

**Brett Goldstein**  
Special Advisor to the Chancellor  
Research Professor in Engineering  
Science & Management  
Vanderbilt University, Nashville, TN  
Brett.goldstein@vanderbilt.edu

**Brett Benson**  
Associate Professor of Political  
Science and Asian Studies  
Vanderbilt University, Nashville, TN  
Brett.benson@vanderbilt.edu

# China's Surveillance Moves Overseas

*This policy paper explains and analyzes a new leak from Geedge Networks, a manufacturer of a commercial version of China's Great Firewall. With authoritarian states increasingly exploring artificial intelligence as a tool to synthesize data gathered on broad swaths of their populations, this leak provides actual evidence of how China may be putting such plans into practice. Ultimately, this paper advocates for stricter U.S. export controls as a key step to counter predictive Chinese surveillance initiatives that weaponize AI against a population.*

## INTRODUCTION

Authoritarian states have always tried to get out ahead of dissent—to determine who is a threat, who they interact with, and what they might do. In support of such goals, these governments have spent years accumulating enormous quantities of data on their citizens: facial recognition feeds, cell tower location histories, internet traffic, browsing activity, and social networks. And while there is a wealth of information, it is difficult to put it to effective use.

Artificial intelligence is now closing that gap, as revealed by a new leak of internal Chinese corporate documents analyzed by the Wicked Problems Lab. AI-backed predictive surveillance is changing what that information can do. Data that once required armies of human analysts to interpret incompletely can now profile individuals at scale and flag potential threats for suppression before dissent emerges.

## THE CRACK IN THE GREAT FIREWALL

Authoritarian systems rarely expose internal discussions about the ambitions and limitations of their surveillance capabilities. However, a series of data leaks in 2025 have opened a window into how China's surveillance ecosystem actually works. In August 2025, the Wicked Problems Lab team at the Vanderbilt Institute of National Security uncovered a set of internal documents belonging to the Chinese company GoLaxy, a Beijing-based firm that claims to have worked for Chinese intelligence and military



institutions. The files revealed that GoLaxy harvests online social media data to build profiles on targeted users, then using those profiles to engage and manipulate targets through adaptable AI personas.

A month later, a massive leak of internal data belonging to a different Chinese company surfaced online. That firm, Geedge Networks, manufactures technology used to censor and monitor internet activity inside China, and is a provider of China’s commercial version of the Great Firewall. Analyzing the Geedge documents, our team found evidence of a comprehensive monitoring architecture that aggregates digital traffic, location data, and social connections into a single profile for each citizen. This newer leak provides a rare window into the ambitions, architecture, and constraints of next-generation authoritarian surveillance systems.

While GoLaxy and Geedge are just two companies, the now-public cache of information we know about them gives substantial insight into how China’s surveillance ecosystem is structured. China’s top governing institutions set the broad aspirations for security and surveillance. Then, the Chinese Academy of Sciences—China’s massive, state-owned research institute—develops the talent and research institutes to advance these goals. The Academy spins off commercial firms like GoLaxy and Geedge. These firms productize the technology, sell the capabilities to state institutions, and deploy the systems against their own citizens. Many of these firms have dual-use commercial operations alongside their state contracts, often clouding the distinction between legitimate commercial activity and surveillance operations built for the state.

China’s surveillance ecosystem does not stop at the country’s borders. The Geedge documents reveal the export of these systems into other countries including Myanmar, Pakistan, Ethiopia, and Kazakhstan. The risks extend beyond the spread of discrete Chinese-made surveillance platforms. Chinese-built infrastructure deployed abroad creates the potential for backdoor access into data collected by those systems. The Geedge documents do not show this is happening. But the concern is not hypothetical. It reflects longstanding concerns about covert access to personal data from Chinese telecommunications and digital infrastructure abroad.

### **From Reactive to Proactive**

Looking through minutes and progress reports from Geedge Network’s research teams, it is clear that they were focused on exploring how large language models could synthesize enormous volumes of intercepted data. That data included location histories, social ties, browsing activity, and other metadata. The documents discuss linking users’ physical movements to their online activity in real time and at scale. The goal was to build behavioral profiles of individuals deemed “harmful”—not simply to understand what people have already done, but to anticipate what they might do next and with whom.

Predictive surveillance changes the character of authoritarian control. The traditional authoritarian playbook is largely reactive—find out what citizens said or did, then punish them for it. Predictive capacity was limited. Human analysts can only do so much with fragmented data.



But AI-backed predictive surveillance promises continuous behavioral modeling across entire populations. In systems like these, ordinary activities—where someone travels, whom they meet, what they read and say, what patterns they resemble—can become inputs into algorithmic judgments about the political risks they pose. Importantly, these systems move government intervention earlier in the chain. They identify the people and networks that could become a threat. They infer intent. They intervene before dissent has organized itself enough to be visible. The trigger for state action is no longer something the citizen did. It is something the state believes the citizen will do.

