



Jackson School of
Global Affairs

CHINA'S TECHNOGENOCIDE CAPSTONE

Shining a Light on China's
Uyghur Genocide

Authors:

Maxwell Cota, Beckett Elkins, Owen Haywood, Jasmine Jones, Sarah Markey, Isabella Panico, Karla Perdomo Nuñez, Julian Rivera, Aidan Urbina, and Anouk Y.

Our Client:



Supervised By:

Professor Scott Worden

Table of Contents

Executive Summary	3
Introduction	4
Artificial Intelligence as a Weapon of Technogenocide	6
• AI Weapons	
• IJOP Case Study	
Inputs of Technogenocide	
• Digital Components	10
• Hardware	
• Knowhow	
The Global Expansion of China's Surveillance Technology	29
• China's Digital Silk Road	
Existing Regulatory Framework	33
• Regulatory Imperative	
• Coverage Problems	
• Systemic Failures	
Recommendations	39
Conclusion	52

EXECUTIVE SUMMARY

The Chinese Communist Party is carrying out a systematic campaign to destroy the Uyghur people through what can be understood as technogenocide: the use of advanced digital technologies to enable mass repression, cultural erasure, and social control at unprecedented scale. This campaign relies on constant surveillance, predictive policing, forced assimilation, and the criminalization of everyday life. Technology is not incidental to these abuses; it is their enabling infrastructure. Since 2017, more than one million Uyghurs have been detained, millions more subjected to forced labor, family separation, religious repression, and invasive population control. At the core of this system is a dense surveillance architecture combining facial recognition, biometric data collection, spyware, and artificial intelligence–driven predictive policing. These tools allow authorities to flag individuals as “suspicious” based on routine behaviors such as prayer, travel, communication patterns, or device usage, often without any human decision-maker involved. Central to this system is the Integrated Joint Operations Platform (IJOP), an AI-powered policing and data fusion platform that aggregates information from cameras, checkpoints, mobile phones, government databases, and home visits. The IJOP automatically assesses “risk” and prompts detention, interrogation, or “re-education,” transforming civilian governance into a militarized system of preemptive control. This represents a fundamental shift in how repression is carried out: from punishing acts to policing identity, belief, and potential future behavior.

This report finds that China’s technogenocide of the Uyghurs has been enabled by three critical inputs: digital components, hardware, and know-how, many of which originate in or are supported by Western technology ecosystems. U.S. and allied companies have provided cloud computing services, advanced microchips, software tools, investment capital, research partnerships, and talent pathways that Chinese entities use to build, train, and scale surveillance systems in Xinjiang. Existing export controls have failed to address these forms of enablement, particularly with respect to cloud computing, digital services, and intangible technology transfers. Without urgent regulatory reform, accountability mechanisms, and human-rights-centered technology governance, technogenocide risks becoming a durable and exportable model of repression. This report calls for immediate action to close regulatory gaps, restrict technologies used in mass surveillance and repression, and ensure that Western technology is not complicit in crimes against humanity.

INTRODUCTION

The Uyghur people, a Turkic, predominantly Muslim ethnic group, have been subjected to the most sophisticated technological oppression in the world. With a population nearing 12 million, the Uyghurs reside in the Xinjiang Uyghur Autonomous Region of China, known to Uyghurs as East Turkestan.¹ Differences in the region's terminology highlight the historic tension between the People's Republic of China and the Uyghur people over who holds claim to the territory. For more than two centuries, China has maintained a colonial relationship with the Uyghurs, yet Uyghur culture continued to thrive and resist assimilation into the 21st century.² However, Chinese policies began to intensify in the late 1990s after the government launched its "Strike Hard" campaign against the "three evils" of terrorism, extremism, and separatism.³ The Chinese state capitalized on the moment by equating the "expressions of Uyghur identity, including language, culture, and religion" and their "aspirations for independence" to the very substance of the three evils.⁴ This characterization partnered with increased securitization in the early 2000s, laid the foundation for the PRC to initiate a methodology of ethnic cleansing.

In 2014, China released its fourth "Strike Hard" campaign explicitly aimed to curb violent extremism.⁵ Under the falsehood of counterterrorism, the CCP enacted a host of assimilationist and carceral policies designed to completely transform the region's demographics, culture, geography and economy. In the years following, China developed a system of mass surveillance, where cameras, police checkpoints, and data collection centers spanned every corner of the region.

By 2017, more than 1 million Uyghurs were forcibly detained in concentration camps, which the PRC labeled re-education centers. At these camps, internees were subject to prison-like conditions where they were forced to study the Chinese language and consume Communist Party propaganda. The Uyghur language and cultural practices were prohibited. In a leaked internal document, the PRC described its program as "washing brains, cleansing hearts, strengthening righteousness and eliminating evil."⁶

Since 2017, China has implemented a system that "can be unequivocally described as cultural genocide," according to Sean Roberts, a leading expert on Uyghur history.⁷ China claims to have ended its re-education centers, in 2019, but its repressive tactics have merely taken new form. As of 2023, nearly 3 million Uyghurs remain subjected to forced labor, and over half a million of the detainees are currently held in formal prisons.⁸ The PRC continues to destroy Uyghur culture through bans on Uyghur language education, destruction and desecration of mosques and burial sites, and restrictions on Islamic fasting, prayer, and attire.⁹ Family destruction initiatives place Uyghur children into boarding schools, forcibly marry Uyghur women to Han Chinese men, and sterilize Uyghur women.¹⁰ Each of the PRC's policies intend to collectively destroy the Uyghur identity. In 2021, the United States Department of State determined that China is committing genocide, and more than four years later there has been little progress to hold the PRC accountable.¹¹ Although the United States condemns China's genocide, it has failed to prevent its own technology from aiding in the development of Xinjiang's surveillance system.

This report will expand on how Western technology and corporations are complicit in the facial recognition, predictive policing, and spyware currently employed by the PRC.

It will also address vulnerabilities in research and data-sharing, which are at risk of being exploited by China to gain technical expertise.

The Uyghur genocide deviates from previous human rights concerns in two fundamental ways. First, it is the model framework for how artificial intelligence can be used as a system of mass surveillance and oppression. With new technology, China has empowered automated systems with the ability to profile, flag, and continuously monitor individuals. This changes how we understand government control, where data from phones, biometric indicators, and daily activity are processed and ready to exploit within minutes. Second, the genocide does not involve mass killings of individuals. Rather, China's system works because it is able to suppress the voices of Uyghurs within East Turkestan and maintain largely covert operations.

Several American national security concerns emerge from the Uyghur genocide. First, growth in China's technological capacity is increasing its global power in relation to the United States. Second, China has developed an exportable model of technological oppression, which can easily be spread across China's Digital Silk Road. If the west does not act now to address the gaps in its technology export legislation, there is an increasing risk that China's authoritarian allies will adopt the same playbook. Third, Uyghurs around the world face transnational repression like family coercion, online harassment, and systems of spy surveillance from the CCP. As China continues to implement such technologies, their expansion of transnational practices can potentially pivot towards American citizens, threatening their safety and privacy.

The following report examines how the CCP's campaign against the Uyghurs has been enabled and accelerated by modern technology and how Western governments and corporations have failed to prevent their own tools from being used in crimes against humanity. It analyzes the role of artificial intelligence as a weapon of repression and traces the key inputs that sustain this system: digital components such as cloud computing and spyware, physical hardware including microchips and surveillance equipment, and the transfer of technical know-how through research, investment, and partnerships. Finally, the report evaluates existing regulatory frameworks and exposes their systemic failures, before offering concrete policy recommendations aimed at closing legal loopholes, strengthening accountability, and ensuring that technology is no longer used to facilitate genocide.

ARTIFICIAL INTELLIGENCE AS A WEAPON OF TECHNOGENOCIDE



The CCP's campaign of genocide against the Uyghurs would not be possible without advanced technology. A complex, integrated system of physical infrastructure, data collection software, and data processing tools is what allows the CCP to erase the culture of nearly 12 million Uyghurs in a region three times the size of France.¹² The use of advanced technology to wage such an effective and destructive campaign of genocide is without precedent: the world's first example of a technogenocide.¹³ The CCP's most powerful weapon in its technogenocide against the Uyghurs is Artificial Intelligence (AI). This section will explore AI's role in facilitating the genocide, as well as the AI-powered surveillance weapon at the center of genocide: the Integrated Joint Operations Platform (IJOP).

AI WEAPONS

Artificial Intelligence refers to “computer systems capable of performing tasks that typically require human intelligence, such as reasoning, learning, perception and language understanding.”¹⁴ Traditional AI, like that used by the CCP in its genocide, is “focused on processing and analyzing data to provide predictions or insights.”¹⁵ An example would be models trained to recognize patterns and events in CCTV camera surveillance of public spaces.¹⁶ This is distinctive from Generative AI models, such as ChatGPT and DeepSeek, which produce new content in response to prompts.

Creating Artificial Intelligence models is a complex process that requires algorithms, computing power, and data.¹⁷ Researchers develop complex algorithms that allow AI models to “learn” from large sets of training data (often through a process of iterative pattern recognition called “machine learning”).¹⁸ These repeated, iterative rounds of learning/training require large amounts of computing power to process the data. Artificial Intelligence models have been essential to the scale and intensity of the Uyghur genocide by removing the constraints of human intelligence. Without AI, mass surveillance regimes are limited by the ability of human operators to analyze incoming data. AI models remove these limits by condensing and automating the data analysis process and enhancing the ability of human operators to engage in surveillance.¹⁹

AI weapons have been used throughout the entire genocide. Facial recognition software was deployed to surveil Uyghurs throughout East Turkestan around 2017, at the beginning of Uyghur mass internment.²⁰

In the period since, the CCP’s use of AI in the genocide has become increasingly sophisticated.²¹ In addition to facial recognition algorithms, predictive policing platforms and large-language models (LLMs) have also been deployed to facilitate the genocide.^{22,23} The following are further details on the types of AI weapons that have been developed and used in China against the Uyghur population.

- **Facial Recognition Models:** These models are capable of identifying individuals based on facial characteristics from video surveillance feeds. Models specializing in identifying Uyghurs, such as those designed by the Chinese companies Yitu or Huawei, have been used throughout the genocide.^{24,25} Facial recognition models trained by IBM, Amazon, and Microsoft have also been used by the CCP.²⁶
- **Predictive Policing Algorithms:** Predictive policing algorithms are at the center of the technogenocide.²⁷ These models analyze individuals’ personal data to target arrests. See IJOP case study below for more details.
- **Large-Language Models:** Trained on large bodies of language, these models are increasingly used by the CCP to surveil text and audio conversations by Uyghurs.²⁸ CCP-linked entities have also attempted to use Generative LLMs, such as OpenAI’s ChatGPT, for assistance in designing surveillance tools to use on the Uyghurs.²⁹

IJOP CASE STUDY

The Integrated Joint Operations Platform (IJOP) is a big-data, AI and predictive policing system used by the Chinese state in its repression of Uyghurs. Data is gathered on individuals through the system and then analyzed to flag Uyghurs as suspect or untrustworthy, after which such individuals are sent to detention centers.³⁰ The IJOP system has been in place at least since August 2016.³¹ Kashgar Prefecture was one of the first places the system was implemented.³² The IJOP gets information from various “sources” or “sensors.”³³ Many of these are CCTV cameras, some of which have facial recognition and infrared “night-vision” capabilities and are placed in “locations police consider sensitive, [including] entertainment venues, supermarkets, schools, and homes of religious figures.”³⁴ Another sizable portion of the IJOP sensors are so-called “wifi sniffers,” which “collect the unique identifying addresses of computers, smartphones, and other networked devices.”³⁵ In addition, numerous vehicle and security checkpoints collect “information such as license plate numbers and citizen ID card numbers.”³⁶ The checkpoints both transmit information to the IJOP section and “receive, in real time, predictive warnings pushed by the IJOP” so as to “identify targets for checks and control.”³⁷

The IJOP system compiles existing information including “vehicle ownership, health, family planning, banking, and legal records,” and police are obliged to report any activities deemed “unusual” or “related to stability,” which can be as mundane as “possession of many books,” according to one interviewee.³⁸

Some of the data that enters the system is gathered in person by the police officers as well and other government officials who volunteer for in the government initiative called fanghuiju (访惠聚), an acronym for “Visit the People, Benefit the People, and Get Together the Hearts of the People.”³⁹ Fanghuiju groups make visits to Uyghur homes, sometimes as often as every day, and Uyghur residents are compelled to “provide a range of data about their family, their ‘ideological situation,’ and relationships with neighbors.”⁴⁰ In other instances, as in the case of an Urumqi-based businessman, Uyghurs are forced to fill out detailed questionnaire forms with “questions on religious practices, such as how many times the person prays every day and the name of the person’s regular mosque...whether and where the person has traveled abroad...whether the person is a Uyghur, has been flagged by the IJOP, and is ‘trustworthy’ to the authorities.”⁴¹ Information that might lead to being flagged as “untrustworthy” and subjected to further investigation can be as mundane as “donating to mosques or preaching the Quran without authorization” and as arbitrary as using more electricity or fertilizer than normal, not using the front door, “stor[ing] large amounts of food in [one’s] home,” and being “related to people who have obtained a new phone or have foreign links.”⁴² The IJOP system also tracks people’s movement by “monitoring the ‘trajectory’ and location data of their phones, ID cards, and vehicles.”⁴³

The IJOP is supplied by the Xinjiang Lianhai Cangzhi Company (新疆联海创智公司), a subsidiary of China Electronics Technology Group Corporation (CETC 中国电子科技集团公司). CETC is a state owned military contractor that was awarded in March 2016 a

contract to “build a big data program that would collate citizens’ everyday behavior and flag unusual activities to predict terrorism.”⁴⁴

Officials can access the IJOP through a mobile app, which allows them to log information, report suspicious activities, and launch investigations into individuals the IJOP flags.⁴⁵ The policing app was designed by Hebei Far East Communication System Engineering Company (HBFEC, 河北远东通信系统工程有限公司), which, at least as recently as 2019, was owned by China Electronics Technology Group Corporation (CETC), the the state-owned company also more broadly behind the IJOP system.⁴⁶

INPUTS OF TECHNOGENOCIDE: DIGITAL COMPONENTS, HARDWARE AND KNOWHOW



The technological tools that China uses to commit genocide against the Uyghurs are made up of three fundamental components: digital components, hardware, and know-how. The following three sub-sections explain how each component type supports the unprecedented scale and detail of the CCP's technogenocide.

DIGITAL COMPONENTS

“Digital components” are non-physical technological assets that enable the CCP’s genocide against the Uyghurs. This includes any intangible goods or services that are digital technology or are inherently relevant to digital technology.⁴⁷ Examples include model training data, software, Infrastructure as a Service (IaaS), Software as a Service (SaaS), digital platforms, etc. Digital components may interact with physical assets inside or outside of China and often do require physical assets to operate. Crucially, however, digital components are not specific to any particular physical asset. For example, video surveillance data training data may exist on a specific server – a form of hardware – in China. However, this data is not inherently tied to that specific server, and could conceivably exist on a different hardware device.

