

Today, Khamenei supervises key organizations within the system that deal with cyber issues and has a large presence on the Internet. Given the sensitivity of the cyber portfolio, Khamenei appears to exercise tighter control and oversight of it (on par with the regime's past nuclear weapons program) than is generally the case in other areas. This is further discussed under the section on the Supreme Council of Cyberspace). His office operates a number of social media accounts in multiple languages on all key platforms and maintains many websites (also in several languages). A number of "individual" accounts then amplify this content. Khamenei often uses his official speeches, media appearances, and multimedia and social media activity to highlight key themes in Iran's information manipulation. Some examples of this activity are examined further.

The Supreme National Security Council

The Supreme National Security Council (SNSC), whose function resembles the U.S. National Security Council (NSC), is an organization intended to streamline national security decision-making and to allow different power centers to coordinate their efforts. In the context of Iran's authoritarian efforts, the SNSC likely plays an important role in facilitating decision-making on strategy. It is also responsible for deconflicting key organizations' involvement and coordinating policy implementation. As power centers within the regime are often redundant, disjointed, and in competition with one another, this exercise is particularly significant, as it allows the system to act as a unitary actor. Whereas the U.S. NSC falls squarely within the executive branch, the Iranian SNSC spans different branches and power centers, to include the supreme leader's office, the president and cabinet, the judiciary and legislative branches, and members of the Iranian armed forces (both the conventional military and the IRGC).

The Supreme Council of Cyberspace

The Supreme Council of Cyberspace was created by Khamenei in 2012. In 2015, he announced that the council would have sole authority to design cyber policy.[117] On paper, the council's role is to streamline the governance of cyber activities in Iran, help place the nation among key cyber powers, and facilitate economic activities using

the Internet.[118] The council was also tasked with operationalizing the "national" Internet and promoting Iranian and Islamic values and lifestyle.[119] As in other authoritarian states which have toyed with the notion of a national Internet, this initiative is designed to effectively stop the flow of information considered undesirable by the regime. The broader strategic objective of creating the council was designed to allow a small and fairly conservative body aligned with Khamenei to dominate decision-making pertaining to cyberspace.

IRGC and IRGC Intelligence

Other key entities include the IRGC and, in particular, the IRGC intelligence organization, which is often in competition with the civilian-controlled Ministry of Intelligence and Security (MOIS), but also closely coordinates with it. The IRGC in general and the IRGC intelligence organization in particular are significant players in Iran's cyber efforts—both in terms of involvement by the Guards themselves and IRGC-backed and affiliated individuals and entities.[120] The relationship between the Guards and individuals and entities involved in hacking attempts against democracies (such as Charming Kitten) are not well-documented; however, it is clear that some of these entities are only loosely affiliated with the IRGC. These entities are often less driven by ideological alignment with the Guards and nationalism than they are by profit.[121] Hence, many such actors serve as contractors to the IRGC, which provides them with a "side hustle" to make more money.[122]

Additionally, the IRGC in general and IRGC intelligence in particular have also built a media ecosystem allowing them to overtly push propaganda and disinformation. The Guards operate a media conglomerate. Several outlets are officially and directly connected to the Guards and formally present its position and inject its viewpoint into the debate. Others are informally and loosely linked to the IRGC and serve to advance the Guards' narrative while operating under the guise of more independent outlets sanctioned by the force. Examples of IRGC-affiliated media outlets include Fars News and Tasnim with both English and Persian-language websites, as well as the aforementioned Mashgregh News. The Guards also operate a number of official and informal social media accounts on nearly all available platforms.

It is in part thanks to this presence that Soleimani was able to rise to become a well-known figure inside and outside Iran during the 2014-2020 timeframe, after decades in the shadows. The IRGC and its affiliates pushed and amplified content presenting Soleimani as the face of Iran's counter-ISIS efforts. The IRGC also controls a sprawling business network, which it has long leveraged to circumvent U.S. sanctions. The Guards are involved in illicit procurement and blackmarket activities; however, their involvement in malign finance designed to undermine democracy abroad seems fairly limited for now.