The current capabilities of these systems remain unclear, and their actual predictive accuracy may be weaker than their designers hope. But even imperfect AI-enabled behavioral modeling can expand the repressive capacity of the state by targeting harmless individuals through mistaken or overly suspicious inference while casting a pervasive shadow of fear over ordinary life.

### **The Cost of Seeing the Future**

The predictive surveillance system laid out by Geedge is not cheap work. It requires enormous compute, and this is where U.S. export controls on advanced GPUs began to bite—until they were lifted.

A well-documented GPU bottleneck squeezed China from late 2022 to the present. In October 2022, the Biden administration imposed a ban on the export of high-end GPUs, such as those produced by NVIDIA and AMD. This immediately disrupted Beijing's ability to conduct large-scale AI training. As a temporary workaround, NVIDIA introduced downgraded A800 and H800 chips designed to comply with export thresholds. Think of these as deliberately trimmed back versions of the most advanced chips—fast enough to be useful but capacity-capped to keep them below the most demanding AI workloads.

Access to these chips brought temporary relief to Chinese tech companies. Yet in October 2023, these loopholes were closed, and the export of those chips was also restricted. At the same time, demand for compute power surged. Major firms like Alibaba, Tencent, and Baidu accelerated efforts to train large models, deploy AI-enabled services, and expand cloud offerings. A growing group of AI startups entered the market, while state-backed initiatives expanded compute clusters and scaled inference-heavy systems, including surveillance and data integration platforms. These activities required large, simultaneous access to GPUs. Supplies could not keep pace. Firms relied on stockpile inventory, competed for limited cloud capacity, or turned to lower-performance domestic substitutes.

Large tech firms shifted strategy away from massive training runs toward smaller models optimized for efficient inference. Smaller firms pivoted to renting GPU time rather than owning their own clusters, downsizing training runs, or altogether paused or scaled back projects.

The Geedge dump reveals the effects of compute constraints. In the 2024 portion of the dump (the most recent year available), the researchers explicitly discuss "GPU



limitations," after which we see a shift toward more static knowledge-base approaches. The documents suggest Geedge was adapting its technical pathway to operate within constrained compute limits.

We see Geedge pivot clearly in two distinct ways. One is through the legacy methods of knowledge graphs; at the same time, the team is starting to find creative ways to better use their existing NVIDIA A800s by exploring potential "two-stage fine-tuning." Restricting GPUs can make advances materially harder—in this case, for a Chinese company developing next-generation surveillance methods to "predict" who might be a problem. Their progress appears to have slowed.

## **CONCLUSION AND POLICY RECOMMENDATIONS**

The timing of all these factors is telling. Geedge Network's pivot to static knowledge-graph approaches tracks closely with both China's surging demand for advanced chips and the expanded chip restrictions that cut off supply. Geedge's adaptability shows that Beijing will find workarounds—denying GPUs is not a permanent solution.

But export controls do not need to be permanently effective to provide critical support to U.S. interests. Delay and timing matter. Such restrictions create time for policymakers and technical experts to adapt, develop solutions, and deploy countermeasures. In the AI revolution, time is everything. Democratic countries need a window to build resilient domestic tech infrastructure, to close back-door vulnerabilities in Chinese-made systems, to develop legislative guardrails, and to detect and counter surveillance data collection at scale.

For the past two years, export controls were quietly suffocating Beijing's surveillance ambitions. Now the pressure is relaxing. The key policy adjustment shifted from blanket denial of advanced GPUs to conditional access. Notably, the export of some more advanced chips including NVIDIA H200, and comparable products from AMD and Intel, were approved to vetted Chinese customers. The conditional access framework assumes that chip end-use can be monitored and enforced. In China's state-directed system, meaningful separation between commercial and state-directed compute allocation is difficult to guarantee. Many compute-intensive firms serve the objectives of the state. Compute granted in one part of the ecosystem frees up capacity elsewhere. Following the implementation of the relaxed policy, Chinese firms immediately placed large orders. Yet Beijing blocked them, not for lack of demand for compute, but to speed the development of domestic chips and to create leverage for access to the most advanced western chips. Whether China develops its own compute or gains access to western chips, the brake is loosening.

Beijing's ambitions to deploy AI-driven predictive behavioral surveillance against its citizens and export these capabilities to other like-minded countries depends on its ability to generate the compute power required to run these demanding systems. If access to advanced semiconductors loosens, then Chinese firms will be better positioned to scale their predictive authoritarian surveillance capabilities. Export controls are not by



themselves a solution. But they are the difference between a threat that arrives before we are ready and one that arrives after.

## **ACKNOWLEDGEMENTS**

This report and all contents within would not have been possible without the generous support of the William & Flora Hewlett Foundation.

The Wicked Problems Lab at the Institute of National Security acknowledges the support of the Vanderbilt University Office of the Provost through the Discovery Vanderbilt initiative as well as the Office of the Chancellor, the School of Engineering, College of Arts & Science, and Peabody School of Education for their collaboration and assistance.