Cloud Computing

Cloud computing refers to “on-demand access to computing resources...over the internet with pay-per-use pricing.”⁴⁸ Users of cloud computing services rent compute time or data storage on physical servers operated by a Cloud Services Provider (CSP). As of Q2 2025, the top five CSPs by market share are all major US companies.⁴⁹ The two largest global cloud services are Amazon Web Services (AWS) with 30% market share and Microsoft Azure with 20% market share.

Chinese firms and government agencies rent compute time on Amazon Web Services, Microsoft Azure, and other cloud service providers to train and deploy surveillance-applicable models like those used in East

Turkestan. This includes video recognition and other surveillance models, as well as services to companies sanctioned for their involvement in the surveillance of Uyghurs.⁵⁰ An October 2025 investigation by the Associated Press found that AWS and Azure both directly advertise cloud storage of video surveillance data to Chinese customers.⁵¹ Both AWS and Azure also partner with companies sanctioned for conducting surveillance in East Turkestan. AWS works with sanctioned Chinese surveillance giants Dahua and Hikvision to support surveillance technologies abroad; Microsoft Azure similarly facilitates Hikvision’s surveillance technologies abroad.^{52,53} Cloud service providers – including Amazon Web Services and Microsoft Azure – provide services to Chinese customers through data centers both inside and outside of China.⁵⁴ Cloud services located inside China are highly localized, with international companies operating through local partners in compliance with Chinese regulation.⁵⁵ There is very little transparency into what customers these localized data centers are servicing.

Cloud computing services allow Chinese companies to circumvent existing restrictions on semiconductor exports to China. Chinese entities have used AWS, Microsoft Azure, and other CSPs located outside of China to access the computing power of chips blocked from exports to China per US regulation.^{56,57} It should be noted that, as of December 8, 2025, the chips these companies accessed through AWS and Microsoft Azure are no longer subject to export restrictions;⁵⁸ however, the fact remains that the cloud was used to avoid

export controls while they were in place. This problem is also not just limited to the major US-based CSPs. A November 12, 2025 investigation by the Wall Street Journal found an example of Indonesian CSP Indosat selling compute on 2,300 Blackwell Nvidia chips for use in training Chinese AI models.⁵⁹ Physical exports of the Blackwell chip series to China are still banned by the US as of December 8, 2025.⁶⁰ While the AI models trained were not directly relevant to the Uyghur genocide, this example reveals how entities in China can use the cloud to access the equivalent computing power of export-controlled GPUs.

Moreover, cloud computing services as such are not subject to export controls. The Bureau of Industry and Security (BIS) has held that it is not an export to provide computing services or data storage services over the cloud so long as the provider is not transferring export-controlled commodities, software, or technology.⁶¹ AWS' own documentation on export compliance reflects this policy: "SaaS [Software as a Service] and IaaS [Infrastructure as a Service] is not an export-controlled activity. Use of cloud hosted software is not an export-controlled activity as long as the software is not downloaded."⁶² AWS' Global Export Compliance also makes clear that any burden of export compliance falls on cloud users, not providers: "Cloud users are responsible for any export compliance requirements that would arise when storing controlled content and/or transmitting it across international borders."⁶³ A Microsoft Azure White Paper on export controls similarly emphasizes that the customer bears the burden for export control compliance.⁶⁴ This lack of specific restriction on the provision of cloud services is known as the "Cloud Computing Loophole."⁶⁵

Regulation and legislation closing the Cloud Computing Loophole has been proposed; however, no such rule is currently in effect,

and proposed rules do not target the use of cloud services in surveillance and human rights violations. The U.S. Framework for Artificial Intelligence Diffusion, issued in January 2025 under the Biden administration, sought to prevent the "unauthorized training of controlled models" in certain countries, including China, and placed restrictions on US-based CSPs to prevent training these models.⁶⁶ However, the framework made no mention of models used in surveillance or human rights violations.⁶⁷ The Bureau of Industry and Security (BIS) rescinded this framework in May 2025, leaving in place only restrictions on models with "WMD or military-intelligence"⁶⁸ applications.⁶⁹ Legislation limiting China's access to high-powered chips through cloud computing services has been proposed in Congress. This includes the bipartisan "Remote Access Security Act," which has been unsuccessfully proposed four times since September 2024.^{70,71,72,73} As with the AI Diffusion Framework, the "Remote Access Security Act" does not specifically reference the use of cloud services in facilitating human rights violations.

Tech companies have successfully lobbied to block proposed restrictions on cloud services. Unfortunately, this campaign has been successful even despite the broad, bipartisan support for legislation that closes the Cloud Computing Loophole.⁷⁴ Per the Associated Press, tech industry lobbyists have dismissed the extent of US complicity in the surveillance regime in East Turkestan; they argue that most companies are not involved in supporting the genocide and will lose valuable business to address small-scale complicity.⁷⁵

This fits with common arguments made by tech industry proponents against restricting the sale of advanced dual-use technologies to China: denial of company or industry involvement, dismissal of the scale of the problem, and defense of US tech "competitiveness" as

necessary for innovation and securing leadership over Chinese domestic alternatives.^{76,77,78} For example, lobbyists for semiconductor manufacturers made a similar series of arguments regarding export controls for advanced chips.^{79,80} However, export controls were ultimately passed, with proponents successfully arguing that chips should be seen first and foremost as relevant to national security, thus outweighing any business concerns.^{81,82} Rather than argue that all chips are used against US interest, they convinced policymakers that the export of chips created enough overall risk to justify controls.⁸³ However, it is important to note that the recent rollbacks on these restrictions have highlighted the continued sway of the argument used by the tech industry against export controls.⁸⁴

This fits with common arguments made by tech industry proponents against restricting the sale of advanced dual-use technologies to China: denial of company or industry involvement, dismissal of the scale of the problem, and defense of US tech “competitiveness” as necessary for innovation and securing leadership over Chinese domestic alternatives.^{76,77,78} For example, lobbyists for semiconductor manufacturers made a similar series of arguments regarding export controls for advanced chips.^{79,80} However, export controls were ultimately passed, with proponents successfully arguing that chips should be seen first and foremost as relevant to national security, thus outweighing any business concerns.^{81,82} Rather than argue that all chips are used against US interest, they convinced policymakers that the export of chips created enough overall risk to justify controls.⁸³ However, it is important to note that the recent rollbacks on these restrictions have highlighted the continued sway of the argument used by the tech industry against export controls.⁸⁴

Spyware

Spyware, as used in this report, refers to digital surveillance tools that enable the extraction and analysis of behavior. This category includes two closely related forms of software: (1) software-based surveillance systems that analyze social behavior, and biometric indicators, and (2) intrusive device-level spyware that directly compromises personal phones and computers to extract relevant data. As a digital component, spyware is intangible, scalable, and separable from specific hardware systems. It can be developed and maintained independently of cameras or physical infrastructure, while still feeding into centralized repression platforms. In the context of China’s repression of Uyghurs, digital surveillance tools form a critical operational layer of the technogenocide architecture. The data they extract supplies predictive policing systems, most notably IJOP—with granular inputs that enable social mapping, risk scoring, and preemptive intervention. In this way, spyware enables a shift from monitoring behavior to policing belief, association, and identity.

Software-Based Intrusive Surveillance Spyware and Western Enablement

A central subset of intrusive digital surveillance tools consists of software-based systems that analyze and classify personal behavior at scale, even when they do not directly infect individual devices. These systems include AI-powered population monitoring platforms, facial and biometric recognition software, social media scraping tools, and emotion-analysis technologies. Together, they enable authorities to infer identity, ideology, trustworthiness, and social affiliation from digital traces.

Several Chinese firms operating in this space have materially enabled the Western technology ecosystems, particularly U.S. based technology investors. Baidu, one of China’s largest technology companies, has provided

mapping and data-processing logic used within the IJOP system and has developed broader AI surveillance capabilities deployed by Chinese security services. Despite their implication in the repression system, Baidu has received substantial investment from U.S. asset managers and financial institutions, including Jane Street, Primecap, and Dodge & Cox. These investments have helped sustain a company whose technologies underpin population-monitoring systems central to repression in East Turkestan.⁸⁵

Other firms have received more direct forms of Western technical support. DataGrand, which specializes in social media monitoring and speech analysis, has been supported through Microsoft's startup programs in China.⁸⁶ DeepGlint, a facial recognition company that built a joint laboratory with the Urumqi Public Security Bureau and counts the Urumqi police as its top customer, has received funding from Sequoia Capital and support through Microsoft's incubator programs.⁸⁷ Hydata, which served as a technical support unit for Xinjiang police and reportedly provided services to approximately one-third of China's police market, also partnered with Microsoft to establish a joint incubator in Hangzhou, receiving office space, mentorship, and Azure cloud credits.⁸⁸

These relationships do not require Western firms to design repression tools themselves. Instead, they lower barriers to entry and scale for companies developing intrusive surveillance software, embedding those capabilities within global technology and financial ecosystems. As with cloud computing services, this form of enablement often occurs through legally permissible commercial relationships that are not evaluated through a human-rights lens. The result is that software systems capable of analyzing intimate digital behavior, and feeding that analysis into predictive policing architectures, despite their documented use in mass repression.

Device-Level Spyware and Transnational Intrusion

In addition to software-based surveillance systems that analyze digital behavior at scale, China's repression architecture relies on device-level spyware that directly compromises personal phones and computers. These tools enable covert or compelled access to communications, files, microphones, location data, and application activity, allowing authorities to extract highly granular information from individuals in real time. Device-level spyware represents the most intrusive form of digital surveillance, as it collapses the distinction between public behavior and private life by transforming personal devices into instruments of state monitoring.

Within Xinjiang, such tools are frequently deployed through coercive mechanisms, including forced device inspections and mandated software installation.⁸⁹ Outside China, similar capabilities have been used covertly against Uyghur communities abroad, journalists, and advocacy organizations, extending the reach of repression beyond China's borders.⁹⁰ Surveillance against the diaspora operates through deception and social engineering, reflecting a broader pattern of transnational repression. Investigations have identified multiple state-linked spyware families used in these campaigns, including BadBazaar and Moonshine, which have targeted Uyghur NGOs, journalists, and community members.⁹¹ These tools have been distributed through fake Quran applications, counterfeit messaging tools, and links shared within Uyghur-language Telegram channels.⁹² Once installed, the malware enables persistent access to sensitive device data, allowing operators to map networks, identify organizers, and monitor political and religious expression. Reports have linked these campaigns to Chinese state-aligned entities, including firms associated with UPSEC and

related contractors.⁹³

Although these spyware tools are developed by Chinese-linked actors, their deployment often depends on Western digital infrastructure. Social engineering campaigns rely on global app distribution ecosystems, hosting services, and communication platforms that are largely operated by U.S. or allied companies. In this way, Western platforms function as unwitting intermediaries, enabling the dissemination and operation of spyware even when the underlying intent is political repression.

Device-level spyware is particularly significant to China's repression architecture because it supplies a form of data that cannot be reliably obtained through cameras, checkpoints, or ambient surveillance alone. By extracting private communications and social connections directly from devices, spyware enables authorities to infer ideology, religious practice, and trustworthiness with far greater precision. These data streams feed directly into predictive policing systems such as the IJOP, strengthening their ability to flag individuals based not on criminal acts, but on inferred beliefs, associations, or potential future behavior.⁹⁴ In this sense, device-level spyware amplifies the preemptive logic of repression, allowing the state to intervene before dissent becomes visible in public space.

As with other digital components, the governance of device-level spyware remains poorly aligned with human rights risk. Existing regulatory frameworks tend to focus on national security threats to U.S. users or on narrow definitions of cybercrime, rather than on the use of spyware in mass repression abroad. As a result, spyware tools (and the Western infrastructure that enables their deployment) continue to operate within legal gray zones, despite their central role in sustaining China's technogenocide against the Uyghurs.

HARDWARE

Hardware refers to the physical technological infrastructure that enables China's system of mass surveillance and repression, including microchips, servers, data centers, cameras, drones, and other surveillance equipment. These physical components provide the computational power, data collection capacity, and operational backbone necessary for artificial intelligence-driven monitoring, predictive policing, and large-scale population control.

The Role of Microchips

One of the key types of U.S.-based hardware that is contributing to China's technogenocide of the Uyghurs in East Turkestan are American microchips. Microchips are tiny integrated circuits built on silicon wafers that contain complex networks of integrated electrical circuits that work to perform tasks such as processing data, performing computations, and storing information.⁹⁵ In the 21st century, microchips now spearhead the function of nearly every technological device, from smartphones to cars and refrigerators. U.S. microchips have powered three key components of Xinjiang's surveillance apparatus: the IJOP, the Urumqi Cloud Computing Center, and PRC AI-powered surveillance drones.

Integrated Joint Operations Platform

As previously mentioned, the IJOP is an AI-powered predictive policing system in East Turkestan that flags certain individuals as "suspicious" and need to be detained based on key biometric information, personal data, and identifying surveillance footage funneled in

from surveillance cameras, data doors, and police checkpoints around East Turkestan.⁹⁶ The IJOP currently uses Intel's Xeon CPU processors⁹⁷ and NVIDIA's Tesla T4 GPU⁹⁸ to power its ability to comb through over hundreds of hours of surveillance camera footage and input data in one day. At the height of the IJOP's operations, it once flagged over 2400 individuals as "suspicious" in one week, leading to the majority of the flagged individuals being detained.⁹⁹

Urumqi Cloud Computing Center

Another aspect of the Xinjiang surveillance state that U.S. microchips support is the Urumqi Cloud Computing Center (UCCC). Powered by Xinjiang Sugon Cloud Computing Co., the UCCC is a large-scale complex of computers, 2019 ranked as the 135th fastest set of computers in the world in 2019, designed to host high-performance servers and serve as the region's computational power center.¹⁰⁰ Powered also by NVIDIA and Intel microchips, the UCCC is said to be able to "connect to 10,000 video feeds and analyze 1,000 simultaneously, using artificial intelligence."¹⁰¹ Built right next to six prisons--or re-education centers--the UCCC not only supports the supercomputing power of the IJOP, but was originally said by local law enforcement officers to have been constructed to support the PRC's "Sharp Eyes" surveillance project, a nationwide effort to collect "blood samples from men and boys from across the country to build a genetic map of its roughly 700 million males"—one of the PRC's most invasive surveillance and biometric hacking projects yet.¹⁰²

As of July 8, 2025, Bloomberg News reported that the PRC has begun construction plans for a brand new constellation of data centers in East Turkestan that the PRC aims to arm with over 115,000 Nvidia chips.¹⁰³ The creation of a data centers this size not only poses a notable threat to the U.S.’s technological lead, but also is a foreboding premonition of the increasing surveillance that Uyghurs in Xinjiang will face in the coming years. The aim of acquiring 115,000 NVIDIA chips is clearly spelled out in CCP’s official planning documents, but at the time this document was drafted, the export of such NVIDIA chips was strictly banned by the U.S. government, indicating the CCP’s confidence in evading U.S. restrictions.

