

# IRANIAN DIGITAL INFLUENCE EFFORTS: GUERRILLA BROADCASTING FOR THE TWENTY-FIRST CENTURY



Emerson T. Brooking  
Suzanne Kianpour

**The Digital Forensic Research Lab (DFRLab)** is a start-up incubated at the Atlantic Council and leading hub of digital forensic analysts whose mission is to identify, expose, and explain disinformation where and when it occurs. DFRLab promotes the idea of objective truth as a foundation of governance to protect democratic institutions and norms from those who would undermine them.

**The Atlantic Council's Middle East programming** provides a forum for informing and galvanizing the transatlantic community to work together to address the range of challenges and support opportunities for growth in the region. Through our sub regional, country-specific, and functional initiatives, we work with allies and partners in Europe and the wider Middle East to protect US interests, build peace and security, and unlock the human potential of the region. You can read more about our programs at <https://www.atlanticcouncil.org/programs/middle-east-programs/>.

# IRANIAN DIGITAL INFLUENCE EFFORTS:

## GUERRILLA BROADCASTING FOR THE TWENTY-FIRST CENTURY

Emerson T. Brooking  
Suzanne Kianpour

**Cover:** Iranians pose in front of anti-US murals of the former US embassy in Tehran, now repurposed as a museum. The murals were unveiled in 2019 to commemorate the fortieth anniversary of the Iranian Revolution. Their bright colors and striking aesthetic seem tailor-made for Instagram, which boasts at least twenty-four million Iranian users. Graphic: Kanishk Karan/Instagram; identities have been anonymized.

ISBN-13: 978-1-61977-086-7

© Atlantic Council 2020

All rights reserved.

No part of this publication may be reproduced without the written permission of the copyright owner.

Atlantic Council  
1030 15th Street, NW  
12th Floor  
Washington, DC 20005

Website: [www.atlanticcouncil.org](http://www.atlanticcouncil.org)

# ACKNOWLEDGMENTS

---

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this issue brief's conclusions.

This report is made possible by general support to the Atlantic Council's Middle East Programs and Digital Forensic Research Lab.

# TABLE OF CONTENTS

---

Executive Summary	2
Introduction	4
Double-Edged Sword: Information as Both Weapon and Existential Threat	6
Iran and the Internet	11
Iran’s Digital Influence Efforts	15
Iran’s Digital Influence Efforts in Context	19
Conclusions and Recommendations	22
Appendix: Additional DFRLab Resources on Iranian Influence Operations	24
About the Authors	26

## EXECUTIVE SUMMARY

---

Iran has invested significant resources and accumulated vast experience in the conduct of digital influence efforts. These clandestine propaganda efforts have been used to complement Iranian foreign policy operations for the better part of a decade. Nonetheless, Iranian influence capabilities have gone largely unstudied by the United States, and only came to widespread attention in August 2018 with the first public identification of an Iranian propaganda network. Following the US assassination of Iranian Major General Qasem Soleimani and a sharp escalation in US-Iranian tensions, it is important to understand the perspective, methods, and intent of Iranian influence efforts.

For Iran, information dominance represents a central focus of both foreign and domestic policy. Iran sees itself as engaged in a perennial information war: against Sunni Arab powers, against the forces of perceived Western neocolonialism, and particularly against the United States. Should the information conflict be lost, many Iranian officials believe the collapse of the state will soon follow. Accordingly, Iran has prioritized the development of digital broadcast capabilities that cannot be easily targeted by the United States or its allies.

Iran has also prioritized information control. Although Iran boasts roughly fifty-six million Internet users, these users must navigate a culture of censorship and frequent state intimidation. Following the 2009 Green Movement, the Iranian government came to see social media activism as enabling an existential threat. Authorities created special cyber-police units, built a new legal framework for Internet regulation, and outlawed most Western digital platforms. They also began to develop systems to remove Iranian users from the global Internet entirely.

In pursuit of foreign and domestic information dominance, Iran began operating Facebook and Twitter sockpuppets as early as 2010. As the United States and Iran entered into a period of rapprochement and negotiation, the number of accounts grew exponentially. These accounts have been used to launder Iranian state propaganda to unsuspecting audiences, often under the guise of local media reports. To date, Facebook has identified approximately 2,200 assets directly affecting six million users. Twitter has identified eight thousand accounts responsible for roughly 8.5 million messages.

Much of this Iranian content cannot be characterized as “disinformation.” In sharp contrast to the information operations of Russia, which routinely disseminate false stories with the aim of polluting the information environment, Iran makes less use

of obvious falsehood. Instead, Iran advances a distorted truth: one that exaggerates Iran’s moral authority while minimizing Iran’s repression of its citizens and the steep human cost of its own imperial adventures in the wider Middle East.

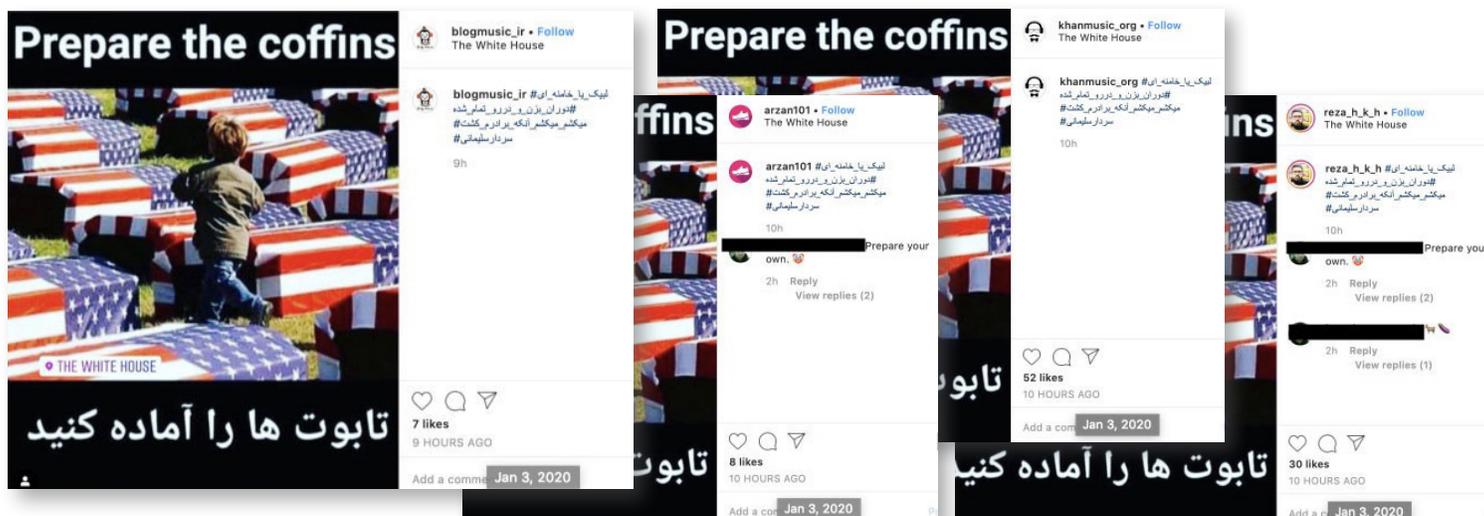
As a whole, Iran’s digital influence operations represent a continuation of public diplomacy, albeit conducted through misleading websites and social media sockpuppets. Iran broadcasts a fairly consistent message to many different audiences: in Africa, in Southeast Asia, in Europe, in North America, and, most notably, in Latin America and the Middle East. The aim of these efforts is to “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.

As the United States considers policies to safeguard its elections and confront Iranian influence activities, three conclusions can be drawn about the nature of Iran’s modern propaganda apparatus.

- 📶 Iran’s digital influence efforts involve centralized goals and disparate agents. Different elements of Iran’s digital propaganda apparatus evidence the involvement of different government agencies. It is not clear how, or if, these agencies coordinate their operations.
- 📶 These goals are closely tied to Iran’s geopolitical interests. Nearly all content spread by Iran’s digital influence efforts relates directly to its worldview or specific foreign policy objectives. Consequently, it is easier to identify the operations of Iran than those of other actors like Russia, whose content is more likely to be politically agnostic.
- 📶 Iran may attempt direct electoral interference in 2020 and beyond. To date, there is little evidence that Iran has sought to affect the outcome of a US election. This does not, however, preclude future such campaigns based on Iranian interest in achieving rapprochement with the United States.

Additionally, five steps can be taken to better prepare the United States to meet this threat.

- 📶 The US Global Engagement Center (GEC) should invest resources in identifying and neutralizing—but not editorializing about—Iran’s digital influence networks.



As US-Iranian tensions sharply escalated in January 2020, Iranian Instagram accounts spammed the White House and members of the Trump family with images of flag-draped coffins. Source: Kanishk Karan/Instagram

Through its funding of the Iran Disinformation Project, an independent organization that launched vociferous attacks (without evidence) on allegedly “pro-Iranian” US journalists, the GEC inadvertently damaged the credibility of efforts to counter Iranian influence.<sup>1</sup> A more effective approach would be to invest US resources in organizations that track and identify Iran’s digital influence networks without over-editorializing their findings.

- 📶 The US Department of State should address regular press briefings to the Iranian people. Official US press briefings, addressed to the Iranian people, have traditionally been widely disseminated and received. By using such a megaphone, the United States could push back against Iran’s propaganda apparatus in a strong, cost-effective manner.
- 📶 The US Agency for Global Media (USAGM) should not engage in overt pro-US influence operations. Iranians are savvy media consumers who have traditionally sought out diverse points of view. They are less inclined to embrace obvious pro-Western propaganda.
- 📶 The Office of the Director of National Intelligence (ODNI) should independently attribute foreign influence operations. In January 2017, the ODNI attributed a significant foreign influence operation to Russia.<sup>2</sup> In nearly three years since,

dozens more disinformation campaigns have been publicly identified and attributed—but only by corporations like Facebook, Google, and Twitter. US intelligence services should work with social media companies to attribute future foreign influence operations.

- 📶 The Department of Homeland Security (DHS) should create an appropriate intergovernmental entity to publicize foreign influence operations. Although the US intelligence services should work to defend the American people against foreign disinformation campaigns, they are not the entities that should publicize these operations on a regular basis. Instead, that job should fall to an organization modeled on the National Cyber Awareness System of the Cybersecurity and Infrastructure Security Agency (CISA) and under the purview of DHS, which can communicate regular advisories across the US government and to the population at large.

In 2011, Iran’s former intelligence minister, Heidar Moslehi, remarked, “We do not have a physical war with the enemy, but we are engaged in heavy information [warfare].”<sup>3</sup> At the time of Moslehi’s speech, Iran had just begun to seed the digital landscape with fabricated websites and social media personas. Today, it commands tens of thousands of them, waging an information war that shows no sign of ending.

1 Julian Borger, “US Cuts Funds for ‘Anti-propaganda’ Iran Group That Trolled Activists,” *The Guardian*, May 31, 2019, <https://www.theguardian.com/us-news/2019/may/31/us-cuts-funds-for-anti-propaganda-group-that-trolled-activists>.  
 2 “Assessing Russian Activities and Intentions in Recent US Elections,” Intelligence Community Assessment, Office of the Director of National Intelligence, January 6, 2017, [https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf).  
 3 “Iran Adopts Aggressive Approach Toward Enemies,” *Tehran Times*, July 18, 2011, <https://www.tehrantimes.com/news/244231/Iran-adopts-aggressive-approach-toward-enemies>.

# INTRODUCTION

---

Social media has fundamentally transformed the nature of foreign influence activities. Today's propagandists can cheaply and effectively influence the populations of distant nations, sharing micro-targeted content while masking their identities. Although this phenomenon came to the attention of many Western observers only after successful Russian interference in the 2016 US election, non-Western states have invested in digital influence capabilities for more than a decade. One pioneer is the Islamic Republic of Iran.

Modern Iran, born from Islamic revolution and engaged in a 41-year cold war with the United States, has been quick to study and exploit new communications technologies. This is the case even as it restricts use by its own citizens. Following the 2009 Green Movement—a series of pro-democracy protests, enabled by Twitter and other platforms, that threatened the stability of Iran's theocratic government—Iranian propagandists vowed to use social media for their own ends.

