OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
3 MARCH 2021 IA-45978-21

*FOREIGN INFLUENCE*

# *(U)* Iranian Influence Efforts Primarily use Online Tools to Target US Audiences, Remain Easily Detectable for Now

*(U//FOUO)* **Scope:** This *Intelligence In Focus* (*IIF*) is a companion piece to the I&A *IIF*, "Iranian Efforts to Manipulate US Media Narratives," released on 24 February 2021, providing baseline assessments of Iran's attempts to conduct malign influence operations against US audiences.

*(U//FOUO)* ***We assess that Iran likely will continue to rely primarily on proxy news websites and affiliated social media accounts to attempt sustained influence against US audiences, while we expect intermittent, issue-specific influence attempts via other means (e.g., e-mails).*** We base this assessment on Iran's actions since at least 2008 to build and maintain vast malign influence networks anchored by proxy websites, as well as Iran's attempts to find new avenues to re-launch established malign influence networks after suspension. Tehran employs a network of proxy social media accounts and news websites that typically launder Iranian state media stories (stripped of attribution), plagiarize articles from Western wire services, and occasionally pay US persons to write articles to appear more legitimate to US audiences.

- *(U)* The American Herald Tribune (AHT)—an Iranian Government proxy website established in 2015 that purported to be a genuine media outlet—was seized by the US Government on 4 November 2020 for attempting to covertly influence United States policy and public opinion, according to a DOJ press release. However, AHT by at least 16 November 2020 resurfaced on a Canada-based domain, according to AHT's website. AHT is also known to pay unwitting US persons to contribute to its disinformation campaigns, according to the same website.
- *(U)* The International Union of Virtual Media (IUVM) since at least August 2018 has maintained a network of proxy accounts and websites posing as news sources that attempted to insert Iranian Government narratives into Western target audiences and to denigrate the United States, Western governments, and other regional adversaries, according to reports from a research institute and a social media analysis firm. Since IUVM started, US social media outlets have repeatedly removed its accounts from their platforms for being engaged in pro-Iran information operations and deceiving users; most recently, the FBI in October 2020 seized IUVM's domains, according to the same reports and a DOJ press release. Despite these setbacks, however, IUVM created new accounts and returned to operations, according to these same reports.

*(U)* Prepared by the Cyber Mission Center. Coordinated with the DHS Intelligence Enterprise (CETC, CIMC, FOD, and ICE).
For questions, contact DHS-SPS-RFI@hq.dhs.gov.

- *(U)* Iranian state media-linked Liberty Front Press, created in 2013, claimed to be an independent media organization that published US political news, including content from other proxies such as IUVM and US-based media sites, according to reports from a media outlet, a cybersecurity firm, and a research institute. Liberty Front Press and its network of affiliated proxy news websites published content directly from other sources, and any original content contained poorly written English, according to the same cybersecurity firm report. In August 2018, US social media platforms deactivated accounts associated with Liberty Front Press because of its connection to Iranian state media, according to media reporting. The Liberty Front Press website was officially seized by the FBI in October 2020, according to a DOJ affidavit. The FBI identified over 1,000 domains, e-mail accounts, and social media accounts associated with Liberty Front Press as part of its investigation, according to the same affidavit.

*(U//FOUO)* ***For at least the next year, we assess that these Iranian-run news websites and affiliated social media accounts targeting US audiences likely will remain easily detectable by the US Government and US social media companies due to Iran's use of thinly masked and often unsubtle promotion of pro-Iranian content.*** We base this assessment on Iran's promotion of pro-Iranian messaging behind a veneer of supposedly otherwise focused pages and the ease at which these pages have previously been identified and removed from US social media platforms and registered domains. While Iranian websites have remained easily detectable to date, if these deceptive outlets improved their obfuscation techniques and replaced obvious pro-Iranian content with divisive anti-US content, these outlets could blend into the information environment and be more difficult to attribute. Thus, it is important for the US Government and social media companies to maintain a close working relationship to continue to detect and uncover Iranian covert influence efforts as they develop and grow in complexity.

- *(U)* In August 2018, a cybersecurity firm made the first major attribution of Iranian proxy accounts attempting to promote political narratives in line with Iranian interests, which directly led to the suspension and removal of over 900 accounts, pages, and groups from US social media platforms, some accounts dating back as early as 2015, according to reports from a cybersecurity firm and social media companies.