AI-Powered Drones

A third key way that U.S. microchips perpetuate Xinjiang’s surveillance system of Uyghurs is through powering its AI-powered facial recognition drones that surveil neighborhoods in East Turkestan. More specifically, NVIDIA posted on its WeChat account in 2022 that its H20 chips—designed specifically for the Chinese market to circumvent U.S. export restrictions¹⁰⁴—were being used to train the AI-patrol drones of Chinese companies Watrix and GEOAI.¹⁰⁵ These drones have been utilized by the PRC to patrol East Turkestan’s border regions, tracking and responding to individuals attempting to escape the region.¹⁰⁶ As of 2022, the PRC also began using these drones to surveil Yarkant, a Southwestern region in East Turkestan, for potential “terrorists.”¹⁰⁷ Within one week of the drones’ arrival to Yarkant, they had already helped police arrest over 215 “suspicious” individuals, with 18 others surrendering to authorities.¹⁰⁸

NVIDIA Case Study

NVIDIA, a key player in supplying microchips powering Xinjiang’s IJOP, UCCC, and AI surveillance drones, was first barred from exporting its most advanced chips to China

following the U.S. Commerce Department’s Bureau of Industry and Security-imposed updates on export controls to China.

Specifically, the controls “impose restrictive export controls on certain advanced computing semiconductor chips, transactions for supercomputer end-uses, and transactions involving certain entities on the Entity List” and “imposes new controls on certain semiconductor manufacturing items and on transactions for certain integrated circuit (IC) end uses.”¹⁰⁹ Specifically in the case of NVIDIA, the initial 2022 export controls meant that the company could no longer export its most advanced chips—the A100 and H100 GPUS— to China and Hong Kong, unless granted a special license from the U.S. federal government. Functionally, this meant that NVIDIA was banned indefinitely from selling those chips to China and Hong Kong.¹¹⁰

A year later in October 2023, the U.S. federal government, pressured by national security concerns, further tightened export restrictions, effectively banning NVIDIA to sell even its lower-end AI chips like its A800 and H800 GPUs. In April 2025, the U.S. government further ramped up its export controls, banning NVIDIA from also exporting its H20 chips, notably crucial to the powering of Xinjiang’s AI surveillance drones. However, this deal lasted for only a few months.

The U.S. federal government’s harsh crackdown on microchip exports was met with intensive lobbying from semiconductor companies across the board, especially Jensen Huang, CEO of NVIDIA. By July of 2025, it was revealed that NVIDIA had struck a deal with the U.S. government that allowed it to resume exports of its H20 chips in exchange for a 15% cut of their revenues from chip sales in Hong Kong and China.¹¹¹

As reflected in the NVIDIA case study, the U.S. federal government has attempted numerous pieces of legislation to curb U.S. microchip export to China. Most notably, in 2019, the Trump administration made significant Chinese company additions to the The Entity List, a blacklist of companies barred from buying American technology without first receiving a case-by-case waiver from the U.S. government.¹¹²

Despite legislative attempts like The Entity List and further export tweaks by the Department of Commerce, the ongoing NVIDIA case study is a key example of how U.S. attempts to regulate Western technological complicity in the Xinjiang genocide fall short in the face of circumvention tactics like under the table financial deals or bribes. Further failings in federal regulation stem auditing failures to catch fake “shell company” buyers and a lack of consistent enforcement from U.S. prosecutors.

The Chinese Chip Counterfactual

When discussing the role that American chips play in the Xinjiang surveillance state, it is important to interrogate the counterfactual. Namely, if the U.S. halted all microchip exports to China, would Chinese microchips be advanced enough to keep Xinjiang’s technogenocidal surveillance system up and running? Considering the fact that China’s lead semiconductor corporation Semiconductor Manufacturing International Corporation (SMIC) is a “pure play” foundry, meaning that it only manufactures chips and doesn’t design them, the innovative velocity of Chinese chips still lag behind that of U.S. based microchips.¹¹³ Furthermore, most recent 2023 estimates have projected that SMIC’s most advanced 7nm microchips are still “roughly four to five years behind” the most advanced chips of U.S. collaborator chip companies like South Korea’s Samsung and Taiwan’s TSMC.¹¹⁴ This analysis proves that Western

chips are a crucial component of the Xinjiang surveillance system — a crucial component that could significantly delay and disrupt the PRC’s genocidal campaign against the Uyghurs if strategically withheld from China.

The Role of Cameras

While the IJOP system integrates data from multiple sources, CCTV cameras serve as its primary input mechanism.¹¹⁵ More than 1,400 Chinese companies provide facial, voice, and gait recognition capabilities to Xinjiang’s surveillance infrastructure. Total public security spending almost doubled in Xinjiang in 2017 to nearly \$10 billion, with most funding directed toward what surveillance companies call “Safe City” projects—systems that, under the guise of public safety, enable states to monitor populations without privacy protections and maintain 24/7 vigilance over individual movements.¹¹⁶

Implicated Companies

Hikvision and Dahua are the world’s largest surveillance camera manufacturers and the primary perpetrators of the PRC’s surveillance state in Xinjiang.¹¹⁷ Their AI-powered camera systems and backend platforms are designed to automatically detect and track Uyghur individuals. Using facial recognition models trained to identify ethnic minorities, these systems trigger real-time alerts when Uyghurs are detected. This technology is embedded across mosque monitoring networks, detention and concentration camp surveillance infrastructure, and centralized data platforms that aggregate vast amounts of facial data to enable systematic persecution.¹¹⁸

Ethnic Profiling Technology

Both companies have explicitly developed and marketed ethnic profiling technology. Hikvision’s DS-2CD7A2XYZ-JM/RX AI camera was explicitly marketed as capable of analyzing “ethnicity (such as Uyghurs, Han)” with claimed accuracy rates of no less than

90%, live API guides listed video analytics for ethnic minority detection, but evidence was deleted after media inquiries into Hikvision. In October 2022, IPVM found Dahua listed four camera models on its website with facial recognition attributes, including race, skin color, and “Xinjiang/Tibet” which Dahua then later claimed was “outdated.”¹¹⁹

Automated Alert Systems

The automated alert systems immediately notify authorities when Uyghur faces are detected by surveillance cameras.¹²⁰ Dahua deploys “real-time Uyghur warnings” integrated into facial recognition systems, targeting “non-local Uyghurs,” those who don’t already live within a police jurisdiction. March 2020 Dahua document describes subcategories tracked by “Heart of City,” including “Uyghurs with hidden terrorist inclinations”—a designation triggered by mundane characteristics such as having a full beard, owning knives, or attending mosques.¹²¹ Hikvision’s systems function similarly: the Xinjiang Police Files revealed cameras flagging Uyghurs for traveling abroad and marking those with overseas ties for “immediate arrest” under the IJOP “anti-terrorism” platform.¹²²

Data Processing

These companies then aggregate this massive amount of facial recognition data into their data command centers, IJOP, that uses US technology to store, manage and process data. Dahua’s “Sharp Eyes”, an extension of their safe cities projects integrate surveillance data into what the company calls “big data” systems that can track individuals across multiple locations and time periods. The platforms process facial recognition data to identify patterns of behavior, movement, and association that authorities use to target individuals for detention. The systems maintain comprehensive records that enable retroactive analysis of where individuals have been and who they have encountered.¹²³

Flagging for Detention

Camera surveillance data feeds into a broader system of categorization and control. A database obtained by The Intercept reveals evidence of a deeply invasive police state concerned with people’s thoughts and enthusiasms, entering their homes, interfering with their daily movements, and even seeking out crimes in activities perfectly legal at the time they were undertaken. Authorities in the region direct investigations and other police work using an approach one expert, after examining portions of the database, described as “hyperpolicing,” cracking down on any aberrant behavior. The tactics used are all-encompassing, involving civilian brigades, home visits, and frequent checkpoints, targeting people based on perceived danger. The police categorize people in three categories—purported extremists and terrorists of three levels of severity, ranked according to the government’s perception of their mindset and potential to cause harm. Relatives of detainees and former detainees are also labeled, ranked, and tracked by police. Another system categorizes people as trustworthy, normal, or untrustworthy.¹²⁴

US Company Involvement

Export of US technology to China

Hikvision and Dahua are Chinese companies backed by massive CCP funding, yet their surveillance infrastructure depends on American technology. While most manufacturing occurs in China beyond US regulatory reach, these companies rely on critical US components: Intel provides CPU microprocessors for their cameras, NVIDIA supplies GPUs for analytics processing, and Seagate and Western Digital provide storage equipment. This technological dependence creates an opportunity for US regulation to disrupt the surveillance apparatus enabling repression in Xinjiang.

Ambarella

Hikvision and Dahua mainly source video processing chips (SoCs) from HiSilicon— a Chinese fabless semiconductor company (meaning it designs chips but contracts out manufacturing) based in Shenzhen owned by Huawei—and formerly from Ambarella, a US company. Prior to 2019, Ambarella provided SoCs to Hikvision, but the company has since completely exited the Chinese enterprise security market. As of December 2025, Ambarella confirmed "0 revenue from the China market for our enterprise security," eliminating what was previously over 25% of its total revenue.¹²⁵

NVIDIA

Hikvision uses NVIDIA GPUs for its HEOP 2.0 open platform, which requires NVIDIA graphics cards with 8GB memory or above to run third-party applications and video analytics on Hikvision devices.¹²⁶ Hikvision's intelligent servers are powered by NVIDIA Tesla P4 GPU accelerators, and the company combines cameras with NVIDIA Jetson platforms at the edge for AI processing. (IPVM) Dahua similarly depends on NVIDIA technology, with its Deep Sense server using NVIDIA Tesla P4 GPUs.¹²⁷ Both companies leverage NVIDIA's end-to-end AI and deep learning platforms for video stream processing and advanced analytics capabilities. Despite both companies being on the Entity List of Bans, NVIDIA products continue to power these cameras, with technicians aiding in resolving usage bugs.

Intel

Additionally, Intel processors are fundamental to both companies' product architectures. Hikvision's Network Video Recording (NVRs) and open-source smart cameras use Intel processors, while their AI cameras incorporate Intel Movidius Myriad 2 VPUs for edge processing. Dahua NVRs similarly use Intel processors, and their people-counting cameras

incorporate Intel Movidius chips for analytics processing.¹²⁸

Surveillance Hard Drives

American companies Western Digital and Seagate supply the overwhelming majority of surveillance hard drives that enable Xinjiang police to store IJOP data. This supply of hard drives that enable the surveillance infrastructure used to monitor and oppress Uyghurs and other minorities in Xinjiang.¹²⁹ The companies make over \$1 billion annually in China from these sales, with Seagate making about 12% of its total sales in China while Western Digital makes about 20%.¹³⁰

Non-Compliance

Both companies have demonstrated concerning patterns regarding compliance with export controls. Seagate was fined \$300 million by the US government for selling over 7.4 million hard drives to Huawei despite sanctions between 2020-2021, continuing sales even after competitors stopped and entering into a three-year strategic cooperation agreement with the sanctioned company.¹³¹ Western Digital and Seagate only stopped selling to Dahua after 2022 semiconductor export controls, not the original 2019 Entity List designation for human rights violations. This pattern suggests that companies prioritize compliance with economically motivated restrictions over those designed to prevent human rights abuses, creating a hierarchy of sanctions enforcement that undermines the effectiveness of measures intended to prevent American technology from enabling the oppression of ethnic minorities.¹³²

Exploiting Enforcement Gaps

American hardware and technology continues to reach Hikvision, Dahua, and their subsidiaries through multiple channels that exploit enforcement gaps.¹³³ In October 2019, the U.S. government sanctioned both Dahua and Hikvision by adding them to the Commerce Department's Entity List

specifically for human rights violations and abuses against Uyghurs and other minorities in Xinjiang. Even after being placed on the entity list, IPVM found multiple examples of Hikvision products continuing to be powered by Nvidia technology as recently as March 2023.¹³⁴ Nvidia, Intel, Seagate, and Western Digital have historically provided critical components that power surveillance systems used to oppress Uyghurs, and these companies continue accessing restricted technology through stockpiled inventory, distributors, secondary markets, and complex supply chains that regulators struggle to monitor effectively. Despite U.S. export rules around advanced chips, China bought \$20.7 billion worth of chipmaking equipment from U.S. companies in 2024 to bolster its homegrown industry, a report from a congressional committee report from December 2025 warned.¹³⁵

Import of Chinese technology to the US

While Entity List companies are barred from purchasing American products, US law does not restrict American companies from buying from sanctioned entities. Four cases demonstrate how US firms continue to financially support, and derive products from, Hikvision and Dahua despite their role in the Uyghur genocide.

AGM-Hikvision Connection

Documents reveal close ties between AGM, an American company, and Hikmicro, a Hikvision subsidiary. Hikvision employees are listed as authors on AGM product manuals, and shipping records show both direct shipments from Hikvision to AGM and shipments routed through Vietnam to obscure their Chinese origin.¹³⁶

Alat and Saudi

A US-Saudi AI partnership faces serious risks from Dahua's \$200 million joint venture with Alat, an entity funded by Saudi Arabia's Public Investment Fund.¹³⁷ Through Alat AIVisio

Technology Co. Ltd., Dahua is establishing an automated manufacturing hub for surveillance products in Saudi Arabia, creating pathways for both technology espionage and the import of Dahua-manufactured surveillance equipment into the US market. While Alat's CEO stated that "the requests have been to keep manufacturing and supply chains completely separate," he acknowledged that if "partnerships with China would become a problem for the US, we will divest", underscoring the clear conflict of interest.¹³⁸

Amazon and Honeywell

In 2020, Amazon purchased 1,500 cameras from Dahua in a deal valued at nearly \$10 million. At least 500 of those cameras remain in operation at Amazon facilities in the United States today.¹³⁹

Honeywell's Supply Chain Laundering

Honeywell stopped purchasing new cameras from Dahua in April 2022 following the FCC ban but continued sourcing from Sunell, another Chinese manufacturer. Trade records reveal thousands of products labeled "HONEYWELL" cameras marked "100% NEW" being shipped from Sunell factories in China to facilities in Vietnam before export to the United States—a clear attempt to obscure manufacturing origin through transshipment.¹⁴⁰ Additionally, three-quarters of Honeywell's product lines—including the Performance Series and equiP lines—use components from discontinued Dahua products still in inventory, making them non-compliant with the National Defense Authorization Act (NDAA).

