U.S. Army Info War Division Wants Social Media Surveillance to Protect "NATO Brand"

An Army Cyber Command official sought military contractors that could help "attack, defend, influence, and operate" on global social media.

By Sam Biddle

Global Research, May 02, 2023
The Intercept 27 April 2023

Region: USA
Theme: Intelligence

***

The US Army Cyber Command told defense contractors it planned to surveil global social media use to defend the "NATO brand," according to a 2022 webinar recording reviewed by The Intercept.

The disclosure, made a month after Russia's invasion of Ukraine, follows years of international debate over online free expression and the influence of governmental security agencies over the web. The Army's Cyber Command is tasked with both defending the country's military networks as well as offensive operations, including propaganda campaigns.

The remarks came during a closed-door conference call hosted by the Cyber Fusion Innovation Center, a Pentagon-sponsored nonprofit that helps with military tech procurement, and provided an informal question-and-answer session for private-sector contractors interested in selling data to Army Cyber Command, commonly referred to as ARCYBER.

Though the office has many responsibilities, one of ARCYBER's key roles is to detect and thwart foreign "influence operations," a military euphemism for propaganda and deception campaigns, while engaging in the practice itself. The March 24, 2022, webinar was organized to bring together vendors that might be able to help ARCYBER "attack, defend, influence, and operate," in the words of co-host Lt. Col. David Beskow of the ARCYBER Technical Warfare Center.

While the event was light on specifics — the ARCYBER hosts emphasized that they were keen to learn whatever the private sector thought was "in the realm of possible" — a recurring topic was how the Army can more quickly funnel vast volumes of social media posts from around the world for rapid analysis.

At one point in the recording, a contractor who did not identify themselves asked if ARCYBER could share specific topics they plan to track across the web. “NATO is one of our key brands that we are pushing, as far as our national security alliance,” Beskow explained. “That’s important to us. We should understand all conversations around NATO that has happened on social media.”

He added, “We would want to do that long term to understand how — what is the NATO, for lack of a better word, what’s the NATO brand, and how does the world view that brand across different places of the world?”

Beskow said that ARCYBER wanted to track social media on various platforms used in places where the U.S. had an interest.

“Twitter is still of interest,” Beskow told the webinar audience, adding that “those that have other penetration are of interest as well. Those include VK, Telegram, Sina Weibo, and others that may have penetration in other parts of the world,” referring to foreign-owned chat and social media sites popular in Russia and China. (The Army did not respond to a request for comment.)

The mass social media surveillance appears to be just one component of a broader initiative to use private-sector data mining to advance the Army’s information warfare efforts. Beskow expressed an interest in purchasing access to nonpublic commercial web data, corporate ownership records, supply chain data, and more, according to a report on the call by the researcher Jack Poulson.

“The NATO Brand”

Tracking a brand’s reputation is an extremely common marketing practice. But a crucial difference between a social media manager keeping tabs on Casper mattress mentions and ARCYBER is that the Army is authorized to, in Beskow’s words, “influence-operate the network … and, when necessary, attack.” And NATO is an entity subject to intense global civilian scrutiny and debate.

While the webinar speakers didn’t note whether badmouthing NATO or misrepresenting its positions would be merely monitored or actively countered, ARCYBER’s umbrella includes seven different units dedicated to offense and propaganda. The 1st Information Operations Command provides “Social Media Overwatch,” and the Army Civil Affairs and Psychological Operations Command works to “gain and maintain information dominance by conducting Information Warfare in the Information Environment,” according to ARCYBER’s website.

Though these are opaque, jargon-heavy concepts, the term “information operations” encompasses activities the U.S. has been eager to decry when carried out by its geopolitical rivals — the sort of thing typically labeled “disinformation” when emanating from abroad.

The Department of Defense defines “information operations” as those which “influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own,” while “influence operations” are the “United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power."

ARCYBER is key to the U.S.'s ability to do both.

While the U.S. national security establishment frequently warns against other countries' "weaponization" of social media and the broader internet, recent reporting has shown the Pentagon engages in some of the very same conduct.

Last August, researchers from Graphika and the Stanford Internet Observatory uncovered a network of pro-U.S. Twitter and Facebook accounts covertly operated by U.S. Central Command, an embarrassing revelation that led to a "sweeping audit of how it conducts clandestine information warfare," according to the Washington Post. Subsequent reporting by The Intercept showed Twitter had whitelisted the accounts in violation of its own policies.

Despite years of alarm in Washington over the threat posed by deepfake video fabrications to democratic societies, The Intercept reported last month that U.S. Special Operations Command is seeking vendors to help them make their own deepfakes to deceive foreign internet users.

It's unclear how the Army might go about conducting mass surveillance of social media platforms that prohibit automated data collection.

During the webinar, Beskow told vendors that "the government would provide a list of publicly facing pages that we would like to be crawled at a specific times," specifically citing Facebook and the Russian Facebook clone VK. But Meta, which owns Facebook and Instagram, expressly prohibits the "scraping" of its pages.

Asked how the Army planned to get around this fact, Beskow demurred: "Right now, we're really interested in just understanding what's in the realm of the possible, while maintaining the authorities and legal guides that we're bound by," he said. "The goal is to see what's in the realm of possible in order to allow our, uh, leaders, once again, to understand the world a little bit better, specifically, that of the technical world that we live in today."

*

Note to readers: Please click the share button above. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

Featured image source

The original source of this article is The Intercept

Articles by: Sam Biddle