- *(U)* In October 2019, a social media company removed several Iran-based pages attempting to hide behind a façade of otherwise focused pages, while pushing pro-Iranian messaging, including a page supposedly supporting Black Lives Matter[USPER], according to a research institute.

- *(U)* In October 2020, a US social media company removed an Iran-based page attempting to conceal its identity and activity, while pushing false claims and unsubstantiated US election-related threats as part of an influence operation, according to a report from the same social media company.

- *(U)* In October 2020, a social media company acted on information provided by the FBI to take down over a hundred accounts appearing to originate from Iran and attempting unsuccessfully to disrupt the public conversation of the first 2020 US presidential debate, according to a report from the same social media company.

## Source, Reference, and Dissemination Information

| | |
|---|---|
| **Source Summary Statement** | *(U//FOUO)* This product is based on reports from two research institutes, a cybersecurity firm, a social media analysis firm, US social media companies, and press releases from US Government agencies.<br><br>*(U//FOUO)* We assess that Iran likely will continue to primarily rely on proxy news websites and affiliated social media accounts to attempt sustained influence against US audiences, while we expect intermittent, issue-specific influence attempts via other means (e.g., e-mails). We have **moderate confidence** in our assessment based on reports from sources with a history of credible reporting and corroboration of reporting among a wide range of sources including the US Government and the social media platforms themselves. Our confidence would increase if we saw continued evidence of US detection and disruption of Iranian information operations, and we would re-evaluate this assessment if we discovered Iranian online influence that had previously been undetected for a prolonged period.<br><br>*(U//FOUO)* For at least the next year, we assess that these Iranian-run news websites and affiliated social media accounts targeting US audiences likely will remain easily detectable by the US Government and US social media companies due to Iran's use of thinly masked and often unsubtle promotion of pro-Iranian content. We have **moderate confidence** in our assessment based on reports from sources with a history of credible reporting and the corroboration of reporting among a wide range of sources. Our confidence would increase if we saw further evidence of attempts of Iranian obfuscation across multiple platforms and resonating in the US information environment. |
| **Definitions** | *(U//FOUO)* **Disinformation:** A foreign government's deliberate use of false or misleading information intentionally directed at another government's decisionmakers and decision-making processes to mislead the target, force it to waste resources, or influence a decision in favor of a foreign government's interests. Disinformation always depends on falsehoods and is sometimes relayed clandestinely for the target to "discover."<br><br>*(U//FOUO)* **Influence Activities:** The use of covert and overt tools to achieve a foreign government's objectives, sometimes in support of broader influence operations. Activities may be carried out by an array of actors, independently or in coordination.<br><br>*(U//FOUO)* **Influence Operations:** Broad use of influence activities conducted by various state and nonstate actors, sometimes to achieve specific goals under a larger influence campaign objective. |
| **Dissemination** | *(U)* Senior DHS leadership, federal officials, governors, lieutenant governors, secretaries of state, homeland security advisors, fusion center directors and their staff. |
| **Civil Rights and Civil Liberties** | *(U//FOUO)* US persons linking, citing, quoting, or voicing the same arguments raised by these influence activities likely are engaging in First Amendment-protected activity, unless they are acting at the discretion or control of a foreign threat actor. Furthermore, variants of the topics covered in this product, even those that include divisive terms, should not be assumed to reflect foreign influence or malign activity absent information specifically attributing the content to malign foreign actors. This information should be considered in the context of all applicable legal and policy authorities to use open source information while protecting privacy, civil rights, and civil liberties. |

| | |
|---|---|
| **CISA Guidelines for Countering Foreign Influence** | *(U)* CISA defines foreign influence as malign actions taken by foreign governments to spread disinformation designed to manipulate the public, sow discord and ill will, discredit the electoral process, disrupt markets, and undermine the interests of the American people. Recognize the risk: understand how foreign actors try to affect behavior. Question the source: check who produced the content and question their intent. Investigate the issue: search for other reliable sources before sharing. Think before you link: ask yourself why you're sharing, and let your emotions cool. Talk to your circle: talk to your social circle about the risks of spreading disinformation. |
| **Warning Notices & Handling Caveats** | *(U)* **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.<br><br>*(U)* This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label USPER and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other US person information has been minimized. Should you require the minimized US person information on weekends or after normal weekday hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@hq.dhs.gov. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov. |