Circumventing US Export Controls

Despite Entity List designations and export restrictions, Hikvision, Dahua, and other sanctioned Chinese surveillance companies continue accessing US technology through multiple evasion tactics:

- Distributor Networks and Secondary Market Access
 - US companies lack effective mechanisms to monitor end users of their products after initial sale
 - NVIDIA, for example, acknowledged that while it and its distributors adhere to US export rules, the company "cannot control every future use or sale of its products"
 - Before recent export ban rollbacks, NVIDIA GPUs remained widely available to Chinese entities through distributors and e-commerce platforms
- Supply Chain Circumvention
 - Chinese surveillance companies route purchases through obscure intermediary companies to disguise end users
 - Engineers physically transport AI training data across borders to access restricted computing power. In one case, four engineers traveled to Malaysia with 80 terabytes of data on hard drives to process on NVIDIA-equipped servers rented through a Malaysian entity.¹⁴¹
 - Data centers are booming across Southeast Asia, driven partly by demand from Chinese companies unable to develop AI domestically due to US restrictions, creating access channels difficult for US authorities to monitor

The Regulatory Challenge

Chinese tech firms constantly emerge and evolve, turning regulation into a perpetual game of whack-a-mole where authorities cannot identify and sanction offenders fast enough. China's military-civil fusion strategy further complicates enforcement: because many ostensibly civilian companies support the state's surveillance apparatus, distinguishing between legitimate commercial activity and complicity in atrocities becomes nearly impossible.

KNOWHOW

Joint Ventures and Forced Technology Transfer

Joint ventures are typically 30-50 year agreements between foreign firms seeking to establish a foothold in Chinese industry, and Chinese firms seeking foreign direct investment and access to foreign intellectual property (IP). Both parties share profit, capital, and technical expertise. In practice, however, this structure gives Chinese industry access to knowhow that significantly advances domestic capabilities, eventually rendering the foreign partner obsolete in the Chinese market once the knowhow has spread through Chinese industry.¹⁴² Despite this predictable outcome, the immediate gains from accessing China's massive market are attractive enough that foreign firms accept the long-term cost of IP transfer.

Joint ventures are mandated when foreign firms seek access to the Chinese market in sensitive industries, as defined by China's Negative List for Market Access.¹⁴³ The 2025 update eased restrictions in telecommunications, software, and IT services—ostensibly reducing forced IP transfer, but potentially enabling greater knowhow diffusion to problematic actors simply through increased market access and collaboration.¹⁴⁴

Cloud computing remains a restricted industry requiring joint ventures.¹⁴⁵ Microsoft, for example, must partner with the Chinese company 21 Vianet, which operates Microsoft Azure cloud computing data centers throughout China. Microsoft provides technical documentation and backend architecture guidance to enable these

operations.¹⁴⁶ Similarly, Amazon Web Services (AWS) operates eight known data centers in China through local partners: Beijing Sinnet Technology Co. runs the Beijing region centers, while Ningxia Western Cloud Data Technology Co. operates those in Ningxia.¹⁴⁷

These partnerships raise human rights concerns. China depends on cloud computing to train AI surveillance systems targeting ethnic minorities like Uyghurs in East Turkestan, making Microsoft's and AWS's presence in the Chinese cloud computing industry direct enablers of repression.

Tech Espionage

Tech espionage allows China to accelerate domestic technological advancement through infiltration of US corporate, military, and educational research environments. By stealing IP and technical knowhow, China undermines individual firms and institutions while forcing them to bear the costs of enhanced cybersecurity defenses. This espionage takes two primary forms: state-sponsored cyber operations and insider threats. The sophistication and scale of these operations present a rapidly escalating challenge requiring coordinated US policy responses.

Cyber Espionage

State-sponsored hacker groups present the largest threat to the security of U.S. tech knowhow. Numerous reports by both U.S. government and independent observers note a sharp rise in cyber intrusions targeting American companies, research institutions, infrastructure operators, and government

networks in recent years.¹⁴⁸ The Center for Strategic & International Studies identified at least 224 incidents of Chinese espionage targeting U.S. entities between 2000 and 2022, and at least 104 major incidents of cyber espionage in particular between 2003 and 2022.¹⁴⁹

Chinese hackers fall into three categories: members of People's Liberation Army (PLA) units specialized in cyber warfare, specialists from the Ministry of State Security (MSS) or Ministry of Public Security (MPS), or non-governmental groups operating as de facto MSS affiliates. As the MSS has consolidated control over China's cyber espionage activities, its use of private contractors to conduct hacking operations has increased substantially.¹⁵⁰

A February 2024 leak to GitHub exposed the operations of Anxun Information Technology Co., Ltd. ("I-Soon"), a cyber operations company that processes breached data under contract for the MSS, MPS, PLA, and numerous provincial security bureaus.¹⁵¹ The leak revealed how Chinese government entities conduct competitive bidding for hacking contracts among private firms. Marketing materials in the leak showed I-Soon advertising its experience with "terrorism-related" targets and promoting its capabilities for "counterterrorism" contract work in East Turkestan. The leak also connected I-Soon to three state-sponsored advanced persistent threat (APT) groups—hacker networks that pose national security threats to the United States: "RedAlpha," "RedHotel," and "POISON CARP," each believed to operate as an I-Soon subgroup.¹⁵² Evidence suggests many more APT groups operate through similar private contractor arrangements, including APT41—one of China's most prolific hacking operations—which has been linked to Chengdu 404 Network Technology, another MSS contractor.¹⁵³

These hacking operations target cutting-edge U.S. technologies essential to surveillance infrastructure: AI models, chip designs, quantum technology, and cloud computing systems. They also steal data from American citizens and organizations to train more accurate generative and predictive large language models (LLMs). This stolen knowhow directly enables the AI-powered surveillance systems, facial recognition algorithms, and predictive policing platforms used to oppress Uyghurs in East Turkestan.¹⁵⁴

Insider Espionage

China systematically pursues human intelligence operations targeting academic labs, research centers, and technology companies. Universities conducting advanced scientific research are particularly vulnerable, with Chinese students sometimes acting under direction from PRC institutions.

The China Scholarship Council (CSC), the PRC's primary government scholarship body, funds an estimated 15% of Chinese students at American universities.¹⁵⁵ CSC recipients must regularly submit "situation reports" to Chinese diplomatic missions about their research and are typically required to return to China for at least two years after degree completion, a requirement that has more than doubled since 2012.¹⁵⁶ While many students implicated in espionage claim coercion by state actors, other cases involve CCP-affiliated agents posing as students. One publicized example is "Charles Chen," an alias used by a suspected MSS agent who posed as a Stanford student while repeatedly attempting to recruit a fellow student studying sensitive China-related research, pressuring her to visit Beijing.¹⁵⁷

Universities like Stanford—heavily engaged in STEM research, especially in the field of AI—are particularly vulnerable to espionage and to having their research applied in China's surveillance and military systems.

China also pursues insider espionage activity at tech companies. PRC intelligence agencies recruit insiders to steal proprietary data, trade secrets, and any insider information on research and development. Insider spies use hidden data transfers, encrypted communication channels, and code laundering.¹⁵⁸ In February of 2025, Linwei Ding, a software engineer at Google was charged with stealing trade secrets related to AI as well as Google's Tensor Processing Unit (TPU) and GPU systems, and distributing the information to two Chinese companies engaged in AI: Beijing Rongshu Lianzhi Technology Co., Ltd. ("Rongshu") and his own company Shanghai Zhisuan Technology Co., Ltd. ("Zhisuan").¹⁵⁹ The theft of Google's TPU and GPU architecture, critical components for training large AI models, directly accelerates China's development of surveillance technologies like those deployed against Uyghurs.

Talent Recruitment

Since the turn of the century, China has sought to move toward a highly skilled economy through the development of domestic talent and recruitment of foreign talent. A significant component of this talent drive has been attracting researchers in fields like applied physics, computer science, and electrical engineering, which are particularly relevant for the development of China's AI-based police surveillance technology used to oppress Uyghurs in East Turkestan. Since 2008, the CCP has made significant efforts to compel citizens studying abroad to return to China and apply their skills domestically, beginning with the Thousand Talents Plan (which since 2019 has been rebranded as the National High-End Foreign Experts Recruitment Plan).

National High-End Foreign Experts Recruitment Plan (Formerly the Thousand Talents Plan)

The Thousand Talents Plan was launched in

2008 and expanded in 2011 with five main branches of focus: Innovation(Full-time), Innovation(Short-term), Entrepreneur/Startup, Youth Thousand Talents, and Foreign Expert Talents.¹⁶⁰ The first three branches target Chinese nationals abroad, whereas the latter two branches target foreign experts. All branches of the Thousand Talents Plan (and China's dozens of other talent programs) attempt to lure talented individuals living abroad to China with generous financial, career, and lifestyle benefits.

According to an article by Chinese science journalist Hepeng Jia in Nature in 2018, all applicants to the Thousand Talents program could expect a 1 million yuan (US\$151,000) starting bonus, and the opportunity to apply for a research fund of 3-5 million yuan.¹⁶¹ These privileges were expanded for foreign talents, with employers even obligated to give subsidies for accommodations, meals, relocation, visits home, and education costs, and employers were obligated to find jobs for foreign spouses.¹⁶² Recruits under the Youth Thousand Talents Program (YTTP) received similar benefits.

The YTTP has proven particularly effective at attracting early-career researchers. According to a report published in Science in 2023, YTTP scientists have benefited from the program's generous startup grants and China's abundant supply of STEM students compared to the relative lack of funding for early career scientists in the U.S. and E.U., allowing them to outperform their overseas counterparts in publications.¹⁶³ However, the report also found that "top-caliber" researchers are unlikely to remain in China long-term, if they accept YTT grants at all, likely due to the restrictive political landscape in the Chinese scientific community.¹⁶⁴ Still, the return of experts from U.S. universities to China has been a significant contributor to the progress of the

Chinese AI industry in particular. For example, DeepSeek has recently emerged as the Chinese answer to America's OpenAI. A Hoover Institute look at DeepSeek's research team found that 45% were partially educated outside of China, and that nearly 10% of DeepSeek's research team is currently affiliated with US institutions.¹⁶⁵

Visa Programs

In addition to its Thousand Talents recruitment programs, in 2013, the Chinese government started issuing R-visas, which target high-level or specialist foreign talent to work or study.¹⁶⁶ However, in an effort to attract STEM talent from even earlier career stages, the Chinese government announced the new K-visa on August 7, 2025. K-visas have lower entry requirements for younger STEM talents than the R-visa, with the only requirement being obtaining a Bachelor's degree.¹⁶⁷ Since the K-visa is aimed at early career professionals, it does not even require employer or host institution sponsorship.¹⁶⁸ The K-visa came into effect on October 1, 2025, at a time when the Trump administration has faced scrutiny for its restrictions of H-1B visas.¹⁶⁹ Despite the potential espionage risks presented by the admission of Chinese nationals to the United States, there is also the potential for loss in the comparative advantage of American institutions in attracting top talents from abroad. Therefore, the U.S. government should more carefully discern which talents present a potential security risk, and which talents contribute to the country's comparative advantage, lest the U.S. loses its international talent to China's recruitment programs.

University Relationships

Despite recent restrictions on joint U.S.-China research in sensitive fields, many universities and research institutions maintain close ties to Chinese counterparts. Executive orders like Proclamation 10043 and NSPM-33, along with legislation like the CHIPS and Science Act,

have strengthened controls on collaboration in semiconductors, AI, and defense technology.¹⁷⁰ However, these restrictions leave significant gaps. Universities continue operating joint institutes in China, maintain financial relationships with Chinese institutions, and host Chinese international researchers—some with state-assigned directives—in American lab groups with minimal security oversight by principal investigators.

A recent report by the private intelligence group Strider Technologies identified over 100,000 collaborations between researchers affiliated with U.S. organizations and PLA-associated research institutes ("PLA-RIs") since 2017 on STEM topics like AI, quantum computing, and anti-jamming communications.¹⁷¹ PLA-RIs include PLA research bodies, state-owned defense conglomerates, and the Chinese universities dubbed the "Seven Sons of National Defense". These "Seven Sons of National Defense" include Beihang University, Beijing Institute of Technology, Harbin Institute of Technology, Harbin Engineering University, Nanjing University of Aeronautics and Astronautics, Nanjing University of Science and Technology, and Northwestern Polytechnical University. Over 500 U.S. organizations, mostly universities and government laboratories, were identified by Strider Technologies as having participated in such collaborations. The House Select Subcommittee on the CCP claims that legislation and executive orders already in place have not yet sufficiently addressed direct research collaborations with these entities.¹⁷²

Joint Institutes

American universities often maintain direct ties to PLA-RIs through joint institutes: programs in China that carry American university branding but serve primarily Chinese students under CCP-monitored curricula. The House Select Subcommittee on the CCP has published two major reports detailing these joint

institutes and the pressure the subcommittee has exerted on universities to close them: “CCP on the Quad” in 2024 and “Joint Institutes, Divided Loyalties” in 2025.¹⁷³ In its 2025 report, the House subcommittee listed the following

universities which have yet to end their high-risk joint institutes: Duke University, University of Arizona, University of Delaware, Drake University, University of Houston, Kean University, University of Miami, New York University, University of North Alabama, Northeastern State University, Portland State University, State University of New York - Stony Brook, and Trine University.¹⁷⁴ The Chinese stakeholders in these joint institutes are often engaged in AI and semiconductor research, and with the financial and technical support of American universities, joint institutes present the optimal environment for acquiring American tech knowhow for use in China’s surveillance apparatus.

Financial Gifts

Universities have also faced scrutiny for accepting financial gifts and contracts from Chinese entities. The most prominent example is Harvard University, which between 2010 and 2025, has accepted \$560 million in gifts and contracts from entities based in China and Hong Kong—the most of any American university. While many of these entities were private donors and foundations, some were affiliated with the Chinese government.¹⁷⁵ Section 117 of the Higher Education Act requires universities to disclose certain foreign gifts and contracts to the U.S. Department of Education, and the House Select Subcommittee on the CCP has alleged that various universities, including Harvard, have failed to report their gifts in compliance with the Higher Education Act.¹⁷⁶

Research Collaborations and Open Access

The publication of research conducted in U.S. and other Western universities in AI, surveillance, and semiconductor technology has contributed to China’s technological knowledge base by being largely open-source and open to collaboration with foreign institutions, including Chinese universities and research institutes.¹⁷⁷ Chinese researchers in relevant fields who collaborate with American labs have often either had pre-existing ties to Chinese firms known to contribute to human rights abuses in East Turkestan, or go on to work at these firms later in their careers and contribute the knowhow they acquired through collaborative research.