By 2011, Iran claimed to have built “cyber battalions” that totaled more than eight thousand members trained in blogging, content production, and multimedia design.<sup>4</sup> The same year, Iran was seeding Twitter with bots that it would use to steer international debate; it established the first of countless Facebook accounts that would share political content under false pretexts and fake identities.<sup>5</sup> By 2015, Iran had expanded the scope of its digital influence efforts to include platforms like Reddit, where it sought to shape perceptions of the Syrian Civil War.<sup>6</sup> By 2018, Iran had developed sophisticated online personas that it used to launder propaganda through individual journalists and to even publish letters in regional US newspapers.<sup>7</sup> By 2020, and

following the US assassination of Iranian Major General Qasem Soleimani, Iran was using this apparatus to mount continuous influence operations against the United States.

Even as Western observers placed new emphasis on digital influence in the aftermath of the 2016 US election, they remained largely unaware of Iranian activities in the space. A number of suspicious Iranian tweets, identified by independent researchers, were initially misattributed to Russia. The first major identification of Iranian influence activities came in August 2018, published by the cybersecurity company FireEye.<sup>8</sup> Facebook, Twitter, and Reddit followed with their own announcements, as they each dismantled pieces of the network. This was just the beginning. As of January 2020, Iranian influence activities have been the subject of seven additional takedown announcements by Facebook and Twitter, as well as numerous routine content-moderation actions. Only Russian activities have received more attention.

As focus on Iranian influence efforts has grown, however, so have misperceptions about the nature of these operations. There is a tendency to refer to these cumulative Iranian influence activities as “disinformation”: what the Digital Forensic Research Lab (DFRLab) of the Atlantic Council defines as false or misleading information spread with the intention to deceive. The US Department of the Treasury has characterized all Iranian broadcasts as “disinformation.”<sup>9</sup> For a time, the US Department of State funded the “Iran Disinformation Project,” the stated mission for which was to “bring to light disinformation emanating from the Islamic Republic of Iran.”<sup>10</sup> There is a temptation among some US politicians to blame Iranian “disinformation” for a wide range

---

4 “Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran,” *Article 19* (February 2017): accessed January 24, 2020, [https://www.article19.org/data/files/medialibrary/38619/Iran\\_report\\_part\\_2-FINAL.pdf](https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf)

5 “Taking Down More Coordinated Inauthentic Behavior,” Facebook, last updated August 21, 2018, <https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/>; Ben Nimmo, Graham Brookie, and Kanishk Karan, “#TrollTracker: Twitter Troll Farm Archives,” *DFRLab*, October 17, 2018, <https://medium.com/dfrlab/trolltracker-twitters-troll-farm-archives-17a6d5f13635>.

6 Daniel Amir, “Analysis: A Brief Guide to Iran on Reddit,” *BBC Monitoring*, January 2, 2019, <https://monitoring.bbc.co.uk/product/c200it6l>.

7 Alice Revelli and Lee Foster, “Network of Social Media Accounts Impersonates U.S. Political Candidates, Leverages U.S. and Israeli Media in Support of Iranian Interests,” *FireEye*, May 28, 2019, <https://www.fireeye.com/blog/threat-research/2019/05/social-media-network-impersonates-us-political-candidates-supports-iranian-interests.html> Gabrielle Lim et al., “Burned After Reading: Endless Mayfly’s Ephemeral Disinformation Campaign,” *CitizenLab*, May 14, 2019, <https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflies-ephemeral-disinformation-campaign/>.

8 “Suspected Iranian Influence Operation,” *FireEye* (August 2018), accessed January 24, 2020, <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-FireEye-Iranian-IO.pdf>.

9 US Department of the Treasury, “Treasury Designates Iran’s Foreign Minister Javad Zarif for Acting for the Supreme Leader of Iran,” July 31, 2019, <https://home.treasury.gov/news/press-releases/sm749>.

10 Iran Disinformation Project, “About Us,” accessed on January 24, 2020, <https://irandisinfo.org/about-us/>; Borger, “US Cuts Funds.”



Iranian government proxies operated unattributed Facebook pages devoted to praise of Ayatollah Ali Khamenei and condemnation of the Palestinian occupation. This particular network was removed in May 2019. Source: DFRLab/Facebook

of political obstacles—even including the anti-war movement within the United States.<sup>11</sup>

Although Iran has certainly engaged in the spread of falsehood, this does not represent the majority—or even a significant portion—of its known digital influence efforts. While Iran makes systematic use of inauthentic websites and social media personas, the actual content it disseminates is a mirror of its state propaganda: biased in Iran’s favor and contrary to US interests, but seldom wholly fabricated. If the principal intent of Russia’s digital influence efforts is to distract and dismay, Iran’s goal is most often to persuade. Where Russia uses clandestine means to play both sides of a political issue against each other, Iran uses clandestine means to amplify one side as loudly as possible. The goal is to build a guerrilla broadcasting apparatus that cannot be easily targeted by the United States or its allies.

This issue brief examines the history, development, and operation of Iran’s digital influence efforts, placing them in the broader context of Iranian security and foreign policy

objectives. This work is based on a reading of literature regarding Iran’s conceptualizations of information warfare and international broadcasting, as well as all available analyses of Iran’s clandestine activities on social media platforms. It is supplemented by a review of the DFRLab’s archive of Iranian-operated Facebook pages.

Although this is the most comprehensive effort of its sort, the DFRLab could not directly translate all languages used in Iranian propaganda, nor can it be guaranteed that currently available open-source information provides a comprehensive view of Iranian influence efforts. This study, like all studies of social media manipulation, is subject to change as more facts emerge.

This brief begins with a discussion of the modern Iranian state’s approach to information and information control. It proceeds to a history of the Iranian Internet. Next, it examines the evolution of Iranian digital influence operations, followed by a discussion of the broader information conflict in which they take place. The brief concludes by considering the future nature and intent of Iran’s clandestine digital activities.

11 Marco Rubio (@marcorubio), “URGENT 3/5: The also believe that our internal political divisions combined with the legacy of the #IraqWar will lead a substantial % of Americans to doubt #Iran’s role in such attacks or blame Trump. & they have built propaganda capability to spread narrative in social media,” Twitter, May 15, 2019, <https://twitter.com/marcorubio/status/1128633764584808449>.

## DOUBLE-EDGED SWORD: INFORMATION AS BOTH WEAPON AND EXISTENTIAL THREAT

The Islamic Republic of Iran came into being partly through the control and manipulation of information. Ayatollah Ruhollah Khomeini's sermons, smuggled into the country via audio cassettes and distributed widely, helped give birth to the Islamic Revolution. Following the establishment of a theocratic government in 1979, religious authorities used a mix of bombastic propaganda and brutal censorship to consolidate their political power and demonize potential opponents. Accordingly, information dominance represents a central focus of both foreign and domestic policy. Iran sees itself as engaged in a perennial information war: against Sunni Arab powers, against the forces of perceived Western neocolonialism, and particularly against the United States. Should the information conflict be lost, many Iranian officials believe the collapse of the state will soon follow.



Nineteenth-century portrayal of the 1514 Battle of Chaldiran, which marked a catastrophic defeat for the Safavids at the hands of the Ottoman Empire. The battle set the stage for centuries of imperial and religious conflict. Source: Agha Sadeq/Wikimedia

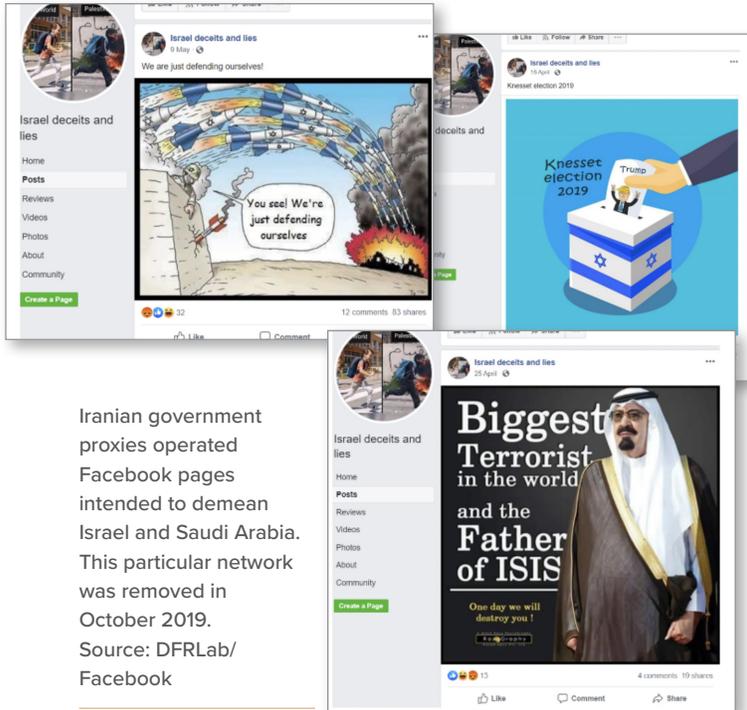
Iran has conceived of itself as a beacon of Shia Islam since 1501, which saw the founding of a new Persian empire under the Safavid dynasty. The Safavid shahs embraced Shia Islam and used the resultant religious fervor to reunite old Persian provinces under their rule. Iran presented itself as an alternate leader of the Muslim world: one destined to clash sharply with the Sunni Islamic Ottoman and Abbasid caliphates to the west. At its peak, Iran controlled Baghdad, Bahrain, and western Afghanistan. Even as Iranian influence receded, as the leading Shia power, Iran's rulers would continue to feel responsible for Shia minorities around the region. Iran would also continue a pattern of religious and ideological warfare against Saudi Arabia and other descendants of the Sunni caliphates.

Through the nineteenth and twentieth centuries, Iran prided and defined itself by its resistance to Western colonial adventures. That changed in 1953, at which time the United States and the United Kingdom overthrew Iran's democratically elected government in order to reverse the nationalization of Iranian oil production. The shah of Iran, with support of the military and Western intelligence agencies, suspended constitutional protections and consolidated political power. For the next twenty-six years, opposition parties ceased to operate and the media was strictly controlled.

Only the religious establishment enjoyed relative freedom of speech and assembly. Its discontent culminated with the 1979 Islamic Revolution by the exiled preacher Ruhollah Khomeini.<sup>12</sup> These revolutionaries framed their movement as a successful resistance to Western neocolonialism. Iran began to cultivate ties with other Islamic or anti-Western revolutionary movements—in Saudi Arabia, in Egypt, and (most successfully) in Lebanon, as well as farther afield in nations like Bolivia and Venezuela. Iran also came to despise Israel, which it saw as a Western imperial project.

The 1979-81 hostage crisis, in which Iranian revolutionaries imprisoned fifty-two US diplomats and citizens at gunpoint, marked a decisive moment in both Iranian and US history. Images of blindfolded US officials, their hands tied behind their backs, were carried by television broadcasts around the world. For Iran, these images demonstrated the strength of the revolution. For the United States, they sowed anger and humiliation in a generation of policy makers.

12 Annabelle Sreberny-Mohammadi, "Small media for a big revolution: Iran," *International Journal of Politics, Culture, and Society* 3, no. 3 (1990): 341-371.



Iranian government proxies operated Facebook pages intended to demean Israel and Saudi Arabia. This particular network was removed in October 2019. Source: DFRLab/Facebook

and invested hundreds of millions of dollars to support Iranian dissidents and opposition groups.<sup>14</sup>

The diplomatic efforts under President Barack Obama that led to the negotiation of the 2015 Iran nuclear deal, formally known as the Joint Comprehensive Plan of Action (JCPOA), saw a softening of rhetoric from both nations. Cyberattacks from Iran appeared to decrease when the JCPOA was in force.<sup>15</sup>

However, US-Iranian tensions increased sharply again under President Donald Trump, following his May 2018 decision to withdraw the United States from the JCPOA. Iran further dismissed new US sanctions, applied as part of a “maximum pressure” strategy, as tantamount to economic terrorism.<sup>16</sup> With the US assassination of General Soleimani in January 2020 and Iranian military retaliation, the two countries have edged closer than ever to open military conflict.

