How The FBI Helps Ukrainian Intelligence Hunt 'Disinformation' On Social Media

In an interview, a senior Ukrainian official defined "disinformation" as any news that contradicts his government's message.

LEE FANG
APR 28, 2023

The Federal Bureau of Investigation pressures Facebook to take down alleged Russian "disinformation" at the behest of Ukrainian intelligence, according to a senior Ukrainian official who corresponds regularly with the FBI. The same official said that Ukrainian authorities define "disinformation" broadly, flagging many social media accounts and posts

that he suggested may simply contradict the Ukrainian government's narrative.

"Once we have a trace or evidence of disinformation campaigns via Facebook or other resources that are from the U.S., we pass this information to the FBI, along with writing directly to Facebook," said Ilia Vitiuk, head of the Department of Cyber Information Security in the Security Service of Ukraine.

"We asked FBI for support to help us with Meta, to help us with others, and sometimes we get good results with that," noted Vitiuk. "We say, 'Okay, this was the person who was probably Russia's influence.'"

Vitiuk, in an interview, said that he is a proponent of free speech and understands concerns around social media censorship. But he also admitted that he and his colleagues take a deliberately expansive view of what counts as "Russian disinformation."

"When people ask me, 'How do you differentiate whether it is fake or true?' Indeed it is very difficult in such an informational flow," said Vitiuk. "I say, 'Everything that is against our country, consider it a fake, even if it's not.' Right now, for our victory, it is important to have that kind of understanding, not to be fooled."

In recent weeks, Vitiuk said, Russian forces have used various forms of disinformation to manufacture fake tension between President Volodymyr Zelenskyy and Valerii Zaluzhnyi, the four-star general who serves as commander-in-chief of Ukraine's military.

Indeed, recent reports have focused on the relationship between the two Ukrainian leaders. The German newspaper Bild reported that Zelenskyy and Zaluzhnyi had argued regarding tactics deployed in the battle over Bakhmut. Vitiuk said that any notion of conflict between Zelenskyy and his military chief, however, is false.

"They try to create problems in Ukraine, and they try to sow the seeds of misunderstanding between Ukraine and our partners that support us," said Vitiuk.

Vitiuk, a senior official in Ukraine's domestic intelligence agency, spoke to me this week at the RSA Convention in San Francisco, an annual gathering that brings together a collection of cyber security firms, law enforcement, and technology giants.

The FBI has elicited scrutiny of late for the influence it exercises over at Twitter, Facebook, and other social media platforms. A series of reports and congressional hearings delved into the agency's role in shaping content moderation decisions related to the 2020 election.

Evidence of FBI pressure on social media companies comes at a time when those companies are already taking proactive steps to hunt down alleged foreign propaganda and fabricated materials. Since Russia's invasion of Ukraine began in Feb. 2022, social media companies have been on the alert for hack and leak operations, fake personas, and other online tricks that might be used by Moscow to sway public opinion around the conflict. But critics charge that in the drive to label and remove content planted by the Russian government, Facebook and other tech firms suppress independent reporting and dissenting views about the war.

Last week, for instance, Facebook applied limited sharing penalties and a "false information" label to links containing journalist Seymour Hersh's Substack story alleging NATO involvement in the destruction of the Nord Stream pipeline, according to Michael Shellenberger, a writer who extensively covers social media censorship. After public outcry, Facebook modified the label to "partially false."

It is unclear how much of social media companies' heavy-handed approach to content moderation is a direct response to government goading.

Type your email... Subscribe

But there is enough of a pattern of the FBI and other national security agencies leaning on tech companies to suggest that these tech firms may preemptively adopt censorious practices to avoid the disapproval of the federal government. In October, based on leaked documents from

the Department of Homeland Security, I reported on government plans to lean more heavily on social media platforms to take down "disinformation" related to "the nature of U.S. support to Ukraine."

Emails revealed through the Twitter Files further show a number of FBI agents in regular correspondence with Twitter executives, pressing for the detection and removal of Russian content. In one exchange revealed by journalist Matt Taibbi, Elvis Chan, a special agent assigned to the San Francisco FBI field office, expressed frustration that Twitter officials had "not observed much recent activity from official propaganda actors on your platform." Chan was part of the FBI team that had weekly meetings with Twitter to warn about Russian disinformation leading up to the 2020 election. Following repeated warnings from the FBI about a potential Russian influence operation, Twitter banned links to a New York Post story about the contents of the Hunter Biden laptop in the weeks before the election.

The extent of U.S. military and intelligence shapes domestic social media conversations about the Ukraine-Russia war is still unclear. This week, researcher Jack Poulson revealed a presentation from U.S. Army Cyber Command shortly after the invasion began, in which Lt. Colonel David Beskow referenced work to defend NATO's "brand" across social media platforms.

Ukraine is, to be sure, responding in part to a real national-security threat. Russian disinformation campaigns have persisted for years and have taken many forms, Vitiuk said. Ukraine's Department of Cyber Information Security has taken down many bot networks used by Russian forces to create confusion and fear within the Ukrainian public, he noted. Russian hackers have targeted power generation, utilities, and much of Ukraine's civil society.

Vitiuk said he did not know about Facebook's recent throttling of the Hersh article. But he cited the well-publicized forgery of the so-called Discord Leaks, in which pro-Russian voices on the platform Telegram had manipulated one of the leaked military documents to falsely claim higher Ukrainian and lower Russian casualty levels during the war, as a prominent example of disinformation.

During the RSA convention, Vitiuk spoke on a panel alongside Bryan Vorndran, the assistant director of the FBI's Cyber Division; Alex Kobzanets, an FBI agent with the bureau's San Francisco office; and Laura Galante from the Office of the Director of National Intelligence.

During the panel, Vitiuk thanked the Ukrainian government's many public and private sector allies in the United States, including Mandiant, Cisco, CrowdStrike, Clearview, Google, Amazon, and Starlink, among others. Cyber security support from American partners has

helped thwart Russian cyber attacks on civilian and military infrastructure and have been a "psychological game changer," Vitiuk said. He emphasized that the FBI has been his agency's "top partner."

The war effort has also taught the FBI new lessons in private-public partnerships, according to Kobzanets. "I don't know how many times we've called the CEOs here in San Francisco to drive to their office on a Sunday afternoon and really engage with our Ukrainian partners," he said.

After rousing closing remarks from Vitiuk, several FBI agents in the audience, including Elvis Chan, stood for applause.

Chan and Kobzanets declined to speak to me and referred me to the FBI's media office, which did not respond to my email request for comment on Vitiuk's claims. Facebook also did not respond to a request for comment.

Image via Lee Fang, llia Vitiuk, chief of the SSU Cyber Security Department (left) poses with Timothy Langen, Executive Assistant Director of the FBI's Criminal, Cyber, Response and Services Branch (right) at the RSA Conference in San Francisco, April 26th, 2023.

A brief note to readers:

This week I migrated the website domain of this Substack to www.leefang.com. If you can, please share this newsletter and subscribe.

I also appeared on several programs to discuss our last investigation into Pfizer's funding of groups that lobbied for the COVID-19 vaccine mandate, including Russell Brand on Rumble, The Hill TV's Rising with Briahna Joy Gray and Robby Soave, and Kim Iverson on Rumble.