Some notable individual examples include:

- Tang Xiao’ou and Wang Xiaogang, cofounders of SenseTime, an AI facial recognition startup known to supply equipment to officials in East Turkestan. Both studied at MIT.¹⁷⁸
- Xi Zhou, the founder of AI company CloudWalk, who partnered with his former professor Thomas S. Huang at the University of Illinois Urbana-Champaign to jumpstart CloudWalk’s AI research.¹⁷⁹ CloudWalk has been listed by the Treasury Department as one of the Chinese firms known to directly support the surveillance of Uyghurs in East Turkestan.¹⁸⁰
- Zhu Long, the cofounder of Yitu Technology, another AI surveillance company known to contribute to the genocide in East Turkestan.¹⁸¹ Zhu Long studied at MIT and UCLA, and is a technical leader for Yitu’s “Dragonfly Eye” AI facial recognition algorithm.¹⁸²
- Yitao Liao, founder of MassPhoton HK, a semiconductor technology company, who is managing the chip production line in the

Yuen Long Microelectronics Center in Hong Kong.¹⁸³ He is a former U.S. Army Research Laboratory collaborator and researcher at Boston University. According to a Jamestown report, the Chinese version of MassPhoton HK's website claimed that they have a lab at Boston University, possibly connected to Boston University's Wide Bandgap Semiconductor Laboratory, led by Theodore Moustakas.¹⁸⁴

- Pu Shiliang, the former head of research and development for Hikvision, who coauthored multiple papers with U.S. Army Research Laboratory researchers between 2018 and 2020.¹⁸⁵

In an early but consequential case that did not directly involve collaboration with Chinese researchers, Duke's Multi-Target-Multi-Camera (MTMC) Dataset, published in 2016, became a crucial training source for Uyghur tracking algorithms as surveillance activity in East Turkestan rapidly increased starting in 2017.¹⁸⁶ Despite the presumed innocence of all the researchers, this case provides an example of how lack of discretion in publishing sensitive technological knowhow for the general public to access can have dire consequences for human rights.

THE GLOBAL EXPANSION OF CHINA'S SURVEILLANCE TECHNOLOGIES



While the U.S. plays a central role in the digital components, hardware, and know-how underpinning China's repressive surveillance system in Xinjiang, this challenge extends well beyond the U.S. due to China's export of surveillance technologies. China is globalizing the surveillance blueprint developed in Xinjiang through the Digital Silk Road (DSR), announced in 2015 as part of the country's broader Belt and Road Initiative (BRI).¹⁸⁷

CHINA'S DIGITAL SILK ROAD

China is shaping modern surveillance landscape in numerous countries, focusing on technology that governs all aspects of society. Aid from China's DSR spans a country's "telecommunication networks, artificial intelligence capabilities, cloud computing, e-commerce and mobile payment systems, surveillance technology, [and] smart cities," effectively integrating recipient countries into China's technological ecosystem. This expansive reach is dangerous, as it not only strengthens China's technological dominance but also promotes a model of "state-led capitalism and political illiberalism" enabled by digital technology.¹⁸⁸ To understand the ongoing global threat posed by China exporting surveillance technologies and its techno-authoritarian model, it is necessary to understand the scale and objectives driving China's global surveillance apparatus.

Safe Cities

Safe cities are a primary example of China exporting the domestic surveillance blueprint used to repress Uyghurs and other Turkic minorities in Xinjiang on a global scale. The concept is built upon smart cities, which utilize sensors collecting real-time information from thousands of interconnected devices to manage municipal issues like traffic congestion and sustainable energy.¹⁸⁹ However, public safety, which is achieved through daily surveillance and policing, accelerated the shift from "smart cities" to "safe cities." Under the guise of public safety and crime prevention, safe cities deploy surveillance technologies including tracking devices and video cameras with facial recognition tools to continuously monitor populations and enable predictive policing.¹⁹⁰

The core technologies used in safe cities to conduct mass surveillance are tracking devices

and cameras that leverage biometric data. In Zimbabwe, the government agreed to send biometric data on millions of Zimbabweans to the Chinese company Cloudwalk Technology "to assist in the development of facial recognition algorithms that work with different ethnicities."¹⁹¹ This mirrors evidence involving Chinese companies Huawei and Megvii that were criticized for utilizing Uyghur biometric data for predictive policing. Biometric data is weaponized to develop facial recognition algorithms and fed into databases run by public security bureaus to detect "suspicious" individuals based on ethnic features.¹⁹²

Fifth-generation (5G) telecommunication networks are another key component enabling and scaling Chinese surveillance technology. Chinese 5G technology is the backbone of smart cities, with individual private companies facilitating its export.¹⁹³ Chinese 5G "deploys Fifth-generation (5G) telecommunication networks are another key component enabling and scaling Chinese surveillance technology. Chinese 5G technology is the backbone of smart cities, with individual private companies facilitating its export. Chinese 5G "deploys vast networks of surveillance cameras and facial recognition software" at rapid scale, reinforcing mass surveillance technologies that mirror Xinjiang's repressive system.¹⁹⁴

Where China Exports Its Surveillance Technologies

China prioritizes selling its surveillance technology to developing countries in need of expanding their digital infrastructure. There is strong demand for inexpensive technology to expand wireless phone networks and broaden internet coverage in Africa, the Middle East, parts of Eastern Europe, Latin America, and Southeast Asia.¹⁹⁵ This demand is driven by the

world's infrastructure financing gap estimated to reach \$15 trillion by 2040, positioning DSR investments as attractive opportunities in an era of rapid technological transformation.¹⁹⁶

The African continent is at the center of adopting Chinese technology through strategic partnerships developed under the DSR. In 2020, 41 out of 54 African countries officially joined BRI, and 47 engaged with China's digital infrastructure.¹⁹⁷ In late 2024, the Center for Strategic & International Studies published a report detailing nine African countries actively using safe city surveillance technology.¹⁹⁸ Furthermore, Huawei built 70% of Africa's 4G network and will facilitate the expansion of the continent's 5G network, establishing a digital ecosystem dependent on China.¹⁹⁹ In Africa and beyond, nondemocratic governments are acquiring Chinese surveillance technologies, enabling China to expand its regional influence.

Why China's Surveillance Exports Threaten U.S. Interests

China has strategically leveraged demand in developing countries for surveillance technologies not primarily for profit, but to advance its authoritarian agenda and establish dominance in the global tech order. Through the DSR, China equips vulnerable nations with digital state infrastructure capable of repression. When governments use technology for illiberal governance, populations endure surveillance, censorship, propaganda, and political repression.²⁰⁰ Chinese technicians from Huawei have directly supported African governments in spying on political opponents by intercepting communications and using cell data to track their locations. China plays an active role in enabling recipient countries to use surveillance technologies against political opposition, including training them on how to monitor and censor the internet in real time.²⁰¹

The U.S. should be alarmed by China's support for illiberal regimes because it strengthens

governments that oppose U.S. interests and spreads digital repression globally. Countries that establish alliances with China by substantially adopting its surveillance technologies are a geopolitical concern. China and the U.S. are competing for technological dominance as the two largest economies in the world, with China striving to outpace the U.S. by achieving technological superiority and reducing countries' dependence on U.S. technology.²⁰² Additionally, surveillance-enhanced regimes are less responsive to public pressures and civil society, undermining U.S. principles of democracy. The global trend of democratic backsliding, now in its ninth year of net decline, illustrates the urgency of addressing China's exportation of its techno-authoritarian model.²⁰³

By building digital infrastructure across numerous countries, China is effectively laying the groundwork for long-term reliance on Chinese technology. China's surveillance exports trap countries in its digital ecosystem, making them vulnerable to security risks. Through global exports, Chinese companies are shaping technological standards that bind recipient countries to China's digital ecosystem and influence them to use surveillance technologies for repression. China "provides more financing for information and communications technology than all multilateral agencies and leading democracies combined do across [Africa]," highlighting the failures of the U.S. and its allies to address the erosion of democratic freedoms enabled by the misuse of technology.²⁰⁴

The export of Chinese surveillance technologies poses significant espionage and data security risks directly affecting U.S. national security. Safe city surveillance systems powered by 5G collect vast amounts of sensitive data about host countries, which is vulnerable to backdoors and forced transfer to China. Legal mandates, including China's National Security Law (2015), require Chinese

companies to hand data over to the government if requested.²⁰⁵ Through this legal framework, China gains exclusive access to sensitive information worldwide, enabling intelligence collection that provides strategic advantage over the U.S. and its allies.

Huawei Case Study

Huawei is the world's largest supplier of AI surveillance technology used for public security and illustrates how Chinese surveillance technologies threaten global security and human rights.²⁰⁶ Surveillance systems Huawei developed to oppress Uyghurs in Xinjiang are now being globalized, endangering human rights abroad and amplifying China's technological dominance worldwide.²⁰⁷ The company is the primary exporter of Chinese surveillance technology and is behind two-thirds of the commercially launched 5G networks outside of China. Huawei is a pioneer in the safe city technology ecosystem, which bridges "civil-commercial actors with the state for data-driven governance."²⁰⁸

Despite Huawei's denial that it would provide the Chinese government with sensitive information collected by its surveillance technology, reports have documented the firm's backdoors and hijacking risks.²⁰⁹ Huawei telecommunication gear was reported to be "far more likely than other companies' equipment to have flaws" that enable hackers to access their systems for malicious use.²¹⁰ Although Huawei claims its technology is insulated from the Chinese government, national security laws contradict this statement, and further risks stem from backdoors and system vulnerabilities that enable data exploitation. In 2019, Czech authorities identified Huawei as a potential

national security risk, with Huawei employees reported to have collected sensitive information on Czech government officials and businesspeople, sharing the data with the Chinese embassy through Huawei's central database.²¹¹ Huawei's surveillance technology has additionally resurfaced as a threat to the Uyghur community abroad. An agreement made in 2023 between the Taliban and Huawei compromises the safety of approximately 3,000 Uyghurs living in Afghanistan, many of whom fled religious persecution in China.²¹² If invasive surveillance technologies such as facial recognition cameras and smartphone monitoring software appear in the region, Uyghurs would undeniably be targeted.²¹³ The reality that Uyghurs may be subjected to the same repression beyond China's borders that mirrors ongoing abuses in Xinjiang is an illustrative warning of the human rights and global security dangers facilitated by the exportation of Chinese surveillance technologies.

The Australian Strategic Policy Institute (ASPI) Internal Cyber Policy Centre identifies 214 cases of Huawei's presence across the globe in 5G relationships and smart city-public security projects outside of China.²¹⁴ While the U.S. and Europe have successfully banned Huawei from Western surveillance systems, Huawei continues to target emerging economies.²¹⁵ The U.S. has played an essential role in advancing China's technology used to repress the Uyghurs through contributions to digital components, hardware, and know-how. Therefore, the U.S. is responsible for addressing past harm and acting in the country's national security interest to curtail the expansion of China's dystopian surveillance technologies and digital-authoritarian model.

EXISTING REGULATORY FRAMEWORK



US policymakers, at the urging of Uyghur activists and the broader public, have taken concrete policy action to address US complicity in the Uyghur genocide in the past. Before exploring recommendations on improving the current policies, it will be helpful to examine the design and weaknesses of this existing regulatory framework.

THE REGULATORY IMPERATIVE

Between 2019 and 2025, the United States government has taken significant regulatory measures to curb American complicity in the Uyghur Genocide. Three key developments have defined the overall trajectory. The first development was in 2020 when Congress passed the Uyghur Human Rights Policy Act (UHRPA), which placed sanctions on Chinese entities involved in the detention and surveillance of ethnic Uyghurs.²¹⁶ The second was in 2021, when Congress passed the Uyghur Forced Labor Prevention Act (UFPLA), which placed a near-total ban on imports from Xinjiang on the grounds of widespread forced labor.²¹⁷ And most recently, between 2022 and 2025, the Bureau of Industry and Security fired off a range of export controls designed to restrict China's access to advanced computing chips.²¹⁸ Between these milestones, other mechanisms were introduced as part of the U.S.'s broader China strategy. Executive Order 14032 targeted investment in the Chinese military and surveillance sectors, while the Entry List expanded to include major surveillance firms like Hikvision, Dahua, SenseTime, and Megvii.²¹⁹ Taken together, these policies marked a major reversal, one that ended decades of trade-friendly policies that were willing to look the other way when it came to China's human rights record.

Yet, as noted throughout this report, American companies continue to supply the hardware, software, and technical knowledge that powers China's surveillance ecosystem in Xinjiang. Intel Xeon processors and NVIDIA GPUs still power the IJOP's predictive policing system. Amazon and Microsoft still provide cloud

computing services to key players in China's surveillance apparatus. American universities and research institutions continue to collaborate with Chinese tech companies implicated in the genocide. This begs the question: how is this widespread continued complicity possible given the U.S.'s regulatory countermeasures?

One possible answer is political insincerity. Rather than trying to align the behavior of U.S. companies with values of human rights and democracy, perhaps the real goal of U.S.-Uyghur policy was to engineer this perception without disrupting the status quo. This cynical interpretation carries some credibility, especially in light of the aggressive lobbying campaigns mounted by tech companies to oppose restrictions.²²⁰

However, attributing failures in the current regulatory framework to political insincerity alone is problematic. Indeed, multiple indicators suggest that U.S. countermeasures toward the Uyghur genocide are founded in a sincere desire to do the right thing. Policy surrounding Uyghur human rights often receives overwhelming bipartisan support. In the case of the Uyghur Forced Labor Prevention Act, the House passed it 428 to 1, and the Senate passed it unanimously.²²¹ This broad support also applies to escalatory action. Rather than stopping at low-level performative condemnations, policymakers have proved willing to escalate economic countermeasures at real material cost. To cite one instance, Nvidia stated that the 2025 H20 chip restrictions cost them \$5.5 billion in a recent

SEC filing.²²² Given that policymakers are broadly willing to escalate beyond political theater, lack of motivation does not appear to be the main limiting factor at play. Rather, the problem in the current U.S. approach lies in how these good intentions are put into action.

More precisely, the core issue facilitating U.S. technological complicity in the Uyghur Genocide is an intent-implementation chasm. U.S. regulations are not effective at curtailing the offenses they aim to prevent. This emerges from two key failures: coverage gaps and systemic failures. In this context, coverage gaps refer to the mismatch between regulated behaviors and the behaviors actually facilitating the genocide. Conversely, systemic failures refer to the structural dynamics that undermine enforcement even where regulations theoretically apply. Fully understanding this intent-implementation chasm requires tracing how both of these failures work together to undermine the current U.S. regulatory framework.

COVERAGE PROBLEMS

The first category of policy failure is coverage gaps. These arise because U.S. regulatory tools are designed around flawed notions of how supply chains facilitate human rights abuses. It is assumed that complicity takes certain, well-defined forms: importing goods manufactured under abusive conditions, selling powerful tools to bad actors, buying equity in shady companies. There is no doubt these behaviors require regulation. However, they fail to capture the full range of mechanisms by which complicity can occur in the 21st century. The following section examines three specific mechanisms that lack sufficient regulation and allow American technology, services, and investments to slip through the cracks.

The Import Gap

When the Uyghur Forced Labor Prevention Act was passed in 2021, it represented Congress's most comprehensive effort to target documented and widespread forced labor practices in Xinjiang.²²³ This was in part because, for the first time, the burden of proof was on regional exporters. Rather than customs officials having to prove forced labor on a case-by-case basis, the UFLPA required Chinese companies to demonstrate compliance through "clear and convincing evidence."²²⁴ This presumption meant that goods from Xinjiang were denied entry into the U.S. by default under Section 307 of the Tariff Act of 1930.²²⁵ The UFLPA was broadly successful at targeting the industries implicated in forced labor practices across Xinjiang. The year after the act's introduction, exports from Xinjiang plummeted from \$201.5 million to \$23.6 million as most companies failed to prove compliance.²²⁶

Still, it's not clear to what extent the UFLPA truly disrupted forced labor practices. It may be because it's somewhat early to judge the act's full impacts. However, there is reason to suspect these import restrictions simply shifted exports to other countries.²²⁷ In other words, the practice has been redirected but not eliminated per the UFLPA's original intent.