This US-Iran cold war has left many Iranian policymakers with a siege mentality in which the government lies under constant threat. One solution has been to invest heavily in a national narrative and share it with the world—to portray

Although US-Iranian relations waxed and waned in the decades following the 1979 revolution and subsequent hostage crisis, they entered steep decline in the early 2000s. Following the 9/11 terrorist attacks, Iran initially found itself on the same side of the United States against the Afghanistan Taliban, which had lent support to al-Qaeda and which had marginalized non-Pashtun ethnic groups. But as the United States prepared to invade Iraq, some voices within the George W. Bush Administration lobbied for a subsequent attack on Iran. This culminated in President Bush’s 2002 State of the Union address that named Iran to the “Axis of Evil” alongside Iraq and North Korea. The Iranian government, freshly remembering the devastating 1980-1988 Iran-Iraq War, was shocked.

When the United States invaded Iraq in 2003, Iran maneuvered to ensure its agents of influence would be included in the Iraqi opposition that the United States would rely upon to form a new Iraqi government. As post-invasion US troop levels soared and US rhetoric grew more bellicose, Iran feared a prelude to direct attack. Accordingly, Iran provided arms and training to Shia militias fighting the US occupation, accounting for the deaths of at least six hundred US military personnel.<sup>13</sup> Concurrently, the United States expanded economic sanctions



Above: Blindfolded US hostages and their Iranian captors outside the US embassy in Tehran, Iran, in 1979. Source: US Army/Handout via Reuters



Above right: US students protest in Washington DC during the 1979-81 Iran hostage crisis. Source: Marion Trikosko/Wikimedia

13 Kenneth Katzman, *Iran’s Foreign and Defense Policies*, Congressional Research Service, CRS-7-5700 R44017 (2017), updated on July 23, 2019.

14 Office of the Spokesman, “Update on Iran Democracy Promotion Funding,” US Department of State Archive, June 4, 2007, <https://2001-2009.state.gov/r/pa/prs/ps/2007/jun/85971.htm>

15 Andy Greenberg, “The Iran Nuclear Deal’s Unraveling Raises Fears of Cyberattacks,” *Wired*, May 9, 2018, <https://www.wired.com/story/iran-nuclear-deal-cyberattacks/>

16 Luiz Martinez, “Iran’s Foreign Minister Javad Zarif says US Sanctions are ‘economic terrorism,’” *ABC News*, June 2, 2019, <https://abcnews.go.com/Politics/irans-foreign-minister-javad-zarif-us-sanctions-economic/story?id=63355661>

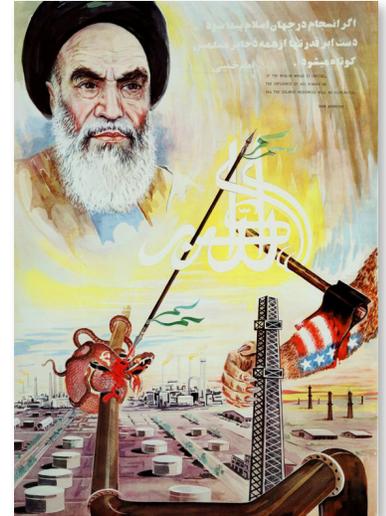
## IRANIAN DIGITAL INFLUENCE EFFORTS GUERRILLA BROADCASTING FOR THE TWENTY-FIRST CENTURY

Iran as a religious beacon, as an anti-imperialist stalwart, and as a perennial underdog vis-à-vis the United States. In turn, this has necessitated that Iran maintain a strong propaganda apparatus for both domestic control and foreign influence. Doing so is not simply a “want,” but is considered integral to the state’s survival.

Accordingly, state monopoly over television and radio broadcasting is mandated by Article 44 of the Iranian Constitution.<sup>17</sup> The head of Iran’s state propaganda agency, Islamic Republic of Iran Broadcasting (IRIB), is appointed by the theocratic supreme leader rather than Iran’s elected president or parliament.<sup>18</sup>

Despite growing economic turbulence and the mounting effects of US sanctions, the IRIB maintains an annual budget of approximately \$750 million.<sup>19</sup> This is roughly equivalent to the budget of the United States Agency for Global Media (USAGM, known as the Broadcasting Board of Governors until 2018).<sup>20</sup> As a proportion of total government spending, however, Iran invests about fifty times as much in the IRIB as the United States does in the USAGM.<sup>21</sup> The IRIB claims more than thirteen thousand employees in more than twenty countries.<sup>22</sup> In 2013, the United States formally sanctioned the IRIB, citing its campaigns of censorship and distortion.<sup>23</sup>

Within Iran, the IRIB operates twelve radio channels and forty-seven regional and national television channels; it also owns the Jam-e Jam newspaper, one of Iran’s largest print publications. Yet, the IRIB represents just one instrument of domestic influence. Other state institutions, like the Ministry of Culture and Islamic Guidance, administer their own newspapers and control the systems of funding and licensing that dictate the editorial positions of Iran’s quasi-independent press. The Office of the Supreme Leader runs another major newspaper and oversees a network of conservative publications that are answerable only to the religious authorities. The Islamic Revolutionary Guard Corps (IRGC) has its own affiliated press operations, as does Iran’s major labor union, which itself exists under the government’s watchful



Iranian propaganda has long been suffused with a resistance to neocolonialism, evidenced by these 1980s posters. In the first (left), an Iranian fist crushes an Iraqi jet emblazoned with the flags of the United States and Soviet Union. In the second (right), radiant weapons attack embodiments of the United States and Soviet Union, which seek Iran’s natural resources. Source: University of Chicago Library

eye.<sup>24</sup> Although these news organizations offer competing views of the world, the spectrum of “acceptable” beliefs is dictated by state censors.

Internationally, the IRIB operates thirty radio channels and nine television networks.<sup>25</sup> This scale of foreign broadcasting significantly increased following the US invasion of Iraq.<sup>26</sup> Today, some of IRIB’s most prominent foreign-facing initiatives are: Al Alam, an Arabic-language station launched in 2003; PressTV, an English-language station launched in 2007; and Hispan TV, a Spanish-language station launched in 2011 and focused on Latin America. In 2016, the IRIB launched Pars Today, a consolidated news agency for IRIB’s international broadcasting efforts that offered programming in thirty-two

17 Alberto Zanconato and Farian Sabahi, “Iran – Media Landscapes,” European Journalism Centre, accessed January 24, 2020, <https://medialandscapes.org/country/iran>

18 Ibid.

19 “IRIB Budget Doubles,” *Financial Tribune*, January 15, 2017, <https://financialtribune.com/articles/economy-domestic-economy/57517/irib-budget-doubles>; Kevin Breuninger, “Trump Sanctions Iran’s Central Bank in Wake of Strikes on Saudi Oil Facilities,” *CNBC*, September 20, 2019, <https://www.cnbc.com/2019/09/20/trump-sanctions-iranian-national-bank-in-wake-of-strikes-on-saudi-oil-facilities.html>

20 “IRIB Budget Doubles.”

21 Iran claims to invest \$750billion in its broadcaster/propaganda agency, the IRIB. We also invest roughly \$750billion in ours (strictly foreign broadcast), the USAGM.

22 Zanconato, “Iran – Media Landscapes.”

23 “Treasury Announces Sanctions Against Iran,” US Department of the Treasury, February 6, 2013, <https://www.treasury.gov/press-center/press-releases/Pages/tg1847.aspx>

24 Zanconato, “Iran – Media Landscapes.”

25 Ibid.

26 Linda Robinson et al. “Modern Political Warfare: Current Practices and Possible Responses,” *Rand Corporation* (2018), 131.

languages.<sup>27</sup> “Islamic Iran is facing a broad media war and the IRIB is at the forefront of this new war,” said the IRIB president of the venture.<sup>28</sup>

This conception of “media war” is owed to the international broadcasts that have long composed a significant part of Iran’s media environment. The oldest of these is Radio BBC, which began its Farsi programming in 1940 and exerted significant political and cultural influence over the Iranian elite, especially prior to the 1979 revolution.<sup>29</sup> Other foreign radio stations include: Radio Zamaneh, based in the Netherlands; Deutsche Welle, based in Germany; Radio France Internationale; and Voice of Israel. With the advent of cheap satellite dishes in the mid-1990s, foreign television broadcasts became widely popular, despite a ban on home satellite use. The first targeted television broadcast was Voice of America-Persian News Network, launched in 1996. BBC Persian launched in 2009, drawing a regular audience of more than ten million. According to a 2010 survey by BBC Monitoring, 40 percent of Iranians were watching foreign satellite broadcasts.<sup>30</sup>

Since 9/11, and with an increasing military presence in the Middle East, the United States has sought to expand its Iran-focused broadcasting. In 2002, the then-Broadcasting Board of Governors (BBG) launched Radio Farda, intended to strengthen its previous radio efforts.<sup>31</sup> Throughout the 2000s, the BBG reduced or eliminated programs in other regions (notably Eastern Europe), while expanding funding for Iranian content.<sup>32</sup> In 2006, the Bush Administration and the US Congress authorized the Iran Democracy Fund, which would allocate tens of millions of dollars to BBG broadcasts, as well as to Iranian opposition groups, many of which had media outlets of their own.<sup>33</sup> Although this effort was softened under the Obama Administration, it has further escalated under the “maximum pressure” strategy of President Donald Trump. The fiscal year 2019 appropriations bill for the US Department of State expressly directed Secretary of State Mike Pompeo to consult with the USAGM to coordinate “counterinfluence programs” against Iran.<sup>34</sup>

These foreign broadcasting efforts are perceived as a grave threat by the Iranian government. Since the mid-2000s and the



A collage of IRIB-branded television channels and other media properties. Proportional to its national budget, Iran spends roughly fifty times as much as the United States on such broadcasting initiatives.

27 “Iran Launches ‘Pars Today’ News Outlet,” *PressTV*, July 5, 2016, <https://www.presstv.com/Detail/2016/07/05/473779/Iran-IRIB-Pars-Today-Abdolali-AliAskari-Mohammad-Akhgari>.

28 Ibid.

29 Sreberny-Mohammadi, “Small Media for a Big Revolution,” 364; Zanconato, “Iran – Media Landscapes.”

30 Zanconato, “Iran – Media Landscapes.”

31 Foad Izadi, “US International Broadcasting: The case of Iran,” *The Journal of Arts Management, Law, and Society* 39, no. 2 (2009): 132-148.

32 Izadi, “US International Broadcasting,” 136.

33 Price Monroe, “Iran and the Soft War,” *International Journal of Communication* 6 (2012): 2402-2403.

34 Department of State, Foreign Operations, And Related Programs Appropriations Bill, S. Rep. 115-282 (2019).



This cartoon portrays an Iranian citizen protesting Iran's presence in Gaza and Lebanon. Although he holds an Iranian flag, he has been radicalized by the Voice of America, BBC, and Gulf state media and is secretly controlled by Israel. The cartoon was shared by an unlabeled Iranian propaganda network on Instagram, removed in March 2019. Source: Facebook/Instagram

“color revolutions” that swept Georgia, Ukraine, and Lebanon, IRGC indoctrination has instilled fear within Iran of a similar revolution fomented by a US-led coalition.<sup>35</sup> With the 2009 Green Movement and the amplification of pro-democracy activists by Western media, Iranian officials saw their worst fears realized. They called it “soft war.”<sup>36</sup> The Islamic Development Organization, a supervisory religious and cultural body created by the supreme leader shortly after the 1979 revolution, described the conduct of soft war as follows:

[E]conomic malady, creation of discontent in the society, establishment of non-governmental organizations, war of media, and psychological operation in order to show government as a weak state...The elements of subversion use the present arenas in the society in order to reach their purposes; also, they try to create discord among the public opinion.<sup>37</sup>

Countering soft war became an all-consuming task. In 2010, Iran labeled sixty media and international organizations as “soft war agents,” prohibiting their operations within the country.<sup>38</sup>

The Iranian Ministry of Defense authorized a dedicated soft-war military force, devoted to cultural preservation and psychological operations, in which even Iranian elementary schools were conceived as potential battlefields.<sup>39</sup> In 2015, Ayatollah Ali Khamenei warned an assembled group of IRGC commanders that “economic and security infiltration” was less a threat than “intellectual, cultural, and political infiltration.”<sup>40</sup> The control and manipulation of information was inextricably linked to national security.

