EINPRESSWIRE

(Video) New Report Reinforces Need for Constant Vigilance Against Iran’s Online Disinformation

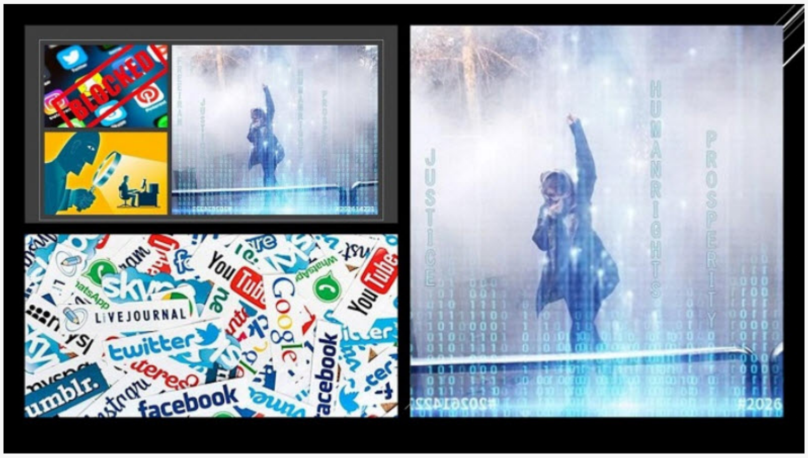
FireEye reported that some Iranian accounts have impersonated US politicians in order to promote policies and talking points that were favorable to the regime.

(PMOI / MEK Iran) & (NCRI) Ministry of Intelligence and Security (MOIS) has long used social media for its own interests, this phenomenon has been outpaced by using fake social media to spread disinformation about the main opposition (MEK) advocating for regime change.

PARIS, FRANCE, December 18, 2021 /EINPresswire.com/ -- The National Council of Resistance of Iran (NCRI) and the People’s Mojahedin Organization of Iran (PMOI / MEK Iran), reported that. Over the past few years, there have been various reports that Iran’s Ministry of Intelligence and Security (MOIS) have long used social media to spread talking points that were favorable to its own interests, but in recent years, this phenomenon has been outpaced by the use of bots and fake social media personas to spread disinformation about domestic opposition activists, often by impersonating the most prominent groups advocating for regime change.

The growth of that practice has led to thousands of accounts being taken down by Facebook, Twitter, and Instagram – a trend that was first publicly identified in 2014 and continues to this day.
Recurring reports of such takedowns underscore the fact that constant vigilance is needed in order to combat disinformation on social media, especially at a time when Iranian state-affiliated hackers are reported to have repeatedly expanded their skillsets and stepped up their coordination.

In fact, that coordination and advancement have no doubt helped fake accounts and deceptive pages to generally proliferate more quickly than they could be removed. In August 2018, Facebook reported that it had removed 652 pages, groups, and accounts involved in the spread of propaganda and disinformation on behalf of the Iranian regime. Hundreds more were removed the following January, and another 513 were taken down in March 2019. Soon thereafter, Twitter proved to be a source of potentially greater concern, as 2,800 Iran-backed accounts were removed for deceptive activity in May, and 4,779 were removed just the following month.



(PMOI / MEK Iran) and (NCRI) Recurring reports of such takedowns underscore the fact that constant vigilance is needed in order to combat disinformation on social media, especially at a time when Iranian state-affiliated hackers are reported to have repeatedly expanded.

Around the time that these successive takedowns were being announced, cybersecurity firms were also sharing reports with the global media about coordinated inauthentic activity in general, and Iran's growing contributions to that field in particular. Some such reports explicitly stated that Facebook and Twitter would likely struggle to identify suspicious accounts and posts quickly enough to halt their expansion, and others highlighted a range of tactics the regime appeared to be using that went beyond the simple spread of disinformation.

One firm called FireEye reported in June 2019 that some Iranian accounts had impersonated US politicians in order to promote policies and talking points that were favorable to the regime. Such impersonation tactics had previously been established as a means by which Tehran defamed opposition activists, especially those affiliated with the country's leading pro-democracy group, the People's Mojahedin Organization of Iran (PMOI-MEK), and its parent coalition, the National Council of Resistance of Iran.

