AMERICAN FOREIGN POLICY COUNCIL

Information Warfare Watch No. 10

December 31, 2021 **Ilan I. Berman**

Related Categories: Human Rights and Humanitarian Issues; International Economics and Trade; Public Diplomacy and Information Operations; China ; Iran; Russia

FACEBOOK FACES CHINESE DISINFO
Meta, the parent company of Facebook and Instagram, has said that it has taken down more than "600 accounts, pages, and groups connected to a Chinese influence operation spreading COVID-19 disinformation, including an account purporting to be a fictitious Swiss biologist." The China-based operation was uncovered after the company was alerted to an account belonging to a fictitious Swiss biologist named Wilson Edwards that was posting claims that the U.S. was pressuring the World Health Organization to blame China for the COVID-19 pandemic. The posts appeared in Chinese media stories as evidence of U.S. intimidation. According to Meta's Ben Nimmo, the Chinese operation was an example of "coordinated inauthentic behavior" where adversaries use "fake accounts" for influence operations, similar to the way Russian operatives impersonated Americans on Facebook in the run-up to the 2016 U.S. presidential election. (Georgia Public Broadcasting, December 1, 2021)

THE KREMLIN EXPANDS ITS GRIP ON (SOCIAL) MEDIA...
The Russian government's ability to shape the country's social media sphere just got a good deal bigger. In early December, state natural gas giant GAZPROM, via a subsidiary, secured a controlling interest in VKontakte (VK), the popular social media platform that serves as the Russian version of Facebook. The arrangement is the culmination of a series of business deals that saw VK's CEO, billionaire financier Alisher Usmanov, relinquish control of the platform, which is estimated to have some 100 million users. As a result, GAZPROM - which is closely tied to the Kremlin and counts confidantes and allies of Russian President Vladimir Putin among its key shareholders - has acquired more than 50% of the voting rights in VK. (The Moscow Times, December 3, 2021)

...AS THE DOMESTIC NOOSE TIGHTENS
In recent months, the Russian government has used the controversial "foreign agent" designation as a way to squelch the vibrancy of the country's independent media - adding scores of journalists and opposition media outlets to a public blacklist that is intended to make it more difficult for those actors to operate and to diminish their credibility inside the country. In late December, this list was expanded even further with the addition of two journalists from Radio Free Europe/Radio Liberty, alongside opposition political figures like Pussy Riot protest group members Nadezhda Tolokonnikova and Veronika Nikulshina. Also added to the list were Andrei Alexeev, a filmmaker from Yaroslavl; Marat Gelman, a former deputy director of Russia's official Channel One broadcaster; and journalists Taisiya Bekbulatova and Viktor Shenderovich, editor in chief of Kholod magazine and a columnist for the New Times newspaper, respectively. The official blacklist now numbers some 111 individuals. (Radio Free Europe/Radio Liberty, December 30, 2021)

A NEW TOOL FOR DIGITAL RESILIENCE IN IRAN
In its struggle against the Islamic Republic, Iran's domestic opposition has a new tool at its disposal. A new Android app called Nahoft ("hidden" in Farsi) is creating the opportunity for Iran's assorted opposition activists to communicate securely, and to coordinate their protests, despite ubiquitous regime surveillance and growing official control over the Internet inside Iran. The software "is an encryption tool that turns up to 1,000 characters of Farsi text into a jumble of random words," explains Wired magazine. "You can send this mélange to a friend over any communication platform — Telegram, WhatsApp, Google Chat, etc. — and then they run it through Nahoft on their device to decipher what you've said."

Nahoft, which was released in September by United for Iran, a human rights and civil liberties group based in San Francisco, also possesses a pair of capabilities designed to sustain opposition forces in their fight with the Iranian regime. The first is its use of steganography, the practice of embedding messages within images, which can be decrypted by recipients using their own version of the app. The second is the app's offline functionality, which allows users to employ Nahoft on their mobile devices even during conditions when the Internet is blacked out by regime authorities, as it was back in November of 2019. (Wired, September 19, 2021)