Information Warfare Watch No. 8

October 21, 2021 **Ilan I. Berman**, **Joaquin Liviapoma**

Related Categories: Democracy and Governance; Human Rights and Humanitarian Issues; Military Innovation; Public Diplomacy and Information Operations; Global Health; China; East Africa; Russia

DISINFORMATION IS RESHAPING KENYAN DISCOURSE

The spread of disinformation in Kenya is reaching new heights, as influencers smear the reputations of journalists, judges and activists in the country via paid social media campaigns. The attacks are coordinated through "WhatsApp groups to avoid detection," with their main purpose to villainize organizations and individuals who oppose entrenched political interests, an investigation by the Mozilla Foundation and *Wired* has found. "Members of civil society and journalists alike have increasingly come under disinformation attacks that seek to silence them, muddy their reputations, and stifle their reach," the magazine notes. Influencers are paid between $10 and $15 to participate in as many as three campaigns a day - making social media manipulation a tremendously lucrative enterprise in a country where annual per capita income stood at around $2,000 last year.

Nor is this sort of social media manipulation unique to Kenya. Throughout Africa "political actors are exploiting Twitter features like trends, its engagement mechanics, and account creation to try to control political narratives — crowding the conversation with disinformation and harassing dissenting voices," *Wired* notes. Twitter, meanwhile, has proven slow to abate such harmful activity, in part because it profits from advertising associated with "trending topics," including on political issues. (*Wired*, September 8, 2021)

CHINA'S WIDENING SOCIAL MEDIA MANIPULATION

Last month, cybersecurity firm Mandiant issued a new report on its tracking of China's influence campaigns on various social media platforms - an effort that, the firm says, has been steadily gathering steam since it began keeping tabs on it in mid-2019. Among Mandiant's findings are that the scope of China's activities are far broader than previously understood, in terms of both the languages and platforms it has leveraged. Chinese influence campaigns are "taking place on 30 social media platforms and over 40 additional websites and niche forums, and in additional languages including Russian, German, Spanish, Korean, and Japanese," the study details. Significant, too, is that much of China's influence activities center on spreading disinformation relating to the coronavirus pandemic. China-linked accounts, Mandiant notes, have "actively sought to physically mobilize protestors in the U.S. in response to the COVID-19 pandemic" - albeit with little success so far. They have also sought to promote conspiracy theories, such as that COVID-19 originated at the U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID) in Fort Detrick, Maryland. (FireEye, September 2021)

THE U.S. ARMY FOCUSES ON THE "INFORMATION ADVANTAGE"

America's military is stepping up its information warfare game. The U.S. Army is said to be embracing the concept of informational advantage, entailing five core tasks for the service: "enabling decision-making; protecting friendly information; informing and educating domestic audiences; informing and influencing international audiences; and conducting information warfare." What this looks like in practice is a range of activities not normally the focus of the American warfighter, but which have become increasingly indispensable on today's battlefield, among them dispelling disinformation and robust messaging to key foreign publics. (*Defense News*, September 9, 2021)

RUSSIAN DISINFO CAMPAIGNS GETTING AROUND WESTERN DEFENSES

In response to crackdowns by Western social media companies like YouTube, Russian propaganda outlets are changing tactics. One shift has been in the platforms on which Russian propaganda is appearing; in response to the banning of posts by Facebook and Twitter, Russian propagandists have taken to the comments sections of western media outlets like *Fox News*, the *Daily Mail* and *Der Spiegel*, researchers at Cardiff University have found. Another change has been the use of "mirror sites" - websites not yet banned by censors and governments - which can be used to repost blocked content, at least temporarily. Finally, in response to moves by YouTube and others to "demonetize" content, Russian propaganda generators have taken their appeals for funds directly to the masses and have embedded requests for donations within their video content. (*Financial Times*, September 23, 2021)

HOW AI WILL REVOLUTIONIZE PROPAGANDA
The field of artificial intelligence is evolving, and the technology is now being used for a growing range of applications in commerce, business and warfighting. Increasingly, however, AI is also being applied to the information space - and could soon be weaponized by malicious actors to spread disinformation and fake news. Researchers at Georgetown University's Center for Security and Emerging Technology (CSET) have warned that AI can be harnessed to generate massive amounts of disinformation using technologies like the Generative Pre-trained Transformer developed by San Francisco-based OpenAI, which train AI to quickly and autonomously generate a wide range of content. The result, CSET researchers say, is the production of "everything from tweets and translations to news articles and novels," carried out rapidly and at a level of sophistication that makes it difficult to discern that it was not generated by humans. (*Breaking Defense*, September 30, 2021)