AMERICAN FOREIGN POLICY COUNCIL

Information Warfare Watch No. 30

February 28, 2024 **Ilan I. Berman**, **Shivani Sharma**

Related Categories: Cybersecurity and Cyberwarfare; Intelligence and Counterintelligence; Public Diplomacy and Information Operations; Science and Technology; Warfare; China; Russia; Ukraine; United States

RUSSIA'S OTHER OFFENSIVE AGAINST UKRAINE
Over the past two years, Russia has waged a full-scale war against Ukraine in an effort to subjugate its western neighbor. While international attention has rightly focused on the military dimension of the Kremlin's "special military operation" against Kyiv, Russia's government has also waged an informational battle to weaken internal cohesion in Ukraine and deepen divisions among the country's top officials and leaders, exploiting openings among a Ukrainian government increasingly on the back foot in the conflict.

Thus, when news broke in January that Ukrainian President Volodymyr Zelensky was planning to fire his top military commander, General Valery Zaluzhny, the Kremlin's vast army of trolls sprang into action, churning out thousands of fake pieces of content on social media platforms and hundreds of articles in news outlets to spread fake rumors about Zaluzhny's sacking. Overall, the *Washington Post* reports, the propaganda campaign was aimed at "dividing and destabilizing Ukrainian society - efforts that Moscow dubbed 'information psychological operations.'" According to the *Post*, the four main goals of Russia's propaganda efforts are "discrediting Kyiv's military and political leadership, splitting the Ukrainian elite, demoralizing Ukrainian troops and disorienting the Ukrainian population." These efforts are said to be led by the Kremlin's first deputy chief of staff, Sergei Kiriyenko.

The Kremlin's disinformation initiative, however, runs much deeper. Russia's government, for instance, has taken advantage of the growing Ukrainian distrust in the country's state-run 24/7 news channel and resulting increased reliance on Telegram to saturate the social media platform with eye-catching headlines, scripted comments under posts, exaggerated statistics, deep fake videos, and more. And in Western Europe, Russia is "cloning and usurping media and government websites, such as those for *Le Monde* and the French Foreign Ministry, and then posting fake content on them denigrating the Ukrainian government," the paper reports. In this way, the government of Russian President Vladimir Putin is attempting to simultaneously weaken European support for Ukraine as well. (*Washington Post*, February 16, 2024)

TECH GIANTS MOBILIZE TO FIGHT AI DISINFO
With elections in the U.S. and other parts of the world looming, tech companies are scrambling to address the growing danger of political deepfakes and other disinformation content generated by artificial intelligence (AI). To that end, earlier this month, 20 prominent technology firms inked an agreement formally pledging to "counteract AI-generated content that is designed to deceive voters." Signatories to the pact, which is known as the "Tech Accord to Combat Deceptive Use of AI in 2024 Elections," include TikTok, X, Snap, LinkedIn, Adobe, Google, Amazon, Meta, and Microsoft. The Accord stipulates that these companies become more transparent about flagging AI-generated content on their platforms, particularly content that could negatively affect election processes.

The problem is acute – and timely. In 2024, elections will be held in over 40 countries, cumulatively affecting more than 4 billion people. Fears of election tampering through AI-generated content, moreover, are increasingly justified. *CNBC*, for instance, has noted that "Machine-learning tech firm Clarity recently reported a 900% annual increase in AI-generated 'deepfake' content, which raises concerns regarding the potential for interference with this year's elections around the globe." (UPI, February 17, 2024)

BEIJING RAMPS UP INFORMATION MANIPULATION
China's government is stepping up the extent of its disinformation and propaganda campaigns. A recent report by Citizen Lab, a cybersecurity research lab at the University of Toronto, lays out that "Chinese websites are posing as local news outlets to disseminate pro-Beijing content." The campaign, which Citizen Lab named "Paperwall," involved over 100 fake news outlets in more than 30 countries which deceptively appear as local news outlets. Citizen Lab has reason to believe that Shenzhen Haimaiyunxiang Media Co., Ltd. (also known as Haimai), a PR firm based in China, is behind the "Paperwall" effort.

Nor is this the first time China has tried to spread pro-Beijing content through social media. In August, China was "officially linked" to a foreign influence campaign known as "Spamouflage" which was aimed at audiences in Taiwan, America, Australia, the UK, and other nations. According to Citizen Lab, the latest revelations "confirm the increasingly important role private firms play in the realm of digital influence operations and the propensity of the Chinese government to make use of them." (*Newsweek*, February 9, 2024)