> Such impersonation tactics had previously been established in which Tehran defamed those affiliated with leading Iran (PMOI-MEK), and its parent coalition, the National Council of Resistance of Iran."
>
> *NCRI*

An open letter published by a former agent of the Iranian regime earlier in the year helped to reveal the sheer scale of another aspect of the regime's disinformation campaign.
The letter in question was written by Hadi Sani-Kani, who after having left the MEKwas promptly approached by Iranian intelligence operatives and incentivized to participate in a far-reaching campaign of disinformation targeting that organization specifically.

Sani-Kani detailed the structure of MOIS operations, the payment that operatives received for writing articles and giving media interviews based on talking points furnished by their handlers, and the ways in which his own network collaborated with -"friendly reporters" and academics to create a sort of feedback loop among regime-produced content and third-party publications and broadcasts.

Naturally, social media played a role in that loop, and Sani-Kani's letter indicated that every person who was recruited for propaganda operations was required to maintain at least one account each on Facebook and Instagram, through which they shared their own articles as well as truncated versions of the same talking points. Each of the network's operatives was expected to produce a minimum of 12 articles per month featuring claims that were unfavorable to the opposition movement, or conclusions that discouraged policies that might have supported it.

Cybersecurity analyses have elaborated upon Sani-Kani's account by identifying numerous false websites that the Iranian regime attempted to use in order to give its internal talking points an air of legitimacy. In June 2021, the threat posed by such sites was underlined when the US government seized around three dozen internet domains on account of their role in the spread of "Iranian disinformation." Of course, most of the sites in question simply migrated to different servers, but their removal from US domains may have made it less likely for them to be taken seriously as legitimate news outlets and used as sources by third-party reporters.

twitter
Google
Fundamentalist Shi'ite Ideas Seem to Gain Ground
Iran's Push in the Virtual Space
The propaganda and fake accounts on various social media, targeting the MEK

(PMOI / MEK Iran) and (NCRI): Disinformation by mullahs. Hundreds more were removed the following January, and another 513 were taken down in March 2019. Soon Twitter proved to be a source of deceptive activity in May, and 4,779 were removed just the following month.

(PMOI / MEK Iran) and (NCRI): Some reports explicitly stated that Facebook and Twitter would likely struggle to identify suspicious accounts and posts quickly to halt their expansion, and others highlighted a range of tactics the regime tried to spread disinformation.

According to Maryam Rajavi president-elect of NCRI, Tehran's practice of impersonation has only grown bolder, as evidenced by the creation of a Twitter account in January 2021 which assumed the identity of the NCRI's US representative Soona Samsami and posted a statement urging

Iranians to gather at the White House or the Capitol. The account in question was promptly taken down by Twitter after being flagged by the NCRI itself, but if recent history is any indication it will prove to be only one of the hundreds if not thousands of false accounts that Tehran attempted to utilize over the past year.

The prior message shared by cybersecurity firms, Hadi Sani-Kani, and the NCRI, therefore, remains as relevant as ever: constant vigilance is required in order to prevent Iran's online disinformation from doing more harm than it already has.

Shahin Gobadi
NCRI
+33 6 51 65 32 31
email us here

(PMOI / MEK Iran) and (NCRI): Such impersonation tactics had previously been established as a means by which Tehran defamed opposition activists, especially those affiliated with the leading pro-democracy group, the People's Mojahedin Organization of Iran and (NCRI).

(PMOI / MEK Iran) & (NCRI) MOIS operations, the payment that operatives received for writing articles and giving media interviews based on talking points furnished by their handlers, and the ways in which his own network collaborated with friendly reporters as feedback.

(PMOI / MEK Iran) and (NCRI): Tehran’s practice of impersonation, evidenced by the creation of a Twitter account in January 2021 which assumed the identity of the NCRI’s US representative Soona Samsami and posted a statement urging Iranians to gather at the White House.

(PMOI / MEK Iran) and (NCRI): Recent history proves this is only one of the hundreds of false accounts that Tehran using over the past years against MEK. So it remains as constant vigilance which is required in order to prevent mullahs' disinformation campaigns.

This press release can be viewed online at: https://www.einpresswire.com/article/558652543

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.