While this suggests that U.S. import controls would benefit from a more internationally-coordinated approach, it also highlights a coverage gap: current import restrictions focus on the industries implicated in forced labor but not the technology that makes these human rights abuses possible in the first place. The UFLPA targets the factory keeping Uyghur detainees, but ignores the security camera company behind the monitoring system.

This mismatch illustrates a broader problem with the current approach to import-controls. The UFLPA asks: "Was forced labor involved in the making of this product?" However, a more comprehensive approach would not only ask whether a company used forced labor but also how material they are to forced labor practices elsewhere. When framed like this, it becomes clear that Chinese surveillance tech companies are equally if not more central to the system of forced labor in Xinjiang. This is particularly evident given the comprehensive role of technology in the genocide outlined in this report. As such, the lack of import controls on the Chinese companies producing facial recognition systems, surveillance cameras, and data collection infrastructure is a critical coverage gap. One that not only enables complicity but also undermines the intent it was built to serve.

The Cloud Computing Gap

When advanced chip and export restrictions were introduced and expanded between 2022 and 2025, it was framed as similarly game-changing restrictions on Chinese access to superior U.S. computing power. Introduced by the Bureau of Industry and Security (BIS), the first round of controls in 2022 banned exports of Nvidia's most advanced AI chips to China.²²⁸ When Nvidia developed the slightly slower A800 and H800 chips as a way to circumvent the export restrictions, the regulators followed suit and tightened the controls to cover these too.²²⁹ These controls were primarily justified on a national security basis; without these chips, it was assumed that China would have less computing capacity to train AI for military applications.²³⁰ However, these export controls also carried important implications for Uyghur rights since Xinjiang's IJOP depends on similar large-scale computing operations.

These chip controls identified a valid problem, yet the solution they offered was insufficient. The regulatory focus on physical hardware exports ignored an alternative means of accessing U.S. computing power: cloud computing services, essentially Chinese entities to rent compute time on the exact chips banned from physical export. However, beyond the immediate ineffectiveness of these restrictions, their flawed implementation goes to show that the cloud computing gap is as much a coverage problem as it is the result of a larger structural problem.

It has been generally noted that policymakers often prefer to follow an incrementalist logic when introducing regulations.²³¹ Rather than pursue an all-at-once comprehensive approach, they implement successive, marginal tweaks to existing policy in a process like the chip export restrictions and adjustments between 2022 and 2025. However, this process of blocking the most obvious pathway first and then waiting for later adjustments was precisely why these chip controls failed on both fronts. Not only did U.S. semiconductor manufacturers absorb billions in losses to Chinese companies, but Chinese surveillance entities were also able to access computing capabilities unimpeded.

SYSTEMIC FAILURES

The second category of policy failures is systemic failures. Whereas coverage gaps describe deficiencies in the current regulatory framework, systemic failures exist independent of specific legislation. These arise from problems inherent to policy creation and enforcement and, as such, are significantly harder to address when aligning intent with implementation.

The Identification Problem

The Entity List is the primary mechanism by which the United States prevents its technology from reaching actors involved in human rights abuses. Since creating the list in 1997, the Bureau of Industry and Security has been responsible for identifying companies, institutions, individuals, and government organizations that are at risk of posing a threat to national security interests.²³² Notably, human rights violations were not initially part of the criteria for Entity List designation yet were eventually included as the concept of “national security” expanded beyond its original meaning.²³³

However, identifying human rights violators using the same system to identify and national security threats is intuitively problematic. In order for an entity to credibly challenge U.S. national security, it has to be large, centralized, and organized enough to pose a material threat. By contrast, human rights abuses can be carried out by a far more diffuse set of actors who lack the visibility needed for Entity List designation. This is why sanctions targeting the Uyghur genocide are difficult to implement: the number of firms that assist China’s surveillance capabilities is vast and continuously growing. In 2023 alone, for

instance, China registered 32.73 million new businesses.²³⁴ As such, the Entity List tends to concentrate on the most high-profile offenders such as HikVision and Dahua while leaving intact the broader network of small subcontractors, data processors, equipment suppliers, and software providers, all of which sustain the Uyghur Genocide.

The International Coordination Problem

Furthermore, even when U.S. authorities do successfully identify and designate human rights abusers, unilateral controls are inherently limited. When considering the effects of semiconductor export controls, for example, it’s important to recognize that much of the supply chain is outside of U.S. jurisdiction. A single firm in the Netherlands is the sole global supplier of the extreme ultraviolet lithography machines required to manufacture semiconductors.²³⁵ Similarly, Japanese firms dominate other key components of the semiconductor manufacturing process, such as coating systems, silicon wafers, and photoresists.²³⁶ Unilaterally adopting a slate of export controls on US semiconductors would thus only affect a single step in China’s chip supply chain—one that could more easily and quickly be replaced.

While multilateral action is ideal in theory, coordinating an international economic response to China poses its own difficulties. A common line heard among government officials while conducting field research in Turkey was that their policy options were constrained by the threat of economic retaliation. This economic retaliation is disproportionately felt by smaller, trade-dependent economies such as Turkey.

RECOMMENDATIONS



The mass surveillance of Uyghurs is enabled by a global ecosystem of technology and capital. Systems such as the IJOP depend on advanced semiconductors, cloud computing, foreign investment, and international corporate partnerships. To meaningfully disrupt this architecture, CFU should pursue a coordinated advocacy strategy aimed at raising the economic, legal, and reputational costs of enabling digital repression. The following recommendations focus on leveraging existing U.S. legal authorities, shaping emerging technology governance, and mobilizing allied governments, investors, and corporations to prevent their resources from facilitating what has been widely recognized as crimes against humanity.

EXPAND EXPORT CONTROLS ON SURVEILLANCE AND DUAL-USE TECHNOLOGIES

CFU should advocate for comprehensive export controls on surveillance and dual-use technologies that enable mass repression in East Turkestan. While the United States currently restricts exports of low-technology policing equipment to Chinese security forces, high-impact technologies, such as surveillance software, cameras, biometric systems, data-integration platforms, and AI surveillance models, remain largely unrestricted. This creates a significant loophole that allows American technology to power China's genocide against the Uyghurs.

Expand Export Controls to Include Mass Surveillance Technologies

- Advocate for legislation that adds mass surveillance as explicit statutory grounds for export controls under the Export Administration Regulations (EAR). This would parallel existing export control categories such as weapons of mass destruction and military applications.
- Push for controls on specific surveillance technologies including facial recognition systems, voice recognition software, gait analysis tools, predictive policing algorithms, biometric collection devices, and data integration platforms designed for mass monitoring.
- Emphasize that treating surveillance technologies as inherently high-risk when exported to authoritarian security services is consistent with existing EAR provisions that consider end-use and end-users in export licensing decisions.

Restore and Strengthen Bans on Advanced AI Chips

- Call for restoration of comprehensive bans on advanced AI chips (including H20-class, H200-class chips, and emerging successors) that are capable of powering large-scale surveillance models.²³⁷ These chips directly enable systems such as IJOP by powering predictive policing, facial recognition, and biometric analysis.
- Advocate for stricter corporate liability regimes for chip manufacturers whose products are diverted to surveillance or repression, modeled on the liability standards applied to arms exporters. This could include mandatory end-use reporting requirements and penalties for failure to provide such reports to the government.
- Support the development of technical controls embedded in advanced chips (such as location tracking or usage monitoring) that would allow authorities to detect when chips are being used by prohibited actors.

Improve Tracking and End-Use Verification Systems

- Push for enhanced BIS reporting standards that require manufacturers and distributors to track and report sales and movements of advanced and dual use technologies, including reporting on downstream distributors and known resellers.
- Support legislation imposing stricter end-use monitoring standards on chip and surveillance technology manufacturers, modeled after existing regulations for arms dealers under the International Traffic in Arms Regulations (ITAR), requiring ongoing due diligence practice even after an initial sale.²³⁸

STRENGTHEN ENFORCEMENT FOR CONTROL VIOLATIONS

Current export controls and sanctions lack robust enforcement mechanisms. CFU should advocate for creating dedicated oversight structures that can identify violations, track technology flows, and ensure accountability for companies that enable the Uyghur genocide.

Strengthen Governmental Oversight and Investigation

- Advocate for the Congressional-Executive Commission on China (CECC) to use its existing oversight authority more robustly by conducting hearings specifically focused on U.S. technological complicity in the Uyghur genocide, calling witnesses from implicated companies and regulatory agencies.
- Push for the Department of Commerce BIS and the Securities and Exchange Commission (SEC) to conduct investigations into whether U.S. companies are complying with restrictions of:
 - BIS End-Use List²³⁹
 - OFAC Sanctions Lists²⁴⁰
 - Executive Order 14032 (Chinese Military-Industrial Complex companies)²⁴¹
- Support legislation that would require these investigations to be conducted systematically rather than in response to specific complaints for proactive enforcement.

Enhance Penalties and Enforcement

- Advocate for consistent enforcement of existing penalty structures. Current BIS regulation allows penalties of \$374,474 or twice the transaction value, whichever is greater, per violations of the Export Administration Regulations.²⁴² However, actual penalties often fall far short of this maximum, creating inadequate deterrence.
- Push for mandatory minimum penalties that represent a substantial percentage of transaction value to ensure violations are economically disadvantageous rather than mere cost-of-business calculations.
- Support corporate accountability measures that would make executives personally liable for knowingly facilitating technology transfers that enable human rights abuses.

CLOSE THE CLOUD COMPUTING LOOPHOLE

CFU should pursue a three-pronged strategy to stop the use of cloud computing services by Uyghur genocide-linked Chinese firms and entities.

Lobby Congress to Pass New Legislative Tools

- Advocate for passage of H.R. 2683, the Remote Access Security Act, which addresses critical weaknesses in the Export Control Reform Act by requiring the administration to treat remote access to export-controlled technologies as equivalent to a physical export. This legislation has been introduced multiple times with bipartisan support but has faced significant lobbying opposition from the tech industry.²⁵³
- Develop a naming-and-shaming campaign targeting companies that lobby against this legislation, making sure to emphasize their role in enabling access to technologies used in genocide.
- Engage with lawmakers to understand industry objections and identify potential compromise modifications that maintain the legislation's core protections while addressing legitimate business concerns.
- Emphasize that treating cloud services as exports is only effective when paired with comprehensive export controls on surveillance technologies and their supporting services (such as training datasets for facial recognition models).

Lobby Executive Branch to Use Existing Authority

- Advocate for the President to use existing authority under the Export Control Reform Act (ECRA) of 2018 to restrict cloud computing services for "national security" or "foreign policy purposes." The Uyghur Human Rights Policy Act provides additional statutory authority for sanctioning entities linked to surveillance and abuses in East Turkestan.²⁴⁴
- Point to the rescinded Biden-era AI Diffusion Framework as evidence that the executive branch has interpreted its authority as extending to cloud computing services under certain circumstances.
- Push for implementation of existing but unused ECRA authority to restrict U.S. persons from offering cloud services "in support of foreign military, security, or intelligence services."
- Note that executive authority to restrict cloud compute access remains somewhat limited without the Remote Access Security Act, particularly for services operated from data centers located in China.

Develop Corporate Advocacy Strategy

- Build a campaign to pressure major cloud service providers (Amazon Web Services, Microsoft Azure, Google Cloud) to voluntarily adopt policies prohibiting their services from supporting mass surveillance activities.
- Mobilize public and investor pressure by raising awareness of cloud providers' documented role in enabling Chinese surveillance infrastructure in East Turkestan.
- This corporate advocacy strategy may also help limit industry opposition to legislative and executive actions described above.

DEVELOP AND PROMOTE CORPORATE ACCOUNTABILITY

Beyond governmental regulation, CFU should work to create market-based accountability mechanisms that increase reputational and financial costs for companies complicit in surveillance technologies used against Uyghurs.

Establish a 'Uyghur Tech Accountability Benchmark'

- Partner with technology ethics organizations (such as the Distributed AI Research Institute or similar groups) to create a regularly updated public scorecard rating U.S. and allied companies on:
 - Whether they audit their supply chains for surveillance technology misuse
 - Whether they have divested from surveillance-linked Chinese partners
 - Whether their venture capital arms fund Chinese AI or surveillance startups
 - Whether they provide cloud computing or other services to entities on sanctions lists
 - Transparency in disclosing Chinese partnerships and technology transfers
- Use this to inform investors, consumers, and policymakers about which companies are taking meaningful steps to prevent their technologies from enabling genocide.

Partner With Investment Due Diligence Organizations

- Collaborate with organizations that specialize in investment risk assessment (such as the Heartland Initiative) to produce comprehensive risk reports demonstrating that investments in companies with MSS surveillance ties represent significant financial, legal, and reputational risks due to potential sanctions, litigation, and reputational damage.
- Work with organizations including the Responsible Asset Allocator Initiative at New America, RFK Compass Investors, EthicalInvestment Research Services (EIRIS), and the Corporate Human Rights Benchmark (CHRB) to integrate Uyghur human rights considerations into Environmental, Social, and Governance (ESG) investment frameworks.

Create Divestment Incentives

- Advocate for federal legislation creating tax incentives that would allow investors to offset capital losses incurred from divesting from sanctioned or high-risk Chinese firms. This could be modeled after existing tax provisions that allow for capital loss deductions under the Internal Revenue Code Section 165's existing capital loss deduction framework, but would provide enhanced deductions specifically for losses resulting from compliance with sanctions or divestment from human-rights-abusing entities.²⁴⁵

- Support creation of a public disclosure regime where compliant institutions earn certification as 'No Exposure to PRC Surveillance Programs,' providing reputational benefits and potential preferential treatment in government contracting.

Engage Frontier AI Companies on Operational Safeguards

- Advocate for companies developing advanced AI systems (such as OpenAI, Anthropic, Google DeepMind, and others) to build explicit, China-specific operational safeguards into their models to prevent misuse by PRC-linked entities.
- Specific recommended safeguards include:
 - Internal red-teaming exercises simulating state-actor attacks from PRC-linked groups, modeled after existing red-teaming practices used for cybersecurity, misinformation, and bias testing
 - Enhanced geofencing and account verification for users in high-risk jurisdictions or for accounts that appear to be proxying for Chinese entities
 - Automated detection and blocking of queries related to developing or enhancing surveillance systems targeting Uyghurs
 - Transparency reporting on detected attempts to use AI systems for developing repressive technologies

STRENGTHEN INTERNATIONAL COORDINATION

Unilateral U.S. action, while necessary, is alone insufficient to prevent China from accessing surveillance technologies. CFU should advocate for coordinated international approaches that close loopholes created by supply chain fragmentation across multiple jurisdictions.