The Ministry of Intelligence and Security

The Ministry of Intelligence and Security (MOIS) operates under the executive branch and falls within the president's cabinet. Its mandate pertains to intelligence and counterintelligence, and the ministry operates domestically and internationally. Its efforts are often facilitated by the Ministry of Foreign Affairs, whose embassies and other diplomatic facilities can be leveraged in MOIS operations. The MOIS cooperates with the IRGC intelligence organization where the two entities' mandates dictate and their interests align. Initially, the two organizations were meant to complement each other, with the MOIS focusing on foreign issues and the IRGC intelligence organization on the domestic scene.[123] However, the two organizations have more overlap now than they did when they were established. In fact, the MOIS and the IRGC's intelligence have found themselves in competition with one another—a conflict that IRGC intelligence has won given its power and resources.[124] As with other authoritarian states, the Islamic Republic has created redundancies within its security apparatus, particularly in intelligence, for "coup-proofing" purposes and to ensure that a monopoly over core security assets would never be established and potentially leveraged to weaken the regime.

The MOIS' activities geared toward undermining democracy are even less well-documented than those of the

IRGC. This may be due in part to the Guards' primacy in cyberspace and in the realms of information manipulation and malign finance. Moreover, due to the IRGC's relatively high profile in the Iranian security food chain, in some cases, more effort has been made to understand its motivations and activities than those of parallel organizations engaged in similar activities. The MOIS is likely involved in information manipulation efforts.

The Ministry of Information and Communication Technology

The Ministry of Information and Communications Technology (ICT) is another part of the cabinet with a role in operations to undermine democracies abroad. It is involved in the development of some new tools and platforms used at home and abroad. Under Mohammad-Javad Azari Jahromi, Hassan Rouhani's young, technocratic ICT Minister, the ministry became an effective player in information operations in particular—with Jahromi himself serving as the face of a new generation of leaders in the Islamic Republic, one perceived to be more pragmatic and forward-leaning.[125] Jahromi's Twitter account seeks to present him as the face of technological progress in the country—highlighting his role in the space and drone programs, for example.

However, behind this fresh image, Jahromi has played a critical role in crushing dissent and demands for more democratization at home, and disrupting the flow of information to and from Iran at key junctures, including during the November 2019 protests. During that crisis, Tehran shut down the Internet (likely with significant help by the ICT) as it killed several hundred protestors within three days. Jahromi has thus served at once as a propagandist and proliferator of disinformation on behalf of the regime abroad while helping suppress information at home.

The Ministry of Foreign Affairs

The Ministry of Foreign Affairs (MFA) is another key player whose information manipulation efforts are noteworthy. The MFA serves as the face of Iran abroad, but it also acts as a conduit for Iran's intelligence operations in Europe and the United States, as well as all other countries where it has a presence. Unlike in Europe, where Iran has official embassies and consulates (aside from some periods of disruption, as was the case in the United Kingdom in 2011-15), Iran has a very limited diplomatic presence in the United States.[126] The Iranian mission in New York allows the regime to maintain access to the United Nations, and a permanent mission in Washington, D.C. facilitates services for Americans of Iranian descent, Iranian residents in the United States, Americans traveling to Iran, and other parties.

Typically, diplomatic facilities are also used for intelligence purposes, as well as cultural and religious exchange, and the promotion of the regime's ideology. During Rouhani's tenure, the MFA also gained more traction as Zarif has built a large Twitter following and often takes to U.S. media (including television and press) to counter the U.S. narrative on Iran and promote Iran's own narrative.[127] The relative success of Zarif's media and social media engagement in the United States and elsewhere likely contributed to the U.S. decision to add him to the sanctions list in 2019.

