Researchers detail new ‘gray zone conflict’ in AI-driven Chinese propaganda

Documents from Chinese firm GoLaxy detail influence operations aligned with Beijing that run at unprecedented speed and precision. National security experts at Vanderbilt say these developments may forever redefine information warfare.

David DiMolfetta August 11, 2025

MF3d/Getty Images

The Chinese government is enlisting a range of domestic AI firms to develop and run sophisticated propaganda campaigns that look far more lifelike than past public manipulation efforts, according to a cache of documents from one such company reviewed by Vanderbilt University researchers.

The company, GoLaxy, has built data profiles for at least 117 sitting U.S. lawmakers and more than 2,000 other American political and thought leaders, according to the researchers that assessed the documentation. GoLaxy also appears to be tracking thousands of right-wing influencers, as well as journalists, their assessments show.

"You start to imagine, when you bring these pieces together, this is a whole new sort of level of gray zone conflict, and it's one we need to really understand," said Brett Goldstein, a former head of the Defense Digital Service and one of the Vanderbilt faculty that examined the files.

Goldstein was speaking alongside former NSA director Gen. Paul Nakasone, who heads Vanderbilt's National Security Institute, in a gathering of reporters on the sidelines of the DEF CON hacker convention in Las Vegas, Nevada.

"We are seeing now an ability to both develop and deliver at an efficiency, at a speed and a scale we've never seen before," said Nakasone, recalling his time in the intelligence community tracking past campaigns from foreign adversaries to influence public opinion.

Founded in 2010 by a research institute affiliated with the state-run Chinese Academy of Sciences, GoLaxy appears to operate in step with Beijing's national security priorities, despite no public confirmation of direct government control. Researchers said the documents indicate the firm has worked with senior intelligence, party and military elements within China's political structure.

The firm has launched influence campaigns against Hong Kong and Taiwan, and uses a propaganda dissemination system dubbed "GoPro" to spread content across social media, according to the researchers.

Goldstein, as well as his Vanderbilt colleague Brett Benson, first detailed the research in a New York Times guest essay. The Times then separately reported on the findings and confirmed the efforts, citing current and former U.S. officials.

The cache was sent to Vanderbilt from a security researcher in April, Goldstein told reporters. Nearly all of the documentation was written in Mandarin, he added.

The firm has recently altered content on its website that removed references to its work with Beijing and denied the findings. A since-removed blog post, for instance, reveals GoLaxy pitched its AI tools to senior Chinese police and security officials.

"GoLaxy's products are mainly based on open-source data, without specially collecting data targeting U.S. officials," the firm told NYT.

"To my knowledge, China is rapidly building an AI governance system with distinct national characteristics. This approach emphasizes a balance between development and security, featuring innovation, security and inclusiveness," Liu Pengyu, spokesperson for China's embassy in Washington, D.C., said. "The government has introduced major policy plans and ethical guidelines, as well as laws and regulations on algorithmic services, generative AI, and data security. Together, these frameworks aim to improve the safety, fairness, and governance capacity of AI technologies in China."

China's use of GoLaxy's technology is not the first time a U.S. adversary has leveraged AI to conduct influence operations at scale, but GoLaxy's operation goes further, said Max Lesser, a senior emerging threats analyst at the Foundation for Defense of Democracies.

"While AI can certainly augment influence operations, it remains unclear whether it increases their impact," he told *Nextgov/FCW*.

The Trump administration has largely dismantled offices that track influence operations, amid accusations that they have in the past censored Americans' online speech when they coordinated with social media platforms to remove false information about contentious topics like the 2020 election and COVID-19 vaccine efficacy.

Under Director of National Intelligence Tulsi Gabbard, the White House has also sought to diminish previous intelligence community findings that determined Russia launched an influence campaign to sway the outcome of the 2016 election in favor of President Donald Trump. Multiple reviews, including a comprehensive bipartisan Senate Intelligence Committee report, concluded that Russian President Vladimir Putin sought to help Trump win.

ODNI under former President Joe Biden tracked influence operations launched by Russia, China and other foreign adversaries in the lead-up to the 2024 election. But they were never able to provide an assessment of the campaigns' effectiveness because it would require intelligence analysts to pore through Americans' social media posts and compromise their free speech rights, officials previously said.

Asked about whether the intelligence community should be drilling down on the effectiveness of influence campaigns, Nakasone said that the spy community needs to use its already given authorities to track threats overseas, but that there's a "private sector piece" as well.

"You're going to need a team, and it's going to be a team that needs to think how they're going to do this effectively and also creatively in the future," he said.

That may require a regulatory structure. But Goldstein dismissed the idea of new regulations to solve the budding problem of more advanced influence operations.

"How do we have better detect methods, and how do we spur that research, academically [with the] private sector? Pieces like that,” he said. “I don’t know how regulation gets at that. I would be growing the private sector ecosystem. I’d be focused on academic research.”

The documents also suggest that there are accounts and personas hiding on Chinese-aligned infrastructure that can be taken down through standard U.S. operations that have dismantled launch points for hacks, Goldstein said.

“I think I come back to the concept of persistent engagement,” Nakasone said. “We should always be involved with our adversaries here. This is a really good case study of: it’s out there, and we need to find it and we need to be able to take it down.”

Share This:

NEXT STORY: In pitch to hacker community, Trump’s NSC cyber lead says AI key to future of cyberdefense