Expand Allied Awareness and Coordination

- Advocate for the State Department to use diplomatic channels to ensure U.S. allies fully understand how specific Chinese surveillance technologies contribute to genocide in East Turkestan, and encourage them to adopt parallel export restrictions. Target key allies whose cooperation is essential:
 - Netherlands (ASML's extreme ultraviolet lithography machines are essential for advanced chip manufacturing)
 - Japan (dominates coating systems, silicon wafers, and photoresists for chip manufacturing)
 - South Korea and Taiwan (advanced chip manufacturing through Samsung and TSMC)
 - European nations supplying surveillance components (France, Germany, UK)
- Push for creation of a 'Uyghur Human Rights Technology List' by the U.S.-China Economic and Security Review Commission; a publicly released registry naming companies whose technologies enable mass detention, digital monitoring, or coercive data collection in East Turkestan. This list should be:
 - Distributed to U.S. allies through diplomatic channels with requests for parallel action
 - Updated based on new evidence
 - Made available to CFU for advocacy campaigns

Develop Multilateral Export Control Regime

- Advocate for expansion of the Wassenaar Arrangement (the multilateral export control regime for conventional arms and dual-use goods) to comprehensively cover surveillance technologies and mass monitoring systems.
- Push for a new category within Wassenaar specifically addressing 'Technologies for Mass Surveillance and Human Rights Violations' that would include:
 - Facial and biometric recognition systems
 - Predictive policing algorithms and platforms
 - Mass data integration and analysis systems
 - Network surveillance equipment designed for comprehensive population monitoring

ADDRESS IP AND KNOWLEDGE TRANSFER VULNERABILITIES

China's surveillance capabilities depend not only on physical technology but also on knowledge, intellectual property, and research collaborations. CFU should advocate for policies that address these less tangible but equally important vectors of technology transfer.

Establish Patent Review Mechanism for Joint Venture Risk Assessment

- Advocate for mandatory review of patents related to sensitive technologies (AI, semiconductors, biometrics, networking) before companies can enter joint ventures with Chinese companies in these sectors. The mechanism of review should assess whether patented technologies could contribute to surveillance, military, or intelligence applications if transferred to Chinese partners.

Address University Research Vulnerabilities

- Advocate for stronger enforcement of Section 117 of the Higher Education Act, which requires universities to disclose foreign gifts and contracts.
- Push for universities with joint institutes in China to:
 - Implement strict firewalls preventing sensitive research knowledge from being shared with Chinese partner institutions
 - Conduct regular security reviews of collaborative research projects
- Support development of responsible publication guidelines for sensitive research areas, ensuring that open-source publication in areas such as AI surveillance capabilities, biometric algorithms, and semiconductor design includes consideration of potential misuse for human rights violations.
- CFU should educate university technology research labs on the technogenocide of the Uyghurs.

EXPAND SANCTIONS TARGETING THE IJOP

The IJOP represents the technological heart of China's genocide against Uyghurs. While the U.S. has sanctioned many companies involved in surveillance in East Turkestan, key entities that directly supply and maintain the IJOP system remain unsanctioned. CFU should advocate for comprehensive targeting of these entities and the broader IJOP supply chain.

Block All Imports from IJOP-Linked Entities

- Advocate for legislation expanding the Uyghur Forced Labor Prevention Act model to focus on IJOP related technology, blocking imports from any company that supplies technology, data, or services to the IJOP system.
- Develop CFU materials for American consumers educating on the IJOP and how to mitigate their consumption of related products.

Target Key Personnel

- Advocate for individual sanctions (visa restrictions, asset freezes) targeting executives and key technical personnel at IJOP-linked companies, including:
 - Senior executives at CETC, Xinjiang Lianhai, and HBFEC
 - Technical leads responsible for IJOP system design and maintenance
 - Government officials who oversee IJOP implementation and data analysis
- These individual sanctions would be beneficial by creating personal accountability, incentivizing individuals to leave problematic companies, and demonstrating that enablers of genocide will face personal consequences.

STRENGTHEN FINANCIAL MARKET ACCOUNTABILITY

U.S. capital markets continue to channel investment into Chinese companies that enable the Uyghur genocide. CFU should advocate for Securities and Exchange Commission (SEC) reforms that prevent U.S. financial markets from supporting surveillance technologies and human rights abuses.

Reform Foreign Private Issuer Registration Standards

- Advocate for the SEC to condition foreign private issuer (FPI) registration on demonstrated compliance with U.S. human rights, sanctions, and national security standards. Specifically:
 - Foreign investment advisers should be denied or have registration revoked if they hold equity in: companies sanctioned for human rights abuses in East Turkestan, companies providing support to PRC security services, companies engaged in cyber-espionage operations, or companies developing or deploying technologies enabling repression of Uyghurs.
 - Registered firms should be required to divest from high-risk holdings or undergo enhanced due-diligence reviews before maintaining SEC registration.
- This approach leverages the value of SEC registration (which grants access to U.S. investors and capital markets) as a mechanism to prevent U.S. financial markets from indirectly supporting the genocide

Mandate Human Rights Due Diligence in Investment Guidance

- Advocate for the SEC to provide formal guidance requiring investors to conduct human rights due diligence on their portfolios, including examination of investee companies' supply chains for risks related to Environmental, Social, and Governance (ESG) factors.
- Push for mandatory disclosure requirements where investment firms must report:
 - Extent of portfolio exposure to companies on sanctions lists
 - Results of human rights due diligence assessments
 - Steps taken to address identified risks

BUILD COALITION OF TNR VICTIMS

Chinese surveillance technologies developed for use against Uyghurs are being exported globally, creating a common cause among multiple communities suffering under Chinese-enabled repression. CFU should build coalitions with other affected communities to broaden advocacy impact and raise awareness of shared threats.

Identify Coalition Partners

- Build partnerships with advocacy organizations representing communities victimized by Chinese surveillance technology exports, including:
 - Tibetan advocacy groups (Chinese surveillance systems deployed in Tibet)²⁴⁶
 - Hong Kong democracy advocates (extensive surveillance infrastructure)²⁴⁷
 - Iranian democracy and human rights organizations (Iran has imported Chinese surveillance technologies)²⁴⁸
 - Pro-democracy civil society organizations in countries with Chinese 'safe cities' (Zimbabwe, Kenya, Uganda, etc.)²⁴⁹

Develop Shared Advocacy Strategy

- Create a unified advocacy framework emphasizing that Chinese surveillance technologies:
 - Were developed and perfected through genocide against Uyghurs
 - Are now being exported globally to enable repression of diverse populations
 - Represent a transnational threat to democracy and human rights
 - Require coordinated international action to prevent further proliferation
- Develop joint policy positions on:
 - Export controls on surveillance technologies
 - Sanctions on Chinese surveillance companies
 - Restrictions on Western companies enabling surveillance exports
 - International accountability mechanisms
- Organize joint advocacy campaigns including:
 - Coordinated Congressional testimony from multiple affected communities
 - Multinational petitions and open letters to governments and companies
 - Joint reports documenting Chinese surveillance technology proliferation
 - Coordinated media campaigns highlighting the global scope of Chinese surveillance exports

CONCLUSION

These nine recommendations provide CFU with a comprehensive advocacy roadmap addressing the full ecosystem that enables the surveillance state in East Turkestan. Implementing these recommendations will require sustained advocacy directed at Congress, executive branch agencies, regulatory bodies, corporations, investors, allied governments, universities, and international institutions. CFU should pursue these recommendations as components of an integrated strategy that raises costs for technological complicity at every point in the supply chain. Most critically, these recommendations recognize that preventing future genocides enabled by emerging technologies requires action now, while there remains opportunity to shape the governance frameworks that will determine how artificial intelligence, biometric systems, and mass data analysis are deployed globally. The surveillance capabilities developed against Uyghurs represent a model that authoritarian regimes worldwide seek to replicate. By systematically dismantling the technological, financial, and knowledge infrastructure that supports China's technogenocide, the United States and its allies can not only help protect Uyghurs but also prevent the proliferation of these capabilities to enable repression of other populations. This is the urgent imperative that must guide Campaign for Uyghurs' advocacy efforts in the years ahead.

ENDNOTES

- 1 Maizland, Lindsay. 2022. “China’s Repression of Uyghurs in Xinjiang.” Council on Foreign Relations. Council on Foreign Relations. September 22, 2022. <https://www.cfr.org/backgrounder/china-xinjiang-uyghurs-muslims-repression-genocide-human-rights>.
- 2 Roberts, Sean R. 2020. *The War on the Uyghurs: China’s Internal Campaign Against a Muslim Minority*. N.p.:Princeton University Press. (48-49)
- 3 Human Rights Watch. 2018b. “Eradicating Ideological Viruses.” Human Rights Watch, September. <https://www.hrw.org/report/2018/09/10/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs>.
- 4 Human Rights Watch. 2018. “China: Big Data Fuels Crackdown in Minority Region.” Human Rights Watch. February 26, 2018. <https://www.hrw.org/news/2018/02/27/china-big-data-fuels-crackdown-minority-region>.
- 5 Nee, William. 2015. “China: Draconian Anti-Terror Law an Assault on Human Rights.” Amnesty International. March 4, 2015. <https://www.amnesty.org/en/latest/news/2015/03/china-draconian-anti-terror-law/>.
- 6 Zenz, Adrian. 2022. “The Xinjiang Police Files: Re-Education Camp Security and Political Paranoia in the Xinjiang Uyghur Autonomous Region.” *Journal of the European Association for Chinese Studies* 3, no. 2022 (May): 263-311. <https://doi.org/10.25365/jeacs.2022.3.zenz>. (264)
- 7 Roberts, Sean R. 2020. *The War on the Uyghurs: China’s Internal Campaign Against a Muslim Minority*. N.p.:Princeton University Press. (257)
- 8 Uyghar, and Alim Seytoff. 2025. “Report: China Has Half a Million Uyghurs in Prison or Detention.” Radio Free Asia. February 27, 2025. <https://www.rfa.org/english/uyghur/2025/02/27/uyghur-us-report-chinas-atrocities-xinjiang/>.
- 9 Human Rights Watch. 2021. “Break Their Lineage, Break Their Roots.” Human Rights Watch. April 19, 2021. <https://www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting>.
- 10 Ibid.
- 11 Pompeo, Michael. 2021. “Determination of the Secretary of State on Atrocities in Xinjiang.” U.S. Department of State. January 19, 2021. <https://2017-2021.state.gov/determination-of-the-secretary-of-state-on-atrocities-in-xinjiang/>.
- 12 Lindsay Maizland, “China’s Repression of Uyghurs in Xinjiang,” Council on Foreign Relations, last updated October 3, 2025, accessed December 14, 2025, <https://www.cfr.org/backgrounder/china-xinjiang-uyghurs-muslims-repression-genocide-human-rights>.
- 13 James Millward and Dahlia Peterson, “China’s System of Oppression in Xinjiang: How It Developed and How to Curb It,” Brookings Institution, Global China Project, September 2020, accessed December 14, 2025, <https://www.brookings.edu/articles/chinas-system-of-oppression-in-xinjiang-how-it-developed-and-how-to-curb-it/>.
- 14 International Organization for Standardization (ISO), “What Is Artificial Intelligence (AI)?,” accessed December 14, 2025, <https://www.iso.org/artificial-intelligence/what-is-ai>.

- 15 MIT xPRO, “Exploring the Shift from Traditional to Generative AI,” The Curve – MIT, October 22, 2024, accessed December 14, 2025, <https://curve.mit.edu/exploring-shift-traditional-generative-ai>.
- 16 G. Sreenu and M. A. Saleem Durai, “Intelligent Video Surveillance: A Review through Deep Learning Techniques for Crowd Analysis,” *Journal of Big Data* 6, no. 1 (2019): 48, <https://doi.org/10.1186/s40537-019-0212-5>.
- 17 Ben Buchanan, *The AI Triad and What It Means for National Security Strategy*, Center for Security and Emerging Technology, August 2020, <https://doi.org/10.51593/20200021>.
- 18 Daswin De Silva and Daminda Alahakoon, “An Artificial Intelligence Life Cycle: From Conception to Production,” *Patterns* 3, no. 6 (2022): 100489, <https://doi.org/10.1016/j.patter.2022.100489>.
- 19 Darrell M. West, “How AI Can Enable Public Surveillance,” Brookings Institution, April 15, 2025, accessed December 14, 2025, <https://www.brookings.edu/articles/how-ai-can-enable-public-surveillance/>.
- 20 Tom Phillips, “China Testing Facial-Recognition Surveillance System in Xinjiang – Report,” *Guardian*, January 18, 2018, <https://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report>.
- 21 Human Rights Watch, *China’s Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, May 1, 2019, <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass>.
- 22 Ibid.
- 23 Fergus Ryan, Bethany Allen, Shelly Shih, Stephan Robin, Nathan Attrill, Jared Alpert, Astrid Young, and Tilla Hoja, *The Party’s AI: How China’s New AI Systems Are Reshaping Human Rights*, Australian Strategic Policy Institute, December 1, 2025, <https://www.aspi.org.au/report/the-partys-ai-how-chinas-new-ai-systems-are-reshaping-human-rights/>.
- 24 U.S. Department of the Treasury, “Treasury Identifies Eight Chinese Tech Firms as Part of the Chinese Military-Industrial Complex,” press release, December 16, 2021, <https://home.treasury.gov/news/press-releases/jy0538>.
- 25 IPVM Team, “Patenting Uyghur Tracking – Huawei, Megvii, More,” IPVM, January 12, 2021, <https://ipvm.com/reports/patents-uyghur>.
- 26 Dake Kang and Yael Grauer, “Detailed Findings from AP Investigation into How US Tech Firms Enabled China’s Digital Police State,” *Associated Press*, September 9, 2025, <https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-a80904158b771a14d5a734947f28d71b>.
- 27 Human Rights Watch, *China’s Algorithms of Repression*.
- 28 Ryan et al., *The Party’s AI*.
- 29 OpenAI, *Disrupting Malicious Uses of AI: An Update*, October 2025, <https://cdn.openai.com/threat-intelligence-reports/7d662b68-952f-4dfd-a2f2-fe55b041cc4a/disrupting-malicious-uses-of-ai-october-2025.pdf>.
- 30 Human Rights Watch, *China’s Algorithms of Repression*.
- 31 Human Rights Watch, “China: Big Data Fuels Crackdown.”
- 32 Ibid.
- 33 Human Rights Watch, *China’s Algorithms of Repression*.
- 34 Human Rights Watch, “China: Big Data Fuels Crackdown.”
- 35 Human Rights Watch, *China’s Algorithms of Repression*.
- 36 Human Rights Watch, “China: Big Data Fuels Crackdown.”