The foreign ministry has also often spearheaded diaspora outreach efforts (at times coordinated with and featuring the president). Given the large Iranian diaspora in key countries of interest for Iran, especially the United States and major European nations (Great, Britain, Italy, France, and Germany to name a few), the Iranian government seeks to leverage these groups to advance its interests. The MFA's public diplomacy outreach to the diaspora in the United States is facilitated by the ministry's Iranian Expatriates Division. Key goals of the division include: building an Iranian constituency in the West, presenting a positive image of Iran abroad, pushing for sanctions relief in the United States and Europe, and promoting business with Iran in Europe.

Similarly, the MFA has long conducted outreach to key influential groups and individuals, including in Congress, academia, and think tanks. Similarly to the Gulf Arab states' "expert trips," whose aim is to project a positive

image of those countries in the West by cultivating a network of friendly experts, Iran has undertaken similar initiatives with European participants in particular—as similar efforts with Americans are much more challenging. Moreover, in Europe, where direct diplomatic channels with Tehran are more robust, Iran has maintained conduits to influential individuals, civil society groups outside government, and the diaspora in order to present "its side of the story" via more credible and neutral intermediaries. For example, during his March 2020 Persian New Year address and amid the coronavirus outbreak, Zarif appealed to the Iranian diaspora's sense of patriotism to oppose U.S. sanctions, which he blamed for stymying Tehran's response to the pandemic.[128] Zarif has also used his platform to call out what he has described as European hypocrisy in condemning the treatment of Iranian protesters when it did not speak up about the treatment of American demonstrators during the racial justice protests that took place in the United States in spring 2020.

The Islamic Culture and Relations Organization

The Islamic Culture and Relations Organization (ICRO), which is housed within the Ministry of Culture and Islamic Guidance, is the entity in charge of exporting Iran's culture, ideology, and religion beyond its borders. The ministry is tasked with enforcing "proper conduct" and strict adherence to the revolutionary and religious laws and values within the country. A significant area of responsibility for the ministry is censorship; all cultural and artistic products, including books, the press, music, film, and video games are monitored and assessed to ensure they adhere to the regime's guidelines and laws. Abroad, the ICRO cultivates ties with countries and populations, and maintains ties with the Iranian diaspora around the globe (especially in Europe, North America, and the Middle East). In the United States, the ICRO has an office in New York City, and it has a presence in other key North American and European cities (thanks to cultural attachés posted at different embassies and consulates).[129] The organization is a player in Iran's information manipulation efforts.

The Islamic Republic of Iran Broadcasting

The Islamic Republic of Iran Broadcasting (IRIB) is the state-run media organization of Iran. In addition to broadcasting domestically in Persian, IRIB has developed branches broadcasting abroad and in different languages, as well. Today, the English-language PressTV, the Spanish-language HispanTV, the Arabic-language al-Alam, Sahar TV, and al-Kawthar all employ foreign nationals and broadcast for foreign audiences; although, several of these outlets are discontinuing their operations for various reasons, including a lack of funding stemming from U.S. sanctions, a lack of a coherent and cohesive view about their mandate, and low viewership.[130]

These 24-hour traditional media outlets now also have a presence on social media. PressTV has studios in Washington and London, as well as regional desks in key countries of interest for the Islamic Republic.[131] Iran's media infrastructure also tries to cater to the Iranian diaspora, including Iranian Americans and Europeans of Iranian descent, by broadcasting Persian-language programming via Jaam-e Jam. IRIB-linked accounts whose coordinated inauthentic activity has originated in Iran have focused on a number of countries, including the United States and the United Kingdom.[132] With some of these outlets, including PressTV, reportedly closing shop, IRIB may redirect some of the resources used for them to beef up covert activity or strengthen other ongoing overt activities.

Charitable Foundations

Charitable foundations (known in Persian as *bonyad*) are one of the most influential arms of the Iranian state. Their political influence within Iran and access to considerable sums of money and other resources makes them an important powerbroker in Iran and abroad. On paper, these non-profit entities are designed to carry out social services and, as such, they enjoy a number of benefits afforded to them by the Iranian state—including many offered by the U.S. government to non-profit organizations such as tax exemptions.[133] In reality, however, these organizations have a presence in key economic sectors in Iran and abroad. These foundations own land and are

engaged in an array of economic activities in Iran and elsewhere.