Accordingly, Iran’s conventional military and IRGC planning emphasize informational control for both defense and offense. Iranian strategists see a conflict in which Iran is continually on the defensive: against hostile US, British, and Saudi broadcasters; against Israeli and Iranian opposition lobbying in the United States; and against a global information environment from which Iran is largely excluded due to accumulating sanctions.

As Iranian policymakers sought new ways to defend against foreign influence and shift to the information offensive, their attention would inevitably turn to the Internet.

35 Saeid Golkar, “Iran’s Revolutionary Guard: Its views of the United States,” *Middle East Policy* 21, no. 2 (2014): 54.

36 Monroe, “Iran and the Soft War,” 2398.

37 “Soft War Reasons Against Islamic Republic of Iran,” *Islamic Development Organization*, January 2, 2010, <http://old.ido.ir/en/en-a.aspx?a=1388101204>

38 Monroe, “Iran and the Soft War,” 2402.

39 Ibid, 2407-2408.

40 Robinson, “Modern Political Warfare,” 127.

# IRAN AND THE INTERNET

Iran embraced the Internet early and aggressively, recognizing it as a new medium by which the state could strengthen its hand at home and improve broadcasting overseas. Iran's universities joined the global network in 1993, following behind only Israel as the second Middle East nation to embrace the digital age.<sup>41</sup> Initially, the Iranian government did not impose any censorship restrictions. It was thought that a free, unfettered Internet would serve the dual purposes of advancing scientific research and spreading Islamic scripture.<sup>42</sup> Gradually, however, Iran would impose severe limitations on digital communications. With time, the Iranian Internet would become increasingly paradoxical: a rich digital culture increasingly beset by religious authorities who seek to turn it to their own ends.

By the early 2000s, the Internet seemed poised to reshape Iranian society. Although the web offered a new platform to spread Islamic teachings, it also offered a refuge where forbidden ideas could be discussed freely. Many young Iranians took full advantage of the opportunity. In 2001, there were 1,500 Internet cafes in Tehran alone.<sup>43</sup> Blogging became a popular pastime; after the creation of the first Farsi-language blog in 2001, tens of thousands would shortly follow.<sup>44</sup> These politically engaged online communities joined with reform-minded politicians and clerics, creating a push for liberalization that touched most aspects of Iranian society.<sup>45</sup> For a theocratic state ruled by deeply suspicious religious scholars, a conservative backlash was inevitable.

The first major act of digital censorship came in 2001, when Iranian courts asserted control over Internet service providers (ISPs) and subjected them to strict monitoring and censorship standards. This was an extension of a general suppression of opposition media that began in 2000.<sup>46</sup> Following the 2003 US

invasion of Iraq, censorship enforcement became stricter and Iranian authorities began the first widespread arrest and torture of dissident bloggers.<sup>47</sup> Yet, the pattern of repression was still uneven. When the conservative Mahmoud Ahmadinejad ran for president in 2005, for example, he did so promising to roll back restrictions on digital speech. At voting booths in Tehran, Iranians talked excitedly of this modern candidate, in a suit as opposed to clerical garb, promising to open the window to a digital world from which they had been increasingly isolated.

As Iranian authorities were coming to see the Internet as a threat, foreign broadcasters saw new opportunity. BBCPersian.com, which launched in 2001, soon became the BBC's most popular non-English website (it would be blocked by Iran in 2006, although many visitors would find ways to circumvent the ban).<sup>48</sup> In 2003, the BBG created a free proxy service that enabled Iranians to continue to visit the websites of Radio Farda and Voice of America, despite mounting censorship efforts.<sup>49</sup> By the mid-2000s, the US government was investing significant resources in Iran-targeted websites and Internet programming, while young Iranians gravitated to new Western social media platforms like Facebook and Twitter.<sup>50</sup> At the same time, the Iranian government increasingly identified the Internet as the vector through which the United States and its allies were most likely to wage their "soft war."<sup>51</sup>

What remained of the free Iranian Internet was dealt a crippling blow in the aftermath of the 2009 Green Movement. Dozens of bloggers were arrested and detained indefinitely. Facebook and Twitter were blocked. That same year, the IRGC bought a controlling stake in the Telecommunication Company of Iran, the state's principal ISP, bringing Iranian Internet users under tighter surveillance.<sup>52</sup> In 2011, Iran created a "cyber police" unit, which quickly became infamous for detaining a thirty-

41 Babak Rahimi, "Cyberdissent: The Internet in revolutionary Iran," *Middle East Review of International Affairs* 7, no. 3 (2003): 101-115.

42 Ibid.

43 Ibid.

44 Nasrin Alavi, *We are Iran: The Persian blogs*, (Brooklyn: Soft Skull Press, 2005).

45 Rahimi, "Cyberdissent."

46 "False Freedom: Online censorship in the Middle East and North Africa," *Human Rights Watch* 17 no. 10(E) (November 2005): 42.

47 Ibid.

48 "Iran Blocks BBC Persian Website," *BBC*, January 24, 2006, [http://news.bbc.co.uk/2/hi/middle\\_east/4644398.stm](http://news.bbc.co.uk/2/hi/middle_east/4644398.stm).

49 Kevin Poulsen, "US Sponsors Anonymiser – If You Live in Iran," *The Register*, August 29, 2003, [https://www.theregister.co.uk/2003/08/29/us\\_sponsors\\_anonymiser\\_if\\_you/](https://www.theregister.co.uk/2003/08/29/us_sponsors_anonymiser_if_you/)

50 Izadi, "US International Broadcasting," 143.

51 Monroe, "Iran and the Soft War."

52 Zanonato, "Iran – Media Landscapes."



Tens of thousands of Iranians took to the streets to protest irregularities in the 2009 Iranian presidential election. These protests soon became known as the “Green Movement.” In their aftermath, Iranian authorities began to infiltrate and co-opt the digital platforms used by democratic activists. Source: Milad Avazbeigi/Wikimedia

five-year-old blogger and torturing him to death.<sup>53</sup> In 2012, Iran announced a Supreme Council of Cyberspace, which placed Internet regulation more directly in the hands of religious—not secular—authorities.<sup>54</sup> In recent years, Iran has sought ever more control of online spaces, following government consensus that the Internet has become an information battleground, a tool of soft war, to be harnessed by the state and rationed to the people.

More sophisticated surveillance, coupled with regular arrest and imprisonment for “propaganda against the state,” has strangled Iran’s independent journalistic community, even under the watch of the ostensibly moderate President Hassan Rouhani.<sup>55</sup> The government has also begun to crowdsource censorship to thousands of volunteers, who report speech violations to judicial authorities.<sup>56</sup> All the while, Iran continues its slow work on the so-called “National Internet Project,” initiated in 2011,

53 Ibid.

54 Kristin Deasy, “Supreme Council of Cyberspace, New Online Oversight Agency, to Launch in Iran,” *PRI*, March 7, 2012, <https://www.pri.org/stories/2012-03-07/supreme-council-cyberspace-new-online-oversight-agency-launch-iran>

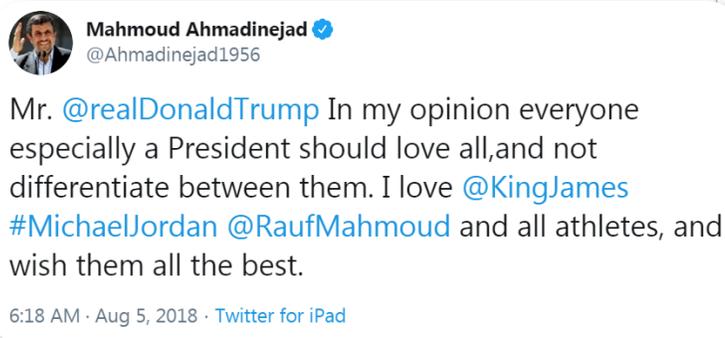
55 Heshmat Alavi, “Analysis: How to Define Iran’s Hassan Rouhani as a ‘Moderate,’” *Al Arabiya*, May 29, 2017, <https://english.alarabiya.net/en/features/2017/05/29/How-to-define-Iran-s-Hassan-Rouhani-as-a-moderate-.html>

56 “Iran’s Revolutionary Guard Targets 450 Social Media Users,” *Seattle Times*, August 23, 2016, <https://www.seattletimes.com/nation-world/irans-revolutionary-guard-targets-450-social-media-users/>.

which envisions the creation of a wholly separate Internet.<sup>57</sup> This “halal” digital ecosystem, free from foreign websites and influence, would allow complete awareness of all Internet traffic in the country—and total control over user data and speech. In May 2019, Iran announced that this system was 80 percent complete, although many questions remain regarding the effectiveness and feasibility of its implementation.<sup>58</sup>

The most significant test of Iran’s new Internet controls came in November 2019, when the government raised fuel prices by 50 percent overnight, sparking widely attended protests in at least one hundred cities.<sup>59</sup> Iranian censors sprang into action, eliminating Internet access in the country for ninety hours—and slowing it to a crawl for days thereafter.<sup>60</sup> By measure of scale and effectiveness, it was the largest Internet shutdown in history.<sup>61</sup> Over that period, police and security officials responded with violence, killing as many as 1,500 unarmed protestors over the course of a month.<sup>62</sup> Despite the staggering death toll, however, the communications blackout effectively starved the protestors of contemporaneous international support.

Yet, even with these tightening government controls, some fifty-six million Iranians—70 percent of the population—are now regular Internet users.<sup>63</sup> Many banned services, like Facebook, still enjoy widespread domestic popularity, thanks to the evasion of Internet filters and toleration by some state enforcers (in 2017, there were still as many as forty million Iranian Facebook users).<sup>64</sup> Today, the locus of Iranian digital life is the fashion-friendly Instagram (at least twenty-four million users) and the encrypted Telegram (at least forty million users, despite a limited ban).<sup>65</sup> Yet, as the Iranian people have found new online refuges, authorities follow close behind. On Instagram,



In recent years, both Ayatollah Ali Khamenei and former Iranian president Mahmoud Ahmadinejad have launched popular English-language Twitter feeds in a bid to communicate with the wider digital public. This occurs even as Twitter remains forbidden to the Iranian people. Source: Twitter



57 “Tightening the Net: Internet Security and Censorship in Iran Part 1: The National Internet Project,” *Article 19* (March 2016), accessed January 24, 2020, <https://www.article19.org/data/files/medialibrary/38315/The-National-Internet-AR-KA-final.pdf>.

58 “Iran Says Its Intranet Almost Ready to Shield Country from ‘Harmful’ Internet,” *Radio Farda*, May 20, 2019, <https://en.radiofarda.com/a/iran-says-its-intranet-almost-ready-to-shield-country-from-harmful-Internet/29952836.html>.

59 Peter Kenyon, “Higher Gasoline Prices in Iran Fuel Demonstrations,” *NPR Morning Edition*, podcast audio, November 19, 2019, <https://www.npr.org/2019/11/19/780713507/higher-gasoline-prices-in-iran-fuel-demonstrations>.

60 “Internet disrupted in Iran Amid Fuel Protests in Multiple Cities,” *Netblocks*, November 15, 2019, <https://netblocks.org/reports/Internet-disrupted-in-iran-amid-fuel-protests-in-multiple-cities-pA25L18b>.

61 Tamara Qiblawi, “Iran’s ‘Largest Internet Shutdown Ever’ is Happening Now. Here’s What You Need to Know,” *CNN*, November 18, 2019, <https://edition.cnn.com/2019/11/18/middleeast/iran-protests-explained-intl/index.html>.

62 “Special Report: Iran’s Leader Ordered Crackdown on Unrest – ‘Do Whatever It Takes to End It,’” *Reuters*, December 23, 2019, <https://www.reuters.com/article/us-iran-protests-specialreport/special-report-irans-leader-ordered-crackdown-on-unrest-do-whatever-it-takes-to-end-it-idUSKBN1YR0QR>.

63 “Iran,” *Internet World Stats*, accessed January 24, 2020, <https://www.internetworldstats.com/me/ir.htm>.

64 Zanconato, “Iran – Media Landscapes.”

65 Fariba Parsa, “Forget Telegram: Iranians are Using Instagram to Shop,” *Atlantic Council*, October 17, 2019, <https://atlanticcouncil.org/blogs/iransource/forget-telegram-iranians-are-using-instagram-to-shop/>.

## IRANIAN DIGITAL INFLUENCE EFFORTS GUERRILLA BROADCASTING FOR THE TWENTY-FIRST CENTURY

state-aligned trolls harass and threaten users, particularly women, who are perceived to act in an “un-Islamic” fashion.<sup>66</sup> On Telegram, the administrators of popular discussion groups have been regularly summoned by the IRGC, which reminds them that they are being watched.<sup>67</sup>

Ironically, as Iran has curtailed Internet freedom for its own citizens, the state has greatly expanded its use of social media platforms for diplomacy and propaganda abroad. These public-facing activities have been most prominent on Twitter. In 2013, President Rouhani famously shared his desire for rapprochement with the United States via his English-language Twitter account.<sup>68</sup> Soon thereafter, Ayatollah Khamenei—who had registered a Twitter account shortly after the 2009 Green Revolution—also began to regularly tweet in English,

commenting on issues like the 2014 Black Lives Matter protests in Ferguson, Missouri.<sup>69</sup> Even former President Ahmadinejad, who himself oversaw the banning of Twitter in 2009, joined the platform in 2018 to build his foreign following. His seemingly innocuous sports commentary briefly made him a US social media celebrity.<sup>70</sup>

Yet, the increasing Twitter activity of Iranian politicians represents just the most visible piece of a much broader digital influence campaign.<sup>71</sup> In the last five years, the major foreign broadcasting initiatives of the IRIB—Al Alam, PressTV, Hispan TV, and Pars Today—have all established significant web presences. At the same time, Iran has seeded a vast network of social media sockpuppets and fabricated websites, forging a new kind of propaganda apparatus in the process.

---

66 Simin Kargar and Adrian Rauchfleisch, “State-aligned trolling in Iran and the double-edged affordances of Instagram,” *New Media & Society* 21, no. 7 (2019): 1506-1527.

67 “Iran’s Revolutionary Guard.”

68 Christophe Lachnitt, “Twitter Revolutionizes International Relations,” *Superception*, October 6, 2013, <https://www.superception.fr/en/2013/10/06/twitter-revolutionizes-international-relations/>.

69 Kay Armin Serjoie, “Why the Twitter Account Believed to Belong to Iran’s Supreme Leader Keeps Mentioning Ferguson,” *Time*, December 3, 2014, <https://time.com/3618706/iran-ferguson-u-s-twitter/>.

70 Joseph A. Wulfsohn, “Slate Publishes Puff Piece on Mahmoud Ahmadinejad, Calls Him a ‘Lovable Twitter Rascal,’” *Fox News*, December 12, 2018, <https://www.foxnews.com/entertainment/slate-publishes-puff-piece-on-mahmoud-ahmadinejad-calls-him-a-lovable-twitter-rascal>.

71 Golnaz Esfandiari, “Iranian Politicians Who Use Twitter Despite State Ban,” *RadioFreeEurope Radio Liberty*, August 28, 2017, <https://www.rferl.org/a/iranian-politicians-twitter-ban/28701701.html>.

# IRAN'S DIGITAL INFLUENCE EFFORTS

Iran operates an immense web of online personas and propaganda mills, virtually none of which disclose their affiliation with the Iranian government. The first major attribution of Iran's foreign influence efforts was made in August 2018 by the cybersecurity company FireEye.<sup>72</sup> In the eighteen months since, disclosures by social media platforms and journalists have shed light on operations that began as early as 2008. These operations have targeted dozens of nations with tens of millions of pieces of content, varying widely in their message and intent. By studying these known influence campaigns in aggregate, one can infer much about the diverse actors that spread propaganda on behalf of the Iranian government, as well as the different objectives that Iran intends to accomplish by targeting its efforts across so many nations and regions.

First, it is useful to review the social media assets that have been definitively attributed to Iran. As of January 2020, Facebook has publicly identified: 766 pages followed by 5.4 million users; fifty-five groups joined by 143,000 users; 1,114 Facebook accounts; and 344 Instagram accounts followed by 439,000 users. Facebook has further attributed forty-three 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 forty-three accounts.

There can be no guarantee that this represents the sum of Iranian efforts on these platforms.

Broadly, Iran's foreign influence efforts evidence a level of routinization that distinguish it from Russia, China, Saudi Arabia, or any other nation that has built a digital influence apparatus. This is a result of the early integration of digital manipulation into Iranian government and military functions. In 2009, Ayatollah Khamenei stated that "content promotion" was "the most effective international weapon" against foreign adversaries.<sup>73</sup> In 2011, the head of the IRIB bragged that he had developed seven cyber battalions of "media experts and specialists," supposedly consisting of 8,400 members.<sup>74</sup> Tehran's IRGC headquarters has trained thousands of recruits in "content production," teaching them social media strategy and graphic design.<sup>75</sup> Given this heavy and longstanding emphasis, it is likely that many elements of the Iranian state—the IRIB, the office of the supreme leader, the intelligence services, the IRGC and associated militias, and the regular Iranian military—each employ their own Internet operatives.

Many Iranian influence efforts are intended to launder Iranian state media through seemingly unconnected sources. To this end, Iranian proxies operate a dizzying number of "independent" news outlets. These websites regularly copy



Logos of the International Union of Digital Medium (IUVM), a cluster of ostensibly independent websites that aggressively repackaged and re-broadcast Iranian state media. The cluster operated, undetected, for five years before being identified in August 2018.

Source: DFRLab/ivumnews.com

<sup>72</sup> "Suspected Iranian Influence Operation."

<sup>73</sup> "Tightening the Net Part 2," 28.

<sup>74</sup> Ibid, 29.

<sup>75</sup> Ibid, 28.

## IRANIAN DIGITAL INFLUENCE EFFORTS GUERRILLA BROADCASTING FOR THE TWENTY-FIRST CENTURY

the source material of Pars Today and other IRIB broadcasters, as well as official Iranian government press releases. In a bid for more content, they also plagiarize from wire services like Reuters and the Associated Press, as well as from Russian, Venezuelan, and Syrian state media.<sup>76</sup> Dozens of such low-effort, high-output websites have been launched by Iranian proxies, beginning as early as 2012.<sup>77</sup> In contrast to similarly structured commercial content mills, none of these websites feature advertising.

An example of this phenomenon can be seen in the International Union of Virtual Media (IUVM), a cluster of ostensibly independent news outlets that began operations

In practice, the IUVM demonstrated the sheer size and complexity of Iran's information-laundering apparatus. The IUVM regularly tweaked and republished official IRIB stories, only to have its articles republished, in turn, by other Iranian propaganda mills. In one case, the IUVM reproduced a message to pilgrims by Ayatollah Khamenei, taken from his personal website. The same day, a wholly different Iran-linked website ("britishleft.com") reproduced the story and shared it with its own audience.<sup>80</sup> In this fashion, a single piece of content could be passed from one website to the next, each with a different readership and editorial style.

A significant portion of Iran-attributed Twitter activity has sought to drive social media users to this underground propaganda network. In 2014, for instance, an Iranian botnet bombarded French journalists and commentators with twenty-three thousand links to a story that promised to reveal, "What they will never tell you about Christmas."<sup>81</sup> Other botnets turned the headlines of Iranian state media reports into seemingly original tweets: "U.S. has wiped Raqqah off the face of the earth" or "[ISIS]...Fails to Prevail over Syrian Army Positions in Eastern Deir Ezzur."<sup>82</sup>

Although Iranians masqueraded as any number of different Twitter users—an unemployed French journalist, or a Venezuelan football commentator—they put little effort into establishing convincing identities or infiltrating the wider political dialogue. Instead, they relentlessly promoted their own material, willing to rapidly switch from one persona to another if it could improve their chances of engagement. In one case, an account that was called "Liberty Front Press" (named after an Iranian propaganda front) abruptly changed its username to "Berniecrats." Even with the sudden identity switch, however, the account's content remained the same.<sup>83</sup>

Sometimes, such Iranian spam tactics proudly broadcast their origin. In January 2019, following Secretary of State Pompeo's announcement of a summit on Iran and Middle East security, his official Instagram page was bombarded by thousands of mostly identical anti-American comments, many garnished with Iranian flags.<sup>84</sup> In January 2020, following the US assassination of General Soleimani, Iranian Instagram accounts tagged the



In a "digital flex," Iranians spammed the Instagram account of Secretary of State Mike Pompeo in January 2019. Source: DFRLab/Instagram

in 2013 and continued until its discovery in 2018. The IUVM's main website declared its intention "to become the largest virtual media network across the globe, in line with our steadfast determination to defend the oppressed peoples of the world."<sup>78</sup> It offered a line of associated properties: IUVMPress and IUVMTV, which functioned as news and video aggregators; IUVMApp, which offered "halal" smartphone games and Quranic education; and even IUVMPixel, which featured a range of anti-Saudi and anti-US comic strips. The IUVM also offered links to dozens of "member" websites, all of which were clearing houses for Iranian propaganda.<sup>79</sup>

76 Ben Nimmo, "#TrollTracker: An Iranian Messaging Laundromat," *DFRLab*, August 29, 2018, <https://medium.com/dfrlab/trolltracker-an-iranian-messaging-laundromat-218c46509193>.

77 See AWD News creation date, "Homepage," *AWD News*, February 6, 2012, <https://web.archive.org/web/20120801000000/http://awdnews.com/>.

78 "About Us," *IUVM*, May 29, 2017, <https://web.archive.org/web/20170529205709/http://iuvm.org/en/about/>.

79 "IUVM Members," *IUVM*, December 25, 2014, <https://web.archive.org/web/20141225232542/http://iuvm.org/members>.

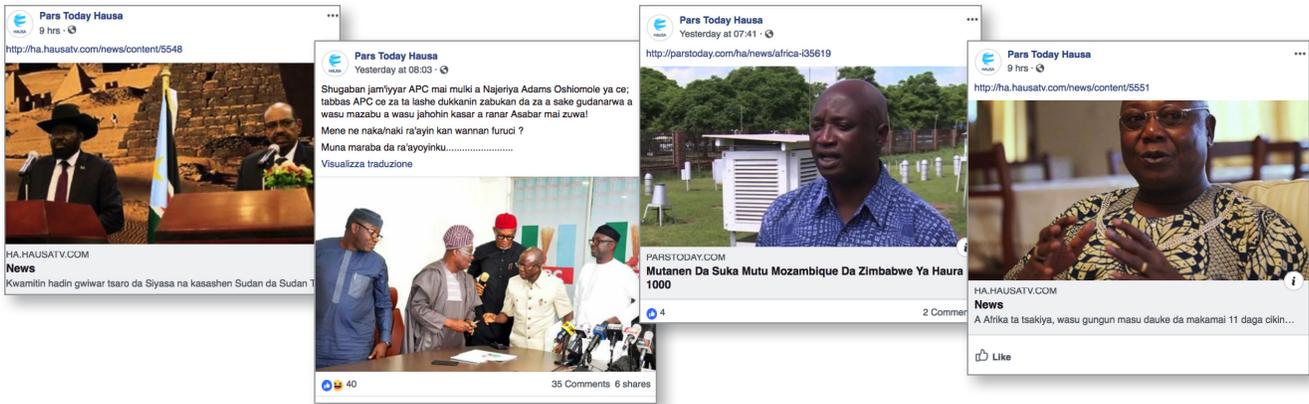
80 Ben Nimmo, "#TrollTracker: An Iranian Messaging Laundromat."

81 Karan, "#TrollTracker: Twitter Troll Farm Archives."

82 Ibid.

83 Ibid.

84 Melissa Hall and Kanishk Karan, "#TrollTracker: Spam Attack on Secretary Pompeo," *DFRLab*, February 25, 2019, <https://medium.com/dfrlab/trolltracker-spam-attack-on-secretary-pompeo-d2ab638f0b5e>.



“Pars Today Hausa” shared content related to Sudanese politics, Nigeria’s All Progressive Congress, crises in Mozambique, and conflicts in the Central African Republic between armed groups and political leaders. It was removed in April 2019. Source: DFRLab/Facebook

White House and members of the Trump family with thousands of graphic, anti-American images and memes.<sup>85</sup> Analyst Cindy Otis described this as a “digital flex,” intended to demonstrate the strength and volume of Iran’s digital communications apparatus.<sup>86</sup>

Atop this network of propaganda mills and Twitter boosters, Iranian proxies operate a vast network of content-focused Facebook and Instagram pages. Some of these seek to drive traffic to Iranian state media or associated websites; others act as standalone news outlets, laundering Iranian propaganda through yet another seemingly unconnected source. Through

Facebook especially, Iran has built hundreds of region-specific pages that have reached millions of users in every corner of the world.

Some of these pages make little effort to disguise their identities. In March 2019, for instance, Facebook removed a network of pages with names like “Pars Today Hausa” (which translated Iranian broadcasts into Hausa) and “Pars Today Bangla” (which did the same for Bengali).<sup>87</sup> This network targeted Facebook users in Nigeria, Bangladesh, India, and Kazakhstan. In case there was any doubt as to the operation’s origins, its administrators listed their location as Iran—and their employer as the IRIB.<sup>88</sup>



“Pars Today Bangla” shared content related to Turkish and Australian politicians, European wariness of artificial intelligence advancements, Chinese innovations, and Saudi Arabian leadership. It was removed in April 2019. Source: DFRLab/Facebook

85 Kanishk Karan, “Tensions Escalate on Social Media Platforms After Soleimani’s Death,” *DFRLab*, January 4, 2020, <https://medium.com/dfrlab/tensions-escalate-on-social-media-platforms-after-soleimanis-death-48f295ecec5e>.  
 86 Jane Lytvynenko and Jeremy Singer-Vine, “A Pro-Iran Instagram Campaign Targeted The Trump Family After Soleimani’s Funeral,” *Buzzfeed*, January 8, 2020, <https://www.buzzfeednews.com/article/janelytvynenko/iran-instagram-trump-campaign>.  
 87 Melissa Hall, Kanishk Karan, and Emerson T. Brooking, “Facebook Dismantled Iranian Influence Operation,” *DFRLab*, April 19, 2019, <https://medium.com/dfrlab/facebook-dismantled-iranian-influence-operation-e7ff859763a8>.  
 88 Ibid.

## IRANIAN DIGITAL INFLUENCE EFFORTS GUERRILLA BROADCASTING FOR THE TWENTY-FIRST CENTURY



Comparison of an Iranian Facebook facsimile, @AlArabyi (top) with the verified version, @AlArabiya (bottom). Although the two pages appeared identical, they broadcast diametrically opposed messages. The Iranian lookalike was removed in May 2019.

Source: DFRLab/Facebook

Other pages go to considerable lengths to cover their tracks. A massive Arabic and English-language influence network, removed by Facebook in January 2019, managed to operate since 2010 while offering few clues about its origins.<sup>89</sup> Instead, the pages (with names like “Stop Killing Palestinian Children” and “Yemen Not Alone”) managed to blend into a broader community of anti-Israeli, anti-Saudi activists.<sup>90</sup> Few Facebook users inclined to share the content of such pages would be disposed to check—or care—if the same content had been previously shared by Iranian state propagandists.

Recently, Iranian proxies have grown bolder in their attempts to undermine or co-opt foreign media outlets. Sometimes, it is as straightforward as a misleading domain name (“tel-avivtimes.

com”), intended to disguise an offshoot propaganda website as a credible local news source.<sup>91</sup> Other times, it involves a mix of plagiarism and creative misspellings, like appending the BBC logo to an Instagram page called “bbcgraphy,” or stealing the Radio Farda logo for an Instagram page called “radiofardaaaaaa.” One cleverly mislabeled Facebook page, “AlArabyi” (similar to the name of a major Saudi-funded broadcaster) accumulated five thousand followers while sharing ardently pro-Iranian material and claiming the real “AlArabiya.net” as its homepage.<sup>92</sup>

A tiny portion of Iranian influence activities demonstrate a level of sophistication that differs markedly from other efforts. These suggest the work of a military organization or intelligence agency rather than that of an IRIB civil servant or patriotic troll farm. In May 2019, Citizen Lab uncovered an advanced network of social media personas and look-alike websites that sought to target and launder content through individual Western journalists.<sup>93</sup> These Iranian proxies showed familiarity with the major actors and influencers within the US Middle East policy community. They also proved adept at social engineering, often masquerading as young women and engaging in extended conversations to cultivate trust in their targets.

In one case, an Iranian sockpuppet pressured a US-based journalist to amplify a false story that claimed a former Israeli defense minister had been dismissed for being a Russian agent. The story was wrapped in a picture-perfect copy of the website of Harvard Kennedy School’s Belfer Center for Science and International Affairs. The only indication was the domain name: “belfercenter.net” instead of “belfercenter.org.”<sup>94</sup> All told, Citizen Lab counted one hundred and thirty-five articles, seventy-two domains, eleven social media personas, and one hundred and sixty persona-authored stories that composed the operation.<sup>95</sup> This was testament to just how far Iran’s digital influence efforts have evolved in the past decade—and how they might develop in the years ahead.

89 Ibid.

90 Ibid.

91 Ibid.

92 Kanishk Karan, Ayushman Kaul, and Ben Nimmo, “Facebook Removes Iran-based Assets. Again,” *DFRLab*, May 30, 2019, <https://medium.com/dfrlab/facebook-removes-iran-based-assets-again-f17358ef21f>

93 Lim et al., “Burned After Reading.”

94 Ibid.

95 Ibid.

# IRAN'S DIGITAL INFLUENCE EFFORTS IN CONTEXT

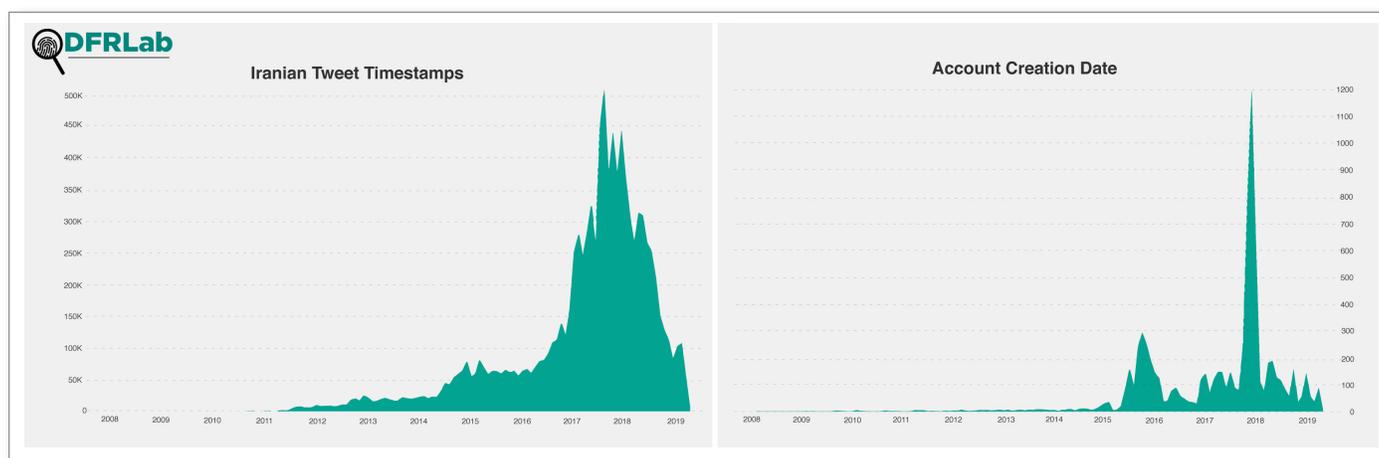
Iran has built a prolific online influence apparatus. Over time, the Iranian government has realigned its propaganda efforts to meet evolving foreign policy goals. It has also been forced to adapt by events beyond its control, often battling its own clumsiness along the way. By considering the general content and context of Iranian influence operations, it is possible to distinguish them from the disinformation campaigns of Russia and other US adversaries.

As a whole, Iran's digital influence operations represent a continuation of public diplomacy, albeit conducted through misleading websites and social media sockpuppets. Iran invests significant energy injecting pro-Iranian content into the information environments of countries that offer little direct strategic utility. For instance, Iranian proxies have built numerous websites and Facebook pages targeting audiences in Indonesia, which boasts the largest Muslim population in the world.<sup>96</sup> They have done the same for Nigeria, which has the largest Muslim population in Africa, and which includes a restive Shia minority.<sup>97</sup> The 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.

Where Iran turns this apparatus against the United States and its allies, it is often to achieve definable foreign policy objectives. In 2014, for example, Iran helped amplify a Lebanese conspiracy theory that the United States had created the self-declared Islamic State of Iraq and al-Sham (ISIS).<sup>98</sup> The clear objective was to blunt US soft-power efforts in Lebanon and to strengthen the relative position of the Iranian-backed Hezbollah, which was engaged in its own propaganda battle. Iran exhibits similar behavior in its routine amplification of Palestinian civilian deaths at the hands of the Israeli Defense Forces, the killing of Yemeni civilians by the Saudi-led coalition, or its focus on the toll of US air strikes in Iraq and Syria. Each is intended to diminish the image of US-aligned powers, while masking Iran's role in these and other proxy conflicts.

More broadly, it is no coincidence that Iranian-attributed Twitter activity saw its most significant spikes in mid-2015 and mid-2018. The first spike aligned with the contentious US domestic debate regarding adoption of the JCPOA, which set limits on Iranian nuclear development; the second aligned with the



Graph of the timestamps and account creation dates of roughly 8.5 million tweets by 8,000 Iranian government-linked accounts, operating between 2008 and 2019. Note activity spikes during mid-2015 and mid-2018. These correspond with the US accession to and subsequent withdrawal from the JCPOA. Source: Kanishk Karan/DFRLab

96 Ben Nimmo et al., "In Depth: Iranian Propaganda Network Goes Down," *DFRLab*, March 26, 2019, <https://medium.com/dfrlab/takedown-details-of-the-iranian-propaganda-network-d1fad32fdf30>.

97 Hall, "Facebook Dismantled Iranian Influence Operation."

98 "The US, IS and the Conspiracy Theory Sweeping Lebanon," *BBC*, August 12, 2014, <https://www.bbc.com/news/world-middle-east-28745990>.

## IRANIAN DIGITAL INFLUENCE EFFORTS GUERRILLA BROADCASTING FOR THE TWENTY-FIRST CENTURY

unilateral US withdrawal from that same agreement. For Iran, this digital influence apparatus represents a natural and potent tool to achieve its geopolitical ends.

Critically, Iran has so far demonstrated little interest in directly affecting US elections. In 2016, Iranian proxies briefly operated a Facebook page that sought to boost the candidacy of Senator Bernie Sanders (D-VT) in the Democratic presidential primary. The effort gained little engagement, however, and lasted only a month before going dormant.<sup>99</sup> It appears that this was an experiment by Iranian propagandists, who subsequently abandoned it for other influence efforts less focused on direct foreign electioneering. More recently, Iranian proxies have sought to compromise email accounts linked to the Trump re-

election campaign, although the objectives and extent of this effort remain unknown.<sup>100</sup>

Instead, Iranian interference in US politics has almost exclusively taken the form of websites, Facebook pages, and Twitter accounts that seek to redirect left-leaning causes to their own ends. An example can be seen in “BLMNews.com,” a relatively popular US outlet identified as an Iranian asset by Facebook in October 2019, which used the language and iconography of the Black Lives Matter movement to launder Iranian state propaganda to progressive activists.<sup>101</sup> The expected stories about US race relations were intermingled with a surprisingly heavy focus on US sanctions policy and the humanitarian work of Lebanon’s Hezbollah. When Iranian propagandists produce material that glorifies particular Western politicians or social movements, it is almost exclusively in the context of advancing a clear Iranian foreign policy objective.

In this way, Iran’s approach to digital influence operations differs sharply from that of Russia. Where Russian sockpuppets may infiltrate either side of a political debate—and often both sides at once—Iranian proxies are fairly consistent in their positions. Where Russia routinely disseminates false stories with the aim of polluting the information environment, Iran makes less use of obvious disinformation (although its messaging is still obviously biased). Where the Russian approach is essentially nihilistic, intended to erode the very nature of “truth,” Iran advances a distorted truth that exaggerates Iran’s moral authority, while minimizing Iran’s repression of its citizens and the steep human cost of its own imperial adventures in the wider Middle East.

Yet, for all the investment that Iran has made in digital influence, it is still the underdog in the broader information struggle. As Iran has developed its social media manipulation capabilities, so have committed Iranian adversaries like Saudi Arabia, the United Arab Emirates, and Israel.<sup>102</sup> In August 2019, for instance, Facebook identified a series of Saudi propaganda assets that sought to undermine Iran’s reputation. With names like “Free Iran,” the pages shared glitzy infographics that highlighted Iran’s high levels of drug addiction or its historic massacre of political prisoners.



“Free Iran” was one of several anti-Iranian Facebook pages, ostensibly operated by Iranian democratic activists. In reality, it was administered by Saudi government proxies and was part of a large influence network removed in August 2019. Source: DFRLab/Facebook

99 Kanishk Karan and Ayushman Kaul, “Facebook Removes Iran-based Assets. Again,” *DFRLab*, May 30, 2019, <https://medium.com/dfrlab/facebook-removes-iran-based-assets-again-f17358ef21f>.

100 Christopher Bing and Raphael Satter, “Trump Re-Election Campaign Targeted by Iran-Linked Hackers: Sources,” *Reuters*, October 4, 2019, <https://www.reuters.com/article/us-cybersecurity-iran-exclusive/trump-re-election-campaign-targeted-by-iran-linked-hackers-sources-idUSKBN1WJ1ZM>; Nicole Perlroth and David E. Sanger, “Iranian Hackers Target Trump Campaign as Threats to 2020 Mount,” *New York Times*, October 4, 2019, <https://www.nytimes.com/2019/10/04/technology/iranian-campaign-hackers-microsoft.html>.

101 Esteban Ponce de León, “Facebook Takes Down Iranian Assets, Some Targeting Latin American Audiences,” *DFRLab*, October 24, 2019, <https://medium.com/dfrlab/facebook-takes-down-iranian-assets-some-targeting-latin-american-audiences-58a964dc0597>.

102 Emerson T. Brooking, “How a ‘Political Astroturfing’ App Coordinates Pro-Israel Influence Operations,” *DFRLab*, August 19, 2019, <https://medium.com/dfrlab/how-a-political-astroturfing-app-coordinates-pro-israel-influence-operations-bf1104fa5c7f>; Kanishk Karan, “Royally Removed: Facebook Takes Down Pages Promoting Saudi Interests,” *DFRLab*, August 14, 2019, <https://medium.com/dfrlab/royally-removed-facebook-takes-down-pages-promoting-saudi-interests-edc0ce8b972a>; Kanishk Karan, Ayushman Kaul, and Mohamed Kassab, “Facebook Disabled Assets Linked to Egypt and UAE-Based Firms,” *DFRLab*, August 14, 2019, <https://medium.com/dfrlab/facebook-disabled-assets-linked-to-egypt-and-uae-based-firms-a232d9effc32>; Brooking, “How a ‘Political Astroturfing’ App.”



This digital landscape is further complicated by the presence of Iranian opposition groups, which have invested heavily in influence capabilities of their own.<sup>103</sup> In particular, the Mojahedin-e Khalq (MEK), an exiled Islamo-socialist militant organization, has purportedly built an “online social media factory” in its 2,500-member-strong Albanian compound.<sup>104</sup> A DFRLab analysis of popular anti-Iran Twitter hashtags—#IslamicRegimeMustGo or #IRGCTerrorists—found significant evidence of inauthentic coordination and amplification.<sup>105</sup> Such hashtag campaigns have been used to lobby US officials for direct military action against Iran.

At the same time, the United States has sought to box Iran out of as much of the global media environment as possible. In November 2018, the US Department of the Treasury fully re-imposed sanctions on seven hundred Iranian entities and individuals, including the entirety of the IRIB.<sup>106</sup> In April 2019, the United States took the unprecedented step of designating the IRGC as a Foreign Terrorist Organization, severely restricting its international activities.<sup>107</sup> In January 2020, Facebook cited this US designation as justification for removing content by Iranian users that “commended” the IRGC or deceased Major General Soleimani.<sup>108</sup>

By necessity, therefore, Iran has turned increasingly to clandestine digital influence activities as its public-facing broadcasts face more challenges in reaching an audience. The result is a new kind of guerrilla broadcasting, calibrated for the social media age.

Stories shared by “BLM News” focused disproportionately on Israel, Lebanon, Yemen, and US sanctions policy. The website was revealed to be an Iranian propaganda front and its assets removed in October 2019. Source: DFRLab/Facebook

103 “Analysis: Opposition Groups and the Online War for Iran’s Future,” *BBC Monitoring*, March 21, 2019, <https://monitoring.bbc.co.uk/product/c200p610>.

104 Borzou Daragahi, “Beyond Control: Iran and its Opponents Locked in a Lopsided Confrontation,” *Atlantic Council*, June 2019, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-control-iran-and-its-opponents-locked-in-a-lopsided-confrontation/>

105 Applying the Coefficient of Traffic Manipulation (CTM), the DFRLab found that #IslamicRegimeMustGo scored 44.56 during its peak usage in September 22, 2018. #IRGCTerrorists scored 46.77 during its peak usage on April 19, 2019. As a general rule, a score over twenty should be considered potentially inauthentic. For more information regarding the CTM, see Ben Nimmo, “Measuring Traffic Manipulation on Twitter,” Project on Computational Propaganda, University of Oxford, Working Paper 2019.1.

106 US Department of the Treasury, “US Government Fully Re-Imposes Sanctions on the Iranian Regime As Part of Unprecedented US Economic Pressure Campaign,” November 5, 2018, <https://home.treasury.gov/news/press-releases/sm541>.

107 The White House, Statement from the President on the Designation of the Islamic Revolutionary Guard Corps as a Foreign Terrorist Organization, April 8, 2019, <https://www.whitehouse.gov/briefings-statements/statement-president-designation-islamic-revolutionary-guard-corps-foreign-terrorist-organization/>.

108 Donie O’Sullivan and Artemis Moshtaghi, “Instagram Says it’s Removing Posts Supporting Soleimani to Comply with US Sanctions,” *CNN Business*, January 13, 2020, <https://edition.cnn.com/2020/01/10/tech/instagram-iran-soleimani-posts/index.html>.

## CONCLUSIONS AND RECOMMENDATIONS

Iran's digital influence operations are best understood as a form of public diplomacy under duress. Because the IRIB has been sanctioned and the IRGC classified as a terrorist group, Iranian messaging is most effective if it appears to come from a neutral third party. But, whereas Russia's ongoing disinformation campaigns are intended to obfuscate truth and discredit Western institutions, Iran's efforts exemplify the art of indirect "Persian persuasion" and deflection. Iran seeks to elevate itself as an alternate leader of the Muslim world, while presenting itself as a bulwark against the perceived forces of neocolonialism and US interventionism. It seeks to do so through a messaging apparatus that its adversaries cannot easily inhibit or destroy.

As the United States considers policies to safeguard its elections and confront Iranian influence activities, three conclusions can be drawn about the nature of Iran's modern propaganda apparatus.

- Iran's digital influence efforts involve centralized goals and disparate agents. Ayatollah Khamenei himself has emphasized the importance of digital influence operations to Iran's survival. Accordingly, the government has invested heavily in such capabilities. Yet, different elements of Iran's digital propaganda apparatus evidence the involvement of different agencies, from the mass dissemination of IRIB content (likely conducted by the IRIB itself) to the targeting of individual Western journalists (likely conducted by the IRGC). It is not clear how, or if, these agencies coordinate their operations.

- These goals are closely tied to Iran's geopolitical interests. Nearly all content spread by Iran's digital influence efforts relates directly to its worldview or specific foreign policy objectives. Consequently, it is easier to identify the operations of Iran than those of other actors like Russia, whose content

is more likely to be politically agnostic. With regard to the United States, these goals are clear. The first goal is the elimination of US military presence in the Middle East. The second goal, at least until Soleimani's January 2020 killing, has been preservation of the JCPOA and ensuring that the US returns to compliance with the agreement.

- Iran may attempt direct electoral interference in 2020 and beyond. To date, there is little evidence that Iran has sought to affect the outcome of a US election. This does not, however, preclude future such campaigns. Iran is certainly aware of Russia's successful interference in the 2016 US election and how a small investiture of resources had such an outsize impact on US political discourse. If a determination is made that Iran's foreign policy goals can be better achieved by President Trump's electoral defeat, Iranian proxies are likely to mount efforts to that end.

Additionally, five steps can be taken to better prepare the United States to meet this threat.

- The US Global Engagement Center (GEC) should invest resources in identifying and neutralizing—but not editorializing about—Iran's digital influence networks. Through its funding of the Iran Disinformation Project, an independent organization that launched vociferous attacks (without evidence) on allegedly "pro-Iranian" US journalists, the GEC inadvertently damaged the credibility of US efforts to counter Iranian influence.<sup>109</sup> A more effective approach will be to invest US resources in organizations that track and identify Iran's digital influence networks without over-editorializing their findings. Basic technological innovations, like automated search and text-matching of Iranian state propaganda products, could greatly assist in this effort. In order to maintain the credibility of their findings, the organizations that unspool these networks should be as

109 Borger, "US Cuts Funds."

objective and transparent as possible in their work. To this end, the GEC should avoid contracting longstanding Iranian opposition groups for such efforts.

- 📶 The US Department of State should address regular press briefings to the Iranian people. Official US press briefings addressed to the Iranian people have traditionally been widely disseminated and received. By using such a megaphone, the United States could push back against Iran's propaganda apparatus in a strong, cost-effective manner. The one-sided claims and attacks by Iran's digital influence apparatus work best when they go unanswered. Currently, most of them do.
- 📶 The US Agency for Global Media (USAGM) should not engage in overt pro-US influence operations. Iranians are savvy media consumers who have traditionally sought out diverse points of view—something that explains the enduring popularity of BBC Persian in the country. They are less inclined to embrace obvious pro-Western propaganda. By tasking USAGM with “counterinfluence programs” against Iran in the fiscal year 2019 appropriations bill for the Department of State, Congress endangers both the editorial independence and effectiveness of the USAGM. An ostensibly independent media broadcaster is not the appropriate entity to conduct such programs.
- 📶 The Office of the Director of National Intelligence (ODNI) should independently attribute foreign influence operations. In January 2017, the ODNI attributed a significant foreign influence operation to Russia.<sup>110</sup> In nearly three years since, dozens more disinformation campaigns have been publicly

identified and attributed—but only by corporations like Facebook, Google, and Twitter. It is inappropriate that such politically consequential work be conducted entirely by private enterprise. US intelligence services should work with social media companies to attribute future foreign influence operations. This is relevant against state actors like Iran. It is also relevant against organized non-state entities like the MEK, which habitually target the American people, but which have received comparatively little intelligence focus.

- 📶 The Department of Homeland Security (DHS) should create an appropriate intergovernmental entity to publicize foreign influence operations. Although the US intelligence services should work to defend the American people against foreign disinformation campaigns, they are not the entities that should publicize these operations on a regular basis. Instead, that job should fall to an organization modeled on the National Cyber Awareness System of the Cybersecurity and Infrastructure Security Agency (CISA) and under the purview of DHS, which can communicate regular advisories across US government and to the population at large. A similar nonpartisan organization already exists in the Critical Election Incident Public Protocol of the Canadian government.<sup>111</sup>

In 2011, former Iranian Intelligence Minister Heidar Moslehi remarked that, “We do not have a physical war with the enemy, but we are engaged in heavy information [warfare].”<sup>112</sup> At the time of Moslehi's speech, Iran had just begun to seed the digital landscape with fabricated websites and social media personas. Today, it commands tens of thousands of them, waging an information war that shows no sign of ending.

110 “Assessing Russian Activities and Intentions.”

111 Alexander Panetta and Mark Scott, “Unlike US, Canada Plans Coordinated Attack on Foreign Election Interference,” *Politico*, September 4, 2019, <https://www.politico.com/story/2019/09/04/canada-foreign-election-meddling-1698209>.

112 “Iran Adopts Aggressive Approach Toward Enemies,” *Tehran Times*, July 18, 2011, <https://www.tehrantimes.com/news/244231/Iran-adopts-aggressive-approach-toward-enemies>.

# APPENDIX

## ADDITIONAL DFRLAB RESOURCES ON IRANIAN INFLUENCE OPERATIONS

---

**Below, please find a list of previous assessments of Iranian influence operations, published by the Atlantic Council's Digital Forensic Research Lab.**

### **JANUARY 10, 2020 Alleged Hack of Kuwaiti News Agency Tweets Bodes Poorly for Crisis Coverage**

DFRLab Senior Fellow Andy Carvin recounts how, at the height of the ongoing US-Iran conflagration, the Kuwaiti News Agency issued a series of tweets claiming that the United States was withdrawing from the country, only to later delete them under the auspices of having been hacked. The piece puts this claim of hacking in the context of other instances when news media are known to have been hacked.

### **JANUARY 4, 2020 Tensions Escalate on Social Media Platforms After Soleimani's Death**

Given the magnitude of the event, traffic on Instagram and Twitter following the death of Qasem Soleimani appeared organic, but highly driven by sentiment. In the immediate aftermath of Soleimani's death, there is no indication of online influence operations with an international focus deriving from Iran that gained a significant impact. Social media platforms are often the first point of escalation in times of crisis—in this case, high-trending hashtags around the event appeared and gained traction quickly.

### **DECEMBER 16, 2019 Visual Forensics Corroborate Reports of Iran's Lethal Crackdown on Protests**

The protests in Iran in November 2019 saw the use of a favorite, and increasingly frequent, tactic of repressive governments: throttling, or entirely blocking, all or parts of the Internet as a means of limiting exposure of often-violent suppression of protests. Despite attempting to limit secure messaging platforms, in the case of the November 2019 Iranian protests, the DFRLab was able to confirm or locate many instances of the use of force by the Iranian government.

### **OCTOBER 24, 2019 Facebook Takes Down Iranian Assets, Some Targeting Latin American Audiences**

Facebook removed a number of pages and groups operated from Iran that specifically targeted Latin America, and even the

United States. As with most other Iranian Facebook operations, the assets removed were not subtle in promoting pro-Iran messaging behind a veneer of supposedly otherwise focused pages, such as one ostensibly supporting Black Lives Matter.

### **MAY 30, 2019 Facebook Removes Iran-based Assets. Again.**

In another content-moderation effort, Facebook shut down a number of pages heavy on pro-Iran messaging for inauthentic, or falsified, engagement. Unlike online influence operations from other countries such as Russia—which are designed to generate or exacerbate societal instability via profiles designed to appear local to the online community targeted—Iran's inauthentic operations are easier to spot. The messaging is often unsubtle in its pro-Iran, sectarian, anti-Israel, anti-United States, or anti-Western bias.

### **APRIL 19, 2019 Facebook Dismantled Iranian Influence Operation**

As with other countries, highly biased—and sometimes outright false—coverage from state-run news outlets, such as IRIB, is often matched with inauthentic social media amplification produced by online networks. In this case, the DFRLab had an exclusive investigation of efforts to game IRIB's online reach on Facebook, with the intent of inflating the Iranian government's narratives, prior to the network's removal from Facebook.

### **MARCH 26, 2019 Key Findings: Iranian Propaganda Network Goes Down**

As with most online influence operations deriving from Iran, the network featured in this piece promoted pro-Iran, sectarian, anti-Israel, anti-US, and anti-Saudi messaging, often reposting content from Iranian state media. This online network was notable for the geographic diversity in its targeting audiences across Africa and much of South Asia, which suggested it to be state-backed, given the resources necessary to undertake such an effort.

### **MARCH 26, 2019** In Depth: Iranian Propaganda Network Goes Down

Given the size of the network summarized above, this in-depth investigation details the open-source and digital forensic evidence of an Iranian online network targeting audiences in most of Africa and much of South Asia.

### **FEBRUARY 25, 2019** #TrollTracker: Spam Attack on Secretary Pompeo

A flood of seemingly coordinated replies to an Instagram post on US Secretary of State Mike Pompeo's official account displayed anti-US or pro-Iran sentiment. The activity showed how Instagram is emerging as a vector for coordinated campaigns, with a handful of accounts generating a significant volume of traffic on individual posts.

### **JANUARY 31, 2019** #TrollTracker: Outward Influence from Iran

Facebook removed yet another Iranian operation, easily identifiable by the content, behavior, and narratives by the assets. Notable in this case, however, was the amount of time many of the assets had been on the platform, with many assets active for more than five years. The finding is a recent, but significant, record of how long Iran has carried out social media influence operations.

### **OCTOBER 26, 2018** #TrollTracker: Facebook Uncovers Iranian Influence Operation

The operation detailed in this report indicated that Iran has the capacity to be more sophisticated in its operations, as the pro-Iran messaging from these assets was often buried in more local, and divisive, political content. For example, many of the pages involved posted content regarding the 2018 US midterm elections, mostly targeting left or left-leaning audiences that would be predisposed to agree with some narratives of the United States as an imperial power.

### **OCTOBER 17, 2018** #TrollTracker: Twitter Troll Farm Archives

In 2018, Twitter released an enormous data set of ten million tweets the platform assessed to be networks aligned or controlled by nation states as a means of covert influence. Of the overall set, nine million were Russian, some operated by the Internet Research Agency, while one million were Iranian. The DFRLab had exclusive access to the data prior to their release, and this investigation dives into the Iranian assets. The Iranian Twitter accounts pointed the platform's users toward off-platform websites, disguised as news outlets, that predominantly posted content backing the Iranian government's foreign policy positions. As with other cases, the DFRLab could only isolate the culprits to the country of Iran, and not to its government.

### **AUGUST 29, 2018** #TrollTracker: An Iranian Messaging Laundromat

Following up on a Reuters report, the DFRLab identified a cluster of websites under the banner of the International Union of Virtual Media (IUVM) posting exclusively pro-Iran content. In doing so, it effectively laundered content from Iranian state media, lending it an air of credibility by stripping the affiliation, thereby enabling it to be passed to less discerning readers as (ostensibly) credible.

### **AUGUST 27, 2018** #TrollTracker: Iran's Suspected Information Operation

Building on a high-profile report from FireEye that exposed an Iranian influence operation, the DFRLab concluded that it was the first instance of a large-scale troll operation targeting Western protest groups (predominantly in the United States and the United Kingdom) run by a nation other than Russia in the lead-up to 2018 US midterms.

# ABOUT THE AUTHORS

---



**Emerson T. Brooking** is a Resident Fellow at the Digital Forensic Research Lab of the Atlantic Council and coauthor of *LikeWar: The Weaponization of Social Media*. Most recently, he was Research Fellow at the Council on Foreign Relations—the youngest researcher in a generation to receive such an appointment. Brooking has spoken regularly on the topic of information warfare and political manipulation, advising multiple U.S. technology companies and national security entities. He has appeared widely in broadcast media, including NPR’s “Fresh Air,” and his work has been published in *Foreign Affairs*, *WIRED*, and *Rolling Stone*, among others. Brooking was recently named to the *Forbes* “30 Under 30.” He holds a BA in Political Science and Classical Studies from the University of Pennsylvania.



**Suzanne Kianpour** is a non-resident senior fellow at the Atlantic Council and a foreign affairs and political journalist. With postings in Washington, Beirut, London, and LA working for the BBC, Kianpour’s reporting has taken her around the world: from conflict zones in the Middle East, to covering Secretary of State John Kerry’s role in the Iran nuclear negotiations in Europe, to Latin America and the US detente with Cuba. Over the course of her career, Kianpour has landed interviews with high-profile individuals, including Iranian Foreign Minister Javad Zarif and Hamas leader Khaled Meshaal. Kianpour is a public diplomacy lecturer at UCLA and a 2018 fellow at Georgetown’s Institute of Politics and Public Service focusing on the media’s role in public service. Her work at the Atlantic Council focuses on Iran in a joint fellowship with the Middle East Programs and the Digital Forensic Research Lab.

## ATLANTIC COUNCIL BOARD OF DIRECTORS

### CHAIRMAN

\*John F.W. Rogers

### EXECUTIVE CHAIRMAN EMERITUS

\*James L. Jones

### CHAIRMAN EMERITUS

Brent Scowcroft

### PRESIDENT AND CEO

\*Frederick Kempe

### EXECUTIVE VICE CHAIRS

\*Adrienne Arsht

\*Stephen J. Hadley

### VICE CHAIRS

\*Robert J. Abernethy

\*Richard W. Edelman

\*C. Boyden Gray

\*Alexander V. Mirtchev

\*John J. Studzinski

### TREASURER

\*George Lund

### SECRETARY

\*Walter B. Slocombe

### DIRECTORS

Stéphane Abrial

Odeh Aburdene

Todd Achilles

\*Peter Ackerman

Timothy D. Adams

\*Michael Andersson

David D. Aufhauser

Colleen Bell

Matthew C. Bernstein

\*Rafic A. Bizri

Dennis C. Blair

Philip M. Breedlove

Myron Brilliant

\*Esther Brimmer

R. Nicholas Burns

\*Richard R. Burt

Michael Calvey

James E. Cartwright

John E. Chapoton

Ahmed Charai

Melanie Chen

Michael Chertoff

\*George Chopivsky

Wesley K. Clark

\*Helima Croft

Ralph D. Crosby, Jr.

\*Ankit N. Desai

Dario Deste

\*Paula J. Dobriansky

Thomas J. Egan, Jr.

Stuart E. Eizenstat

Thomas R. Eldridge

\*Alan H. Fleischmann

Jendayi E. Frazer

Ronald M. Freeman

Courtney Geduldig

Robert S. Gelbard

Gianni Di Giovanni

Thomas H. Glocer

John B. Goodman

\*Sherri W. Goodman

Murathan Günal

\*Amir A. Handjani

Katie Harbath

John D. Harris, II

Frank Haun

Michael V. Hayden

Amos Hochstein

\*Karl V. Hopkins

Robert D. Hormats

Andrew Hove

\*Mary L. Howell

Ian Ihnatowycz

Wolfgang F. Ischinger

Deborah Lee James

Joia M. Johnson

Stephen R. Kappes

\*Maria Pica Karp

Andre Kelleners

Astri Kimball Van Dyke

Henry A. Kissinger

\*C. Jeffrey Knittel

Franklin D. Kramer

Laura Lane

Jan M. Lodal

Douglas Lute

Jane Holl Lute

William J. Lynn

Mian M. Mansha

Chris Marlin

William Marron

Neil Masterson

Gerardo Mato

Timothy McBride

Erin McGrain

John M. McHugh

H.R. McMaster

Eric D.K. Melby

\*Judith A. Miller

Dariusz Mioduski

Susan Molinari

\*Michael J. Morell

\*Richard Morningstar

Virginia A. Mulberger

Mary Claire Murphy

Edward J. Newberry

Thomas R. Nides

Franco Nuschese

Joseph S. Nye

Hilda Ochoa-Brillembourg

Ahmet M. Oren

Sally A. Painter

\*Ana I. Palacio

\*Kostas Pantazopoulos

Carlos Pascual

W. DeVier Pierson

Alan Pellegrini

David H. Petraeus

Lisa Pollina

Daniel B. Poneman

\*Dina H. Powell McCormick

Robert Rangel

Thomas J. Ridge

Michael J. Rogers

Charles O. Rossotti

Harry Sachinis

C. Michael Scaparrotti

Rajiv Shah

Stephen Shapiro

Wendy Sherman

Kris Singh

Christopher Smith

James G. Stavridis

Richard J.A. Steele

Mary Streett

Frances M. Townsend

Clyde C. Tuggle

Melanne Verveer

Charles F. Wald

Michael F. Walsh

Ronald Weiser

Geir Westgaard

Olin Wethington

Maciej Witucki

Neal S. Wolin

\*Jenny Wood

Guang Yang

Mary C. Yates

Dov S. Zakheim

### HONORARY DIRECTORS

James A. Baker, III

Ashton B. Carter

Robert M. Gates

Michael G. Mullen

Leon E. Panetta

William J. Perry

Colin L. Powell

Condoleezza Rice

George P. Shultz

Horst Teltschik

John W. Warner

William H. Webster

*\*Executive Committee  
Members*

List as of January 15 2020



The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

© 2020 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council

1030 15th Street, NW, 12th Floor,  
Washington, DC 20005

(202) 463-7226, [www.AtlanticCouncil.org](http://www.AtlanticCouncil.org)