



Information Warfare Watch No.23

July 10, 2023 Ilan I. Berman, Dinah Gorayeb

Related Categories: Cybersecurity and Cyberwarfare; Islamic Extremism; Science and Technology; Terrorism; Warfare; China; Middle East; Russia; Ukraine

HOW TIKTOK ANIMATES PALESTINIAN EXTREMISM

In the Palestinian Authority, social media is playing a significant role in fueling militancy among Palestinian youth. Specifically, researchers are noting that local extremists in the West Bank and Gaza Strip are increasingly using China's popular TikTok app to spread their radical message and facilitate recruitment among the local populace. In particular, Lion's Den, a local militant outfit from Nablus that rose to prominence in the West Bank over the past year, has been creating short TikTok videos intended to expose youth to violence – and woo them to the group's cause. More established organizations, such as Hamas and the Palestinian Islamic Jihad, are also known to harness social media via longer videos for both recruitment and incitement to violence against Israelis. However, observers are finding that "local factions" are more adept at producing the short TikTok videos that are most appealing and engaging to Palestinian youth. (JNS.org, June 21, 2023)

RUSSIAN DISINFO TARGETS FOREIGN SUPPORT FOR UKRAINE...

Over the past year-and-a-half, Russia's war of aggression against Ukraine has focused world attention on the dangers of the Kremlin's imperialist, adventurist foreign policy. In turn, it has activated new tropes and narratives on the part of the Russian government, as Moscow seeks to rally global opinion to its side. To this end, French authorities uncovered what they say is a global disinformation operation by "Russian actors" and "state entities" that utilized French, Israeli, Jewish, and German news sources to defame and lessen support for Ukraine. The long-running effort apparently began nearly two years ago, and entailed the forgery of websites for an array of real publications, from France's *Le Monde* to Germany's *Der Spiegel* to the English-language *Jewish Journal*. Each falsified website, in turn, carried numerous stories rooted in the same narrative: that the target country's support for Kyiv was harming its economic and strategic interests. "Their goal," reports Israel's *Ha'aretz* newspaper, "was to undermine popular and political support in France, Germany and Israel for aiding Ukraine against Russian aggression." (*Ha'aretz*, June 13, 2023)

...EVEN AS PRIGOZHIN UPENDS RUSSIA'S PROPAGANDA ECOSYSTEM

In the wake of Wagner chief Yevgeny Prigozhin's short-lived mutiny against the Kremlin in late June, the complexion of Russia's disinformation enterprise appears to be changing. Specifically, news outlets controlled by Prigozhin and used in the past to amplify the false narratives promulgated by the notorious Internet Research Agency (IRA) are now being shut down by the Russian government. Outlets like RIA FAN, which are controlled by Prigozhin's Patriot Media holding group, have announced plans to close down and leave "the country's information space." The IRA, meanwhile, is reportedly being disbanded, while the country's official state censor, ROSKOMNADZOR, is said to have "blocked media outlets linked to Prigozhin" in the aftermath of the oligarch's abortive coup. (Reuters, July 2, 2023)

CONGRESS AND THE INFORMATION WAR

As the disinformation campaigns of adversary nations like Russia and China continue to intensify, the U.S. Congress is sharpening its focus on the information domain. "Countries including Russia and China deploy immense resources to wage global information campaigns attempting to shape the narratives of their actions to their advantage, most often by twisting the truth or deflecting attention to distract the public from their true goals," Sen. Ben Cardin (D-MD) noted at a recent hearing of the Senate Foreign Relations Committee. In response, experts have counseled lawmakers that the U.S. government should make added investments in its own public diplomacy and informational capabilities, as well as in the early detection and disarming of disinformation campaigns and the social media accounts that promote them. Notably, however, these ideas remain notional; Congress has not, as yet, developed an updated strategy to respond to modern informational threats. (*The Hill*, May 11, 2023)

DISINFORMATION AIDS CHINA'S "COMPREHENSIVE NATIONAL SECURITY"

Over the past half-decade, the People's Republic of China has made massive strides in the "proficiency" and reach of its use of disinformation, according to a new assessment by the Soufan Center, a respected security think tank. "The People's Republic of China (PRC) has historically utilized censorship, propaganda, and disinformation targeting its own population, and has also utilized similar tactics to target audiences outside of the country's borders," the study notes. "The PRC's tactics, capabilities, and goals have evolved in recent years, particularly since 2019; it is now one of the more proficient state actors utilizing malign information manipulation targeting online users, especially on social media."

"Like many state and non-state actors, Beijing has determined it can make progress on a number of its foreign policy objectives by operating in and through the gray zone, relying on non-kinetic activities like disinformation and cyber-attacks that provide a significant return on investment," it notes. And "[e]merging technologies like facial recognition and artificial intelligence (AI) have allowed the CCP to exert more control over its citizens, both online and offline. Facial recognition, for instance, has been used to surveil the Uighur population in Xinjiang, where the minority Muslim population has been subjected to detention, 're-education programs' and widespread reports of intimidation, torture, and repression of religious belief and expression corroborated by investigations by Western journalists and diplomats."

This enterprise, the Soufan study lays out, has become integral to the concept of "comprehensive national security" that has emerged as a major focus of the Chinese Communist Party under the leadership of Xi Jinping. "Controlling the information environment and wielding information both inside and outside of China" has become "a key component" of ensuring regime security and stability, it posits. (Soufan Center *IntelBrief*, June 6, 2023)