U.S. Seizes Iranian-Government Controlled Websites

by Kenneth R. Timmerman

In an unprecedented and historic move, the Department of Justice and the FBI on Wednesday seized control of 92 domain names they said were "unlawfully used by Iran's Islamic Revolutionary Guard Corps (IRGC) to engage in a global disinformation campaign."

The scope of the Iranian disinformation campaign was global, and included four sites targeting American audiences and masquerading as authentic news sites.

Other seized sites operated in Europe and through the Middle East and South Asia. The DoJ posted a full listing of the

websites here.

The FBI's San Francisco field office coordinated with Big Tech companies Google, Facebook, and Twitter to identify the Iranian disinformation operation. A DoJ press release said that all 92 of the domains were "owned and operated by United States companies."

The four U.S. domain names, "newsstand7.com," "usjournal.net," "usjournal.us," and "twtoday.net," were masquerading as legitimate news sites and were "attempting to influence U.S. public opinion, policy, and law," the DoJ said.

Newsstand7.com was registered by an undisclosed person operating under an anonymous domain registration service in Panama, according to its entry in the WhoIs international data base of domain registration.

USjournal.net listed a "Nanci Nette" of 1619 N. LaBrea Ave. in Los Angeles as its administrative contact, while USjournal.us listed "Amanda Kor" of Palo Alto, CA, as its contact person.

The fourth U.S. fakenews site, twtoday.net, listed an individual in Beirut, Lebanon, Abdur Raheem el Abdallah, as its contact. Mr. Abdallah gave his address as "Near Bacha Restaurant, Jisr El Bacha," Beirut.

TWT is an abbreviation historically used by The Washington Times as email server and some of its webservices, Iranian cyber agents may have chosen that name to mislead and attract Internet users looking for conservative content. The gmail address it listed with the WhoIs data base, twtoday2019@gmail.com, appeared to coincide with the Nov. 3, 2019 date the website was registered.

Newsstand7.com was registered on March 11, 2019, and USjournal.us was created on Dec. 7, 2019. The oldest of the four websites targeting American audiences, USjournal.net, was registered two years earlier, on Aug. 7, 2017.

During the first archived day of its sudden appearance on the World Wide Web, August 13, 2017, USjournal.net ran the following headlines:

> "White Helmets" Latent Militants in Syria Are Killed by Russian Forces
>
> The Mooch To Appear On 'The Late Show With Stephen Colbert' Next Monday
>
> Medieval Genocide: Saudi Arabia Massacres Yemenis by Cholera
>
> Only Stupid People Say Torture Works, and One of Them's in the White House
>
> Trump's strategy against North Korea has more holes than a sieve

The story on the Syrian "white helmets" sounded a familiar theme dear to the Syrian government, namely that the "white helmets" operating as civil defense and EMTs in ISIS-held territory in Syria were "notorious not only for its [ssic] apparent ties to the western intelligence services, but also for providing plans and maintaining ties with the terrorist groups."

Three of the stories aimed at mocking and disparaging President Trump, while the story about Saudi Arabia spreading "cholera" in Yemen supported Iran's goal of defeating the Saudi-backed regime in Yemen and glorifying the Iranian-government backed Houthi rebels. All of the content was generated using WordPress.

TWtoday had all the appearances of a classic Internet news site, with scrolling headlines, news sections, and even a sports section.

A glimpse at archived content from April 2020 shows a far more nuanced and sophisticated influence operation.

One headline praising China for its handling of the coravirus, reads: “China lockdown may have saved 700,000 lives.” Another berates a “Zionist newspaper” in Israel for claiming that the targeted killing of Quds Force commander Qassem Suleymani struck a blow at Iran’s military operations in Syria.

A “soft news” story, “Muslim sailors regularly travelled to Australia centuries before Captain Cook,” evokes pre-Western trade between Muslims in Indonesia and aborigine populations in Australia as a means sending “a powerful message about belonging for young Australian Muslims.”

The sheer scope of the Iranian cyber influence operations should make American decision-makers pause. This was not a one-off hack, nor a script-kiddie attack on some Iranian opposition website – something which happened to the Foundation for Democracy in Iran’s flagship iran.org website ten years ago.

The Iranian regime has emerged as a full-service player in cyberspace, capable of offensive operations such as seizing control of U.S. drones, which it first demonstrated by downing a Lockheed Martin RQ-170 Sentinel drone flying along the Afghan-Iranian border in 2011, as well as cyber influence operations.

From there to hacking U.S. election infrastructure – perhaps even altering votes recorded on computer-driven tabulators, as I project in my latest book, The Election Heist – is just a small step away.

NY Times best-selling author Kenneth R. Timmerman is the author of *Deception: The Making of the YouTube Video Hillary and Obama blamed for Benghazi*, and 10 other works of non-fiction. *The Election Heist*, a fictional account of the 2020 election, is his fourth published novel.