For example, the Imam Reza Shrine (an expansive complex which is built around the mausoleum of the eighth Shia Imam, Imam Reza, and which houses a number of other facilities such as mosques, libraries, and stores) is engaged in not only religious activities, but also business activities worth billions of dollars. In 2007, a *Wall Street Journal* report noted that the foundation owned three-quarters of the lands in the city of Mashhad, the country's second-largest city.[134] And the entity has only expanded since then. The foundation owns farms, mines, factories, and companies in Iran.[135] It has also built infrastructure elsewhere in the Middle East and North Africa region and it is currently building a bridge between Iraq and Syria, laying out water infrastructure in Lebanon, and looking to undertake projects as far afield as Algeria.[136]

Iran also operates religious centers outside of the country. There are organizations and mosques linked to the Iranian state in Europe and the United States. These help facilitate religious services for members of the Iranian diaspora, including performing religious ceremonies and issuing documentation for births, marriages, and deaths. But they also serve to spread the Iranian version of Shiism. The role of these organizations in the web of Iranian organizations involved in authoritarian efforts designed to undermine democracy requires closer examination.

Other Actors

As noted previously, different power centers within the system engage in an intricate bargaining game that allows them to shape national security policy debates and outputs. Ultimately, however, the outcome is the result of the unitary state's consensus. This strategy is then implemented by an array of actors, including many of the same players involved in the decision-making process. Iran's influence operations are conducted in a more decentralized manner than some other parts of its national security strategy. Entities and individuals with loose connections to the central authority design and implement these operations.

For example, a number of the hackers involved in recent efforts targeting U.S. institutions and persons were in fact contractors and only loosely connected to the regime. The level of command and control between the state and government bodies on the one hand and these entities on the other remains obscure but appears loose. Hence, many of these individuals and entities work as contractors for the regime and compete for these contracts—far from being ideological players, many appear mostly by money:

> In essence, in this system, the Iranian regime may not tell the contracted hackers precisely how and when to hit a target. Rather, the government lays out its priorities and what it wants to accomplish, and the middlemen and the hackers figure out how to best to achieve these objectives. In this system, hackers work on behalf of the Iranian regime when 'under contract' but also freelance and work on their own projects at the same time, some of which align with regime interests and some of which are purely criminal or commercial operations.[137]

Similarly, a web of other organizations has built a sprawling Internet presence that curates and promotes content pertaining to specific aspects of Iran's worldview. The Islamic Propaganda Office of the Qom Seminary (whose website includes Persian, English, and Arabic-language versions) promotes Islamic and revolutionary values and lifestyle, as well as anti-Western material.

Acknowledgements

The author would like to thank Laura Rosenberger and David Salvo for their helpful reviews of previous drafts of this report, as well as Nathan Kohlenberg, Tom Morley, and Kayla Goodson, without whom this project would not have been possible. The work also benefited tremendously from inputs by the rest of the team at the Alliance for Securing Democracy, including Kristine Berzina, Jessica Brandt, Zack Cooper, Rachael Dean Wilson, Lindsay Gorman, David Levine, Nad'a Kovalčíková, Joshua Rudolph, Bret Schafer, Sydney Simon, and Etienne Soula.

Endnotes

1 Rebecca Smith and Rob Barry, "America's Electric Grid Has a Vulnerable Back Door—And Russia Walked Through It," The Wall Street Journal, January 10, 2019.
2 Zak Doffman, "Chinese State Hackers Suspected Of Malicious Cyber Attack On U.S. Utilities," Forbes, August 3, 2019.
3 Joseph Berger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case," The New York Times, March 25, 2016; David E. Sanger, "U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam," The New York Times, March 24, 2016.
4 William Evanina, "Statement by NCSC Director William Evanina: 100 Days Until Election 2020," ODNI, July 24, 2020.
5 Ibid.
6 Lachlan Markay and Adam Ransley, "U.S. Intel Officials Eye Disinformation Campaign Targeting John Bolton's Family," The Daily Beast, August 8, 2019.
7 Collin Anderson and Karim Sadjadpour, "Iran's Cyber Ecosystem: Who Are the Threat Actors?" Chapter 3, Iran's Cyber Threat: Espionage, Sabotage, and Revenge, Washington: Carnegie Endowment for International Peace, January 4, 2018.
8 CNBC, "Iran accuses US of 'brazen' plan to change its government," June 28, 2017.
9 Bobby Ghosh, "Iran's fraught relationship with American goods is about to get a little more complicated," Quartz, December 11, 2015; AP, "Iran's supreme leader warns against importing US goods," November 1, 2015.
10 Golnaz Esfandiari, "Iranian Authorities Clip Bogus KFC's Wings," RFE/RL, November 4, 2015.
11 Fouad Izadi, "[Fouad Izadi: America-yeeha migooyand Iran 5 payetakht-e khavar-e mianeh ra control mikonad/hadaf-e America tajzieh-ye Iran ast]," Tasnim News, March 1, 2020; Tasnim News, "[Aya America jang-e hybrid-i ra alayh-e Iran aghaz karde ast?]", March 14, 2020.
12 Carl von Clausewitz, On War, Vol. 1., trans. J.J. Graham, London: Kegan Paul, Trench, Trubner, 1918, Chapter 1.
13 Mashregh News, "[The Do's and Don'ts of Cyber Diplomacy]." October 7, 2013.
14 In particular, Iran appears to be sharing cyber capabilities with key proxies, such as Lebanese Hezbollah. In recent years, Tehran has gradually provided some proxies with more sophisticated weapons and equipment, including precision weapons, which may have also translated into a similar uptick in the cyber realm. See Michael Eisenstadt, Iran's Lengthening Cyber Shadow, The Washington Institute for Near East Policy, July 2016.
15 United States House of Representatives, Committee on Homeland Security, "U.S.-Iran Tensions: Implications For Homeland Security," January 15, 2020, Testimony of Lt. Gen. (ret.) Vincent Stewart ("Stewart Testimony").
16 For a comprehensive account of Iran's relationship with Russia and China see, Dina Esfandiary and Ariane M. Tabatabai, Triple Axis: Iran's Relations with Russia and China, London: I.B.Tauris, 2018.
17 Jay Solomon, "U.S., Europe Face Divisions Over Iran Policy," The Wall Street Journal, May 21, 2017.
18 Mashregh News, "[The Do's and Don'ts of Cyber Diplomacy]."
19 Ibid.
20 Ibid.
21 Ibid.
22 Ibid.
23 Mashregh News, "[Cyber Diplomacy and Its Impact on Relations between Countries]." July 23, 2017.
24 Ibid.
25 Ibid.
26 Nicole Perlroth and David E. Sanger, "Iranian Hackers Target Trump Campaign as Threats to 2020 Mount," New York Times, October 4, 2019

27 "[Hillary Clinton and Iran]." Diplomacy-e Irani, April 21, 2016.
28 Emerson T. Brooking and Suzanne Kianpour, Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century, Section 4, Washington: Atlantic Council, February 11, 2020.
29 "[Hillary Clinton and Iran]." Diplomacy-e Irani; Raja News, "'Trump Raees Jomhur Shod!' Khoshhal Bashim Ya Narahat?! Aya Jang Dar Rah Ast ? BARJAM Che Mishavad?", November 11, 2016.
30 Raja News, "'Trump Raees Jomhur Shod!' Khoshhal Bashim Ya Narahat?! Aya Jang Dar Rah Ast ? BARJAM Che Mishavad?", November 11, 2016.
31 Twitter, "US Elections," accessed June 19, 2020; Jonathan Landay and Mark Hosenball, "Russia, China, Iran sought to influence U.S. 2018 elections: U.S. spy chief," Reuters, December 21, 2018.
32 Craig Timberg and Tony Romm, "It's not just the Russians anymore as Iranians and others turn up disinformation efforts ahead of 2020 vote," Washington Post, July 25, 2019.
33 Ibid.
34 Ibid.
35 Pierre Alonso, "L'Elysée – Messages sur l'Iran : l'identité d'Alexis Kohler usurpée sur Twitter," Libération, November 5, 2019.
36 Mehr News Agency, "France to Expel Members of MKO Terrorist Group: Report," November 5, 2019.
37 Madjid Zerrouky, Marc Semo, and Claire Bastier, "Le faux compte Twitter du consul de France à Jérusalem," Le Monde, July 25, 2019.
38 Ibid.
39 The MeK is a crypto-Shia cult-like group formerly designated by the United States and Europe as a terrorist group. The group has a history of committing acts of terrorism, including against US interests in Iran prior to 1979. The MeK's members were largely exiled (and many killed by the regime) after the revolution and have tried to rehabilitate their image over the past two decades, presenting themselves as an alternative to the Islamic Republic. The group enjoys little support in Iran but has expanded its activities and gained traction in the United States (among some political figures). In recent years, the MeK has built an apparatus (including "troll farms"), which operate against the regime (but also serve to try to shift the discourse in their own favor and against Iran in the United States). Despite being limited in its reach inside and outside Iran, Tehran continues to view the group as a significant threat. As a result, it is not unusual for Iran's influence operations to directly or indirectly include messaging about the MeK.
40 Federal Bureau of Investigation (FBI), et al., "Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, and CISA on Ensuring Security of 2020 Elections," Press Release, November 5, 2019
41 Jay Greene, et al., "Iranians tried to hack U.S. presidential campaign in effort that targeted hundreds, Microsoft says," Washington Post, October 4, 2019.
42 Kathryn Watson, "Chinese and Iranian hackers tried unsuccessfully to hack Biden and Trump campaigns, Google official says," CBS News, June 4, 2020.
43 Zolan Kanno-Youngs and Nicole Perlroth. "Iran's Military Response May Be 'Concluded,' but Cyberwarfare Threat Grows," New York Times, January 8, 2020.
44 Idrees Ali and Phil Stewart, "Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials," Reuters, October 16, 2019.
45 Nicole Perlroth and David E. Sanger, "Iranian Hackers Target Trump Campaign as Threats to 2020 Mount."
46 Anderson and Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," Chapter 3.
47 United States Senate, Select Committee on Intelligence, Statement for the Record of Daniel R. Coates, Worldwide Threat Assessment of the US Intelligence Community, January 29, 2019, pp. 4 ("Coates Statement for the Record").
48 Ibid, pp. 6.
49 Eisenstadt, "Iran's Lengthening Cyber Shadow."
50 Julian E. Barnes and Siobhan Gorman, "U.S. Says Iran Hacked Navy Computers," The Wall Street Journal, September 27. 2013.

51 Ibid.
52 Ibid.
53 Alan Blinder, et al., "Isolated and Adrift, an American Woman Turned Toward Iran," The New York Times, February 16, 2019.
54 Elias Groll, "Meet 'Charming Kitten,' the Iranian Hackers Linked to Air Force Defector," Foreign Policy, February 15, 2019.
55 Jon Cohen, "Massive cyberhack by Iran allegedly stole research from 320 universities, governments, and companies," Science, March 23, 2018.
56 Ibid.
57 Ibid.
58 Jack Stubbs and Christopher Bing, "Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead – sources," Reuters, May 8, 2020.
59 Anderson and Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," pp. 6.
60 Joseph Marks, "The Cybersecurity 202: Get ready for serious cyberattacks from Iran, experts say," Washington Post, January 13, 2020.
61 Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," The New York Times, January 8, 2013.
62 Marks, "The Cybersecurity 202: Get ready for serious cyberattacks from Iran, experts say."
63 New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), "Report Details Iran-Associated Cyber Activity Against Electric, Oil and Gas," January 21, 2020.
64 Fixler, Annie. "The Cyber Threat from Iran after the Death of Soleimani." Center for Combatting Terrorism at West Point, CTC Sentinel 13, no. 2 (February 2020): 20–29, pp. 21.
65 Jack Stubbs and Christopher Bing, "Special Report: How Iran spreads disinformation around the world," Reuters, November 30, 2018.
66 Coates Statement for the Record, pp. 6.
67 Brooking and Kianpour, "Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century," Section 4.
68 Yoel Roth, "Information operations on Twitter: principles, process, and disclosure," Twitter, June 13, 2019.
69 Facebook, 2020.
70 Aaron Stein, "FPRI Targeted in Online Disinformation Campaign," Foreign Policy Research Institute, January 6, 2020; Adam Rawnsley, "Anatomy of a Spoof: How an Iran-Aligned Disinformation Actor Targeted FPRI," Foreign Policy Research Institute, August 31, 2020.
71 Gabrielle Lim et al., "Burned After Reading: Endless Mayfly's Ephemeral Disinformation Campaign," The Citizen Lab, University of Toronto, May 14, 2019.
72 Reuters. "Iran's Khamenei says Floyd's killing exposes real nature of U.S." June 3, 2020.
73 Amber Frankland, et al., "Hamilton Weekly Report: June 6-12, 2020," The Alliance for Securing Democracy, June 16, 2020.
74 RFE/RL, "'Death To America' Aimed At Trump, Not Americans, Iran's Leader Says," February 8, 2019.
75 Ali Khamenei, Twitter post, November 27. 2014, 6:35 AM.
76 Ali Khamenei, Twitter post, December 28, 2014, 5:36 AM.
77 Ali Khamenei, Twitter post, December 24, 2014, 10:25 AM.
78
79
80 Betsy Woodruff Swan, "State report: Russian, Chinese and Iranian disinformation narratives echo one another," Politico, April 21, 2020.
81 Brooking and Kianpour, "Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century," Chapter 4.
82 Robbie Gramer and Emily Tamkin, "California Secessionist Leader Throws in Towel, Moves to Russia," For-

eign Policy, April 18, 2017.
83 Ibid.
84 Brooking and Kianpour, "Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century," Chapter 4.
85 FireEye, "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East," August 21, 2018.
86 Ibid.
87 Ibid.
88 The monarchists seek a return to the status quo ante in Iran, hoping to bring back the Pahlavi dynasty into power. This group has largely rallied behind Reza Pahlavi, the Shah's son, who currently resides in the United States.
89 Tasnim News, "[America Can Make No Mistake]," June 13, 2017.
90 Fars News Agency, Twitter post, April 9, 2020, 3:45 AM.
91 Ibid.
92 Tasnim News, Twitter post, April 1, 2020, 1:38 PM; Tasnim News, Twitter post, April 24, 2020, 1:52 PM; Tasnim News, "[The mask that Corona removed from the face of the West,]" April 18, 2020.
93 Tasnim News, "[The end of the Western management system and the beginning of the decline of the liberal order in the post-Corona era,]" April 29, 10.
94 Javad Zarif, Twitter post, March 29, 2020, 7:45 AM; Javad Zarif, Twitter post, March 26, 2020, 12:41 PM; Javad Zarif, Twitter post, March 25, 2020, 1:47 PM.
95 Zarif, March 29, 2020.
96 Tasnim News, "[Drug sanctions are an example of US terrorism in the field of healthcare,]" ; Khabar Online, "[Why does the U.S. say Iran is not a drug embargo, but Tehran says it is? And why is Washington's claim convincing?]"; Islamic Republic News Agency, "[Denied: US officials claim to lift drug embargo,]" April 18, 2016.
97 United States Institute of Peace, "Zarif on Growing U.S.-Iran Tensions," April 29, 2019.
98 Brooking and Kianpour, "Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century," Chapter 4.
99 Joshua Rudolph and Thomas Morley, "Covert Foreign Money: Financial Loopholes Exploited by Authoritarians to Fund Political Interference in Democracies," Alliance for Securing Democracy, August 18, 2020.
100 Michael Pompeo, "Statement on the Imposition of Financial Countermeasures on Iran," U.S. Department of State, Press Statement, June 21, 2019.
101 U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), "The Use of Exchange Houses and Trading Companies to Evade U.S. Economic Sanctions Against Iran," January 10, 2013.
102 U.S. Department of the Treasury, "Bonyad Support Network: IGRC's Financial Lifeline (October 2018)," accessed June 20, 2020.
103 Financial Action Task Force on Money Laundering (FATF), "High-Risk Jurisdictions subject to a Call for Action – 21 February 2020," February 21, 2020.
104 Ibid.
105 Ibid.
106 U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), "FinCEN Issues Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System," Press Release, October 11, 2018.
107 Donie O'Sullivan, "Exclusive: This site pays Americans to write 'news' articles. Signs indicate it originates in Iran," CNN, January 24, 2020.
108 Ibid.
109 Shafaqna, "[The American Herald Tribune examined: Protests in Iran; How the U.S. "clusters of violence" tactic failed,]" December 25, 2009.
110 Young Journalists Club, "[Reflection of the message of the Leader of the Revolution to the Western youth in

the regional and international media,]" December 30, 2015.
111 BBC, "Ayatollah Khamenei writes letter to Western youth," January 22, 2015.
112 Young Journalists Club, "[Reflection of the message of the Leader of the Revolution to the Western youth in the regional and international media.]"
113 Seth G. Jones and Danika Newlee, The United States' Soft War on Iran, Washington: Center for Strategic and International Studies, June 11, 2019.
114 Diana Stancy Correll, "109 US troops diagnosed with TBI after Iran missile barrage says Pentagon in latest update," Military Times, February 10, 2020.
115 Seth G. Jones and Danika Newlee, The United States' Soft War on Iran.
116 Christian von Soest, "Democracy prevention: The international collaboration of authoritarian regimes," European Journal of Political Research, 2015.
117 Ali Khamenei, "Decree Appointing Members of the Supreme Council of Cyberspace," Information Center of the Office for the Preservation and Publication of the Works of the Grand Ayatollah Seyyed Ali Khamenei, September 4, 2016.
118 Ibid.
119 Ibid.
120 Federal Bureau of Investigation, "IRGC-Affiliated Cyber Actors," February 8, 2019.
121 Elias Groll, "Meet 'Charming Kitten,' the Iranian Hackers Linked to Air Force Defector," Foreign Policy, February 15, 2019
122 Ibid.
123 Library of Congress (LoC), Federal Research Division, Iran's Ministry of Intelligence and Security: A Profile, Washington, December 2012.
124 Library of Congress (LoC), Federal Research Division, Iran's Ministry of Intelligence and Security: A Profile.
125 Rohollah Faghihi, "Is Iran's Information Minister the Islamic Republic's Emmanuel Macron?" Foreign Policy, October 25, 2019.
126 Laura Smith-Spark, "UK reopens its embassy in Iran as relations warm," CNN, August 23, 2015; U.S. Department of State, "Citizen services," U.S. Virtual Embassy Iran, accessed June 20, 2020.
127 Robin Wright, "Iran's Javad Zarif on the Fraying Nuclear Deal, U.S. Relations, and Holocaust Cartoons" The New Yorker, April 25, 2016; Christiane Amanpour and Javad Zarif, "Full transcript of Amanpour's interview with Iran's foreign minister," CNN, February 17, 2017.
128 Fararu, "[Zarif: Corona taught us the need to modernize governance,]" March 19, 2017.
129 Seth G. Jones and Danika Newlee, The United States' Soft War on Iran.
130 Ibid.
131 Ibid.
132 Facebook, "April 2020 Coordinated Inauthentic Behavior Report," May 5, 2020.
133 Seth G. Jones and Danika Newlee, The United States' Soft War on Iran.
134 Andrew Higgins, "Inside Iran's Holy Money Machine," The Wall Street Journal, June 2, 2007.
135 Ibid.
136 Ibid.
137 Fixler, Annie. "The Cyber Threat from Iran after the Death of Soleimani," pp. 23.