- 37 Human Rights Watch, *China's Algorithms of Repression*.
- 38 Human Rights Watch, "China: Big Data Fuels Crackdown."
- 39 Ibid.
- 40 Ibid.
- 41 Ibid.
- 42 Human Rights Watch, *China's Algorithms of Repression*; Human Rights Watch, "Big Data Fuels Crackdown."
- 43 Ibid.
- 44 Ibid.
- 45 Ibid.
- 46 Ibid.
- 47 Emily Benson and Margot Putnam, "Export Controls and Intangible Goods," *Center for Strategic and International Studies, Critical Questions*, April 11, 2023, <https://www.csis.org/analysis/export-controls-and-intangible-goods>.
- 48 Stephanie Susnjara and Ian Smalley, "What Is Cloud Computing?," *IBM*, accessed December 14, 2025, <https://www.ibm.com/think/topics/cloud-computing>.
- 49 Synergy Research Group, "Q2 Cloud Market Nears \$100 Billion Milestone—and It's Still Growing by 25% Year over Year," July 31, 2025, <https://www.srgresearch.com/articles/q2-cloud-market-nears-100-billion-milestone-and-its-still-growing-by-25-year-over-year>.
- 50 Garance Burke, Dake Kang, and Byron Tau, "US Government Allowed and Even Helped US Firms Sell Tech Used for Surveillance in China, AP Finds," *Associated Press*, October 30, 2025, <https://apnews.com/article/chinese-surveillance-silicon-valley-trump-administration-congress-21c5f961b1fd22f9a9e563ebe64e5582>.
- 51 Ibid.
- 52 Ibid.
- 53 U.S. Department of Commerce, Bureau of Industry and Security, "Addition of Certain Entities to the Entity List," *Federal Register* 84, no. 196 (October 9, 2019): 54002–54017, <https://www.federalregister.gov/d/2019-22210>.
- 54 Hanna Dohmen, Jacob Feldgoise, Emily S. Weinstein, and Timothy Fist, "Controlling Access to Advanced Compute via the Cloud: Options for U.S. Policymakers, Part I," *Center for Security and Emerging Technology*, May 15, 2023, <https://cset.georgetown.edu/article/controlling-access-to-advanced-compute-via-the-cloud/>.
- 55 Amazon Web Services, "AWS China Regions," accessed December 14, 2025, <https://www.amazonaws.cn/en/about-aws/china/>.
- 56 Burke, Kang, and Tau, "US Government Allowed and Even Helped US Firms."
- 57 Eduardo Baptista, Fanny Potkin, and Karen Freifeld, "Exclusive: Chinese Entities Turn to Amazon Cloud and Its Rivals to Access High-End US Chips, AI," *Reuters*, August 22, 2024, <https://www.reuters.com/technology/chinese-entities-turn-amazon-cloud-its-rivals-access-high-end-us-chips-ai-2024-08-23/>.
- 58 Ari Hawkins, Katherine Long, and Cheyenne Haslett, "US to Allow Powerful AI Chip Sales to China, Trump Says," *Politico*, December 8, 2025, <https://www.politico.com/news/2025/12/08/u-s-to-allow-nvidias-h200-sales-in-china-trump-confirms-00681619>.
- 59 Liza Lin and Stu Woo, "How a Chinese AI Company Worked Around U.S. Rules to Access Nvidia's Top Chips," *Wall Street Journal*, November 12, 2025, <https://www.wsj.com/tech/ai/china-ai-nvidia-chip-access-6a4fa63d>.

- 60 Hawkins, Long, and Haslett, “US to Allow Powerful AI Chip Sales to China.”
- 61 U.S. Department of Commerce, Bureau of Industry and Security, *Application of the Export Administration Regulations to Grid and Cloud Computing Services*, advisory opinion, January 13, 2009, <https://www.bis.gov/media/documents/application-ear-grid-cloud-computing-services.pdf>.
- 62 Amazon Web Services, “AWS Global Export Compliance,” accessed December 14, 2025, <https://aws.amazon.com/compliance/global-export-compliance/>.
- 63 Ibid.
- 64 Microsoft, *Microsoft Azure Cloud Services: Export Controls of the United States, United Kingdom, European Union, Japan, Australia, Canada, and New Zealand*, February 2022, <https://datacenters.microsoft.com/wp-content/uploads/2023/12/Microsoft-Azure-Export-Controls-White-Paper-Feb-2022.pdf>.
- 65 Michael T. McCaul and Mike Gallagher, letter to Jake Sullivan, National Security Advisor, October 6, 2023, <https://foreignaffairs.house.gov/sites/evo-subsites/republicans-foreignaffairs.house.gov/files/migrated/uploads/2023/10/10.6.23-McCaul-and-Gallagher-ltr-to-NSA-Sullivan-re-October-7-Anniversary-v2.pdf>.
- 66 Lennart Heim, *Understanding the Artificial Intelligence Diffusion Framework*, RAND Corporation, January 14, 2025, <https://www.rand.org/pubs/perspectives/PEA3776-1.html>.
- 67 Ibid.
- 68 U.S. Department of Commerce, Bureau of Industry and Security, *BIS Policy Statement on Controls that May Apply to Advanced Computing Integrated Circuits and Other Commodities Used to Train AI Models*, May 13, 2025, <https://www.bis.gov/media/documents/ai-policy-statement-training-ai-models-may-13-2025>.
- 69 U.S. Department of Commerce, Bureau of Industry and Security, “Department of Commerce Announces Rescission of Biden-Era Artificial Intelligence Diffusion Rule, Strengthens Chip-Related Export Controls,” press release, May 13, 2025, <https://www.bis.gov/press-release/department-commerce-announces-rescission-biden-era-artificial-intelligence-diffusion-rule-strengthens>.
- 70 U.S. Congress, House, *Remote Access Security Act*, H.R. 8152, 118th Cong. (passed House, September 9, 2024), <https://www.congress.gov/bill/118th-congress/house-bill/8152>.
- 71 U.S. Congress, House, *Remote Access Security Act*, H.R. 2683, 119th Cong. (introduced April 7, 2025), <https://www.congress.gov/bill/119th-congress/house-bill/2683>.
- 72 U.S. Congress, Senate, Amendment 3567 to S. 2296, *National Defense Authorization Act for Fiscal Year 2026*, 119th Cong. (submitted August 1, 2025), <https://www.congress.gov/amendment/119th-congress/senate-amendment/3567>.
- 73 Problem Solvers Caucus, “PSC National Security Working Group Endorses 10 Bipartisan NDAA Amendments,” press release, September 4, 2025, <https://problemsolverscaucus.house.gov/media/press-releases/psc-national-security-working-group-endorses-10-bipartisan-ndaa-amendments>.
- 74 U.S. Congress, *Remote Access Security Act* (H.R. 8152, 118th Cong.)
- 75 Burke, Kang, and Tau, “US Government Allowed and Even Helped US Firms.”
- 76 Ibid.
- 77 Dake Kang, “How the AP Uncovered US Big Tech’s Role in China’s Digital Police State,” *Associated Press*, September 8, 2025, <https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-00bed6421ad8d2ccc6e69f104babe892>.

78 Asa Fitch, “Restricting Chip Sales to China Could Backfire on U.S., Industry Group Says,” *Wall Street Journal*, updated July 17, 2023, <https://www.wsj.com/world/restricting-chip-sales-to-china-could-backfire-on-u-s-industry-group-says-dbb7b8df>.

79 Ibid.

80 Eleanor Olcott, “Nvidia Chief Jensen Huang Condemns US Chip Curbs on China as ‘a Failure’,” *Financial Times*, May 20, 2025, <https://www.ft.com/content/a3fce85c-8651-4fec-ab6a-c876ec01a547>.

81 U.S. Department of Commerce, Bureau of Industry and Security, “Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification,” *Federal Register* 87, no. 197 (October 13, 2022): 62186–62240, <https://www.federalregister.gov/d/2022-21658>.

82 Stephen Nellis, Karen Freifeld, and Alexandra Alper, “U.S. Aims to Hobble China’s Chip Industry with Sweeping New Export Rules,” Reuters, October 10, 2022, <https://www.reuters.com/technology/us-aims-hobble-chinas-chip-industry-with-sweeping-new-export-rules-2022-10-07/>.

83 Karen M. Sutter, U.S. Export Controls and China: Advanced Semiconductors, CRS Report no. R48642 (Washington, DC: Congressional Research Service, September 19, 2025), <https://www.congress.gov/crs-product/R48642>.

84 Hawkins, Long, and Haslett, “US to Allow Powerful AI Chip Sales to China.”

85 Yahoo Finance. “BIDU – Holders.” *Yahoo Finance*. <https://finance.yahoo.com/quote/BIDU/holders/>

86 DataGrand. “English Index.” *DataGrand*. <https://www.datagrand.com/english-index>

87 Chiu, Joanna. “Chinese Startups Supported by Microsoft and Google Incubator Programs Worked with Police.” *Rest of World*, November 19, 2024. <https://restofworld.org/2024/microsoft-google-chinese-startup-incubator-police-surveillance/>

88 Ibid.

89 Interview conducted with East Turkistan Human Rights Watch Staff in Istanbul Turkey, October 2025.

90 Interview conducted with East Turkistan Human Rights Watch Staff in Istanbul Turkey, October 2025.

91 Federal Bureau of Investigation. *IC3 Cyber Safety Review 2025*.

92 Ibid.

93 *Intelligence Online*. “Chinese Firm Behind Hacking Operations Against Uyghurs and Tibetans Unveiled.” January 29, 2025. <https://www.intelligenceonline.com/surveillance--interception/2025/01/29/chinese-firm-behind-hacking-operations-against-uyghurs-and-tibetans-unveiled,110368855-evg>

94 Human Rights Watch. “China: How Mass Surveillance Works in Xinjiang.” Human Rights Watch, May 1, 2019. <https://www.hrw.org/news/2019/05/01/china-how-mass-surveillance-works-xinjiang>

95 ASML, “The Basics of Microchips,” ASML, 2022, <https://www.asml.com/en/technology/all-about-microchips/microchip-basics>.

96 Dake Kang and Yael Grauer, “How Silicon Valley Enabled China’s Digital Police State,” *Associated Press*, September 9, 2025, <https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-8e000601dad6aea230f18170ed54e88>.

97 “2024年度常州市金坛区道路交通监控设备维护项目更正公告,” 常州市政府采购网, published July 5, 2024, archived June 18, 2025, at the Wayback Machine, https://web.archive.org/web/20250618040049/https://zfcg.changzhou.gov.cn/html/ns/zfjzcg_gzgg/732074939955900.html

98 “分析报价表”, archived June 18, 2025, at the Wayback Machine, <https://web.archive.org/web/20250618035847/https://jy-datafile.oss-cn-beijing.aliyuncs.com/b7bc6db0034c6714f1ab853cab1ff413ab09dec6d8e5bca8f2ef765a4e1a9e48.pdf>

99 “China Cables: IJOP Daily Bulletin No. 14 (English),” International Consortium of Investigative Journalists (ICIJ), 2019, DocumentCloud, <https://embed.documentcloud.org/documents/6558506-China-Cables-IJOP-Daily-Bulletin-14-English/>.

100 Paul Mozur and Don Clark, “China’s Surveillance State Sucks up Data. U.S. Tech Is Key to Sorting It.,” *The New York Times*, November 23, 2020, sec. Technology, <https://www.nytimes.com/2020/11/22/technology/china-intel-nvidia-xinjiang.html>.

101 Ibid.

102 Sui-Lee Wee, “China Is Collecting DNA from Tens of Millions of Men and Boys, Using U.S. Equipment,” *The New York Times*, June 17, 2020, sec. World, <https://www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html>.

103 Andy Lin et al., “China Wants to Use 115,000 Banned Nvidia Chips to Fulfill Its AI Ambitions (NVDA),” Bloomberg.com (Bloomberg, July 8, 2025), <https://www.bloomberg.com/graphics/2025-china-data-centers-nvidia-chips/>.

104 Pia Singh, “Nvidia Claps Back Against Chinese Accusations Its H20 Chips Aren’t Safe,” CNBC, August 10, 2025, <https://www.cnbc.com/2025/08/10/nvidia-china-h20-chips.html>

105 Dake Kang and Yael Grauer, “How Silicon Valley Enabled China’s Digital Police State,” AP News, September 9, 2025, <https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-8e000601dadb6aea230f18170ed54e88>.

106 Liu Xuanzun, “Xinjiang Gets Border Patrol Drones for Better Missions,” *Global Times*, January 21, 2020, <https://www.globaltimes.cn/page/202001/1177627.shtm>

107 Ibid.

108 Daniel A. Medina, “China Is Now Using Drones to Catch ‘Terrorists’ in Xinjiang,” Quartz, January 10, 2025, <https://qz.com/256104/china-is-now-using-drones-to-catch-terrorists-in-xinjiang>

109 “FOR IMMEDIATE RELEASE BUREAU of INDUSTRY and SECURITY Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People’s Republic of China (PRC),” 2022, <https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file>.

110 Eduardo Baptista, “China’s Military and Government Acquire Nvidia Chips despite US Ban,” *Reuters*, January 14, 2024, <https://www.reuters.com/technology/chinas-military-government-acquire-nvidia-chips-despite-us-ban-2024-01-14/>.

111 “US Will Get a 15% Cut of Nvidia and AMD Chip Sales to China under a New, Unusual Agreement | the Associated Press,” The Associated Press (The Associated Press, August 11, 2025), <https://www.ap.org/news-highlights/spotlights/2025/us-will-get-a-15-cut-of-nvidia-and-amd-chip-sales-to-china-under-a-new-unusual-agreement/>

112 Ana Swanson, Paul Mozur, and Steve Lohr, “U.S. Blacklists More Chinese Tech Companies over National Security Concerns,” *The New York Times*, June 21, 2019, <https://www.nytimes.com/2019/06/21/us/politics/us-china-trade-blacklist.html>.

113 Anton Shilov, “Blacklisted China Chipmaker SMIC Becomes the World’s Second-Largest Pure-Play Foundry by Revenue — Outsells GlobalFoundries and Others,” *Tom’s Hardware*, May 10, 2024, <https://www.tomshardware.com/tech-industry/blacklisted-china-chipmaker-smic-becomes-the-worlds-second-largest-pure-play-foundry-by-revenue-outsells-globalfoundries-and-others>.

114 Matthew Schleich and William Alan Reinsch, “Contextualizing the National Security Concerns over China’s Domestically Produced High-End Chip,” *Center for Strategic and International Studies*, September 26, 2023, <https://www.csis.org/analysis/contextualizing-national-security-concerns-over-chinas-domestically-produced-high-end-chip>.

115 Brookings Institution, “China’s System of Oppression in Xinjiang: How It Developed and How to Curb It,” *Brookings Institution*, 2020, <https://www.brookings.edu/articles/chinas-system-of-oppression-in-xinjiang-how-it-developed-and-how-to-curb-it/>

Emily Lin, “China’s Safe Cities Serve as Solutions and Opportunities for Growth,” *ASMAG*, 2015, <https://www.asmag.com/showpost/19628.aspx>

116 BIT CCTV Solutions, “2024 Global Top 50 Security Companies,” BIT CCTV Solutions, 2