The Era of A.I. Propaganda Has Arrived, and America Must Act

NY Times, August 5, 2025

Russia's efforts to interfere in the 2016 and 2020 U.S. presidential elections were pretty low-tech. Relying on generic bot messaging, low-quality content and mass targeting, their operations probably had limited impact.

Those days are over. With the exponential rise of generative A.I. systems, the greatest danger is no longer a flood of invective and falsehoods on social media. Rather, it is the slow, subtle and corrosive manipulation of online communication — propaganda designed not to shock, but to slip silently into our everyday digital discussions. We have entered a new era in international influence operations, where A.I.-generated narratives shift the political landscape without drawing attention.

A Chinese company called GoLaxy is already undertaking such operations, according to a large cache of documents recently uncovered by the Vanderbilt University Institute of National Security, where we work. The materials show GoLaxy emerging as a leader in technologically advanced, state-aligned influence campaigns, which deploy humanlike bot networks and psychological profiling to target individuals. Its activities and claims suggest it has connections to the Chinese government.

GoLaxy has already deployed its technology in Hong Kong and Taiwan, and the documents suggest it may be preparing to expand into the United States. A.I.-driven propaganda is no longer a hypothetical future threat. It is operational, sophisticated and already reshaping how public opinion can be manipulated on a large scale.

A representative of GoLaxy said the company focused on services for business intelligence and denied it had developed a bot network or psychological profiling tools targeting individuals. The company also denied being under the authority of any government agency or organization.

What sets GoLaxy apart is its integration of generative A.I. with enormous troves of personal data. Its systems continually mine social media platforms to build dynamic psychological profiles. Its content is customized to a person's values, beliefs, emotional tendencies and vulnerabilities. According to the documents, A.I. personas can then engage users in what appears to be a conversation — content that feels authentic, adapts in real-time and avoids detection. The result is a highly efficient propaganda engine that's designed to be nearly indistinguishable from legitimate online interaction, delivered instantaneously at a scale never before achieved.

While the documents offered no specific examples of these conversations, they describe how the technology develops personalized content. By extracting user data and studying broader patterns, A.I. can build synthetic messaging designed to appeal to a wide spectrum of the public. It can adapt to a user's tone, values, habits and interests, according to the documents. Then it can mimic real users by liking posts, leaving comments and pushing targeted content.

According to the documents we uncovered, GoLaxy used its technology to minimize opposition to a 2020 national security law that cracked down on political dissent, identifying thousands of participants and thought leaders from 180,000 Hong Kong Twitter accounts. Then GoLaxy went after what it perceived as lies and misconceptions, "correcting" the sources via its army of fake profiles.

The company struck again in the lead-up to the 2024 Taiwanese election, when China-aligned groups peddled false claims of corruption and posted deepfakes on social media. During the campaign, GoLaxy suggested ways to undermine Taiwan's Democratic Progressive Party, which opposes China's claims over the island. The company gathered and most likely supplied information on trends in Taiwanese political debate and recommended the deployment of bot networks to exploit political divisions between its parties. GoLaxy had already amassed an abundance of data on Taiwan to support such intrusions, according to the documents, including organizational maps of government institutions — down to their political tendencies, attitude toward China and GPS coordinates — and profiles of over 5,000 accounts belonging to Taiwanese people.

In a written statement, GoLaxy denied providing technical support for activities in Hong Kong and Taiwan.

So far, GoLaxy's active deployments appear to have been confined to the Indo-Pacific. Evidence in the documents suggests that the company is positioning itself for expanded operations, including in the United States. GoLaxy has assembled data profiles of at least 117 members of the U.S. Congress and over 2,000 American political figures and thought leaders. Assuming GoLaxy continues to build American dossiers, it is possible the company will bring its operations across the Pacific. It said it has not collected data targeting U.S. officials

GoLaxy operates in close alignment with China's national security priorities, although no formal government control has been publicly confirmed. The company was founded in 2010 by a research institute at the state-controlled Chinese Academy of Sciences, and has been chaired by a deputy director from the same institute. Since then, GoLaxy has, according to the documents, worked with top-level intelligence, party and military bodies, suggesting integration with China's political system.

GoLaxy's strategic alignment became clearer in 2021, when it received funding from Sugon, a Beijing-based supercomputing company flagged by the Pentagon as a Chinese military affiliate. GoLaxy's public-facing A.I. platform coordinates with Sugon's supercomputers and DeepSeek-R1, one of China's leading A.I. models.

These connections are a reminder that influence operations are no longer a sideshow — they are becoming core instruments of statecraft. Battlefields include not only geographic territory with troops and ships but also the online platforms we use every day.

The strategy deployed by GoLaxy and others weaponizes the openness that underpins democratic societies. Debate, transparency and pluralism — hallmarks of democratic strength — are also points of vulnerability. Technological tools like GoLaxy's exploit these qualities. The line between surveillance and persuasion is disappearing, fast.

The danger lies in the stealth and scale of these methods, and the speed with which they are improving. A.I.-generated content can be deployed quietly across entire populations with minimal resistance. It operates continually, shaping opinion and corroding democratic institutions beneath the surface. Imagine today's most effective social media platforms, but on a far greater scale, using a far more comprehensive model of its targets and synthetic propaganda that is even more compelling and difficult to resist.

To counter the growing threat of A.I.-driven foreign influence operations, a coordinated response is essential. Academic researchers must work urgently to map how artificial intelligence, open-source intelligence and online influence campaigns converge to serve hostile state objectives. The U.S. government must take the lead in disrupting the infrastructure behind these operations, with the Defense Department targeting foreign influence networks and the Federal Bureau of Investigation working closely with digital platforms to identify and counter false personas. The private sector needs to accelerate A.I. detection capabilities to bolster our ability to detect synthetic content. If we can't identify it, we can't stop it.

We are entering a new era of gray-zone conflict — one marked by information warfare executed at a scale, speed and degree of sophistication never seen before. If we don't quickly figure out how to defend against this kind of A.I.-driven influence, we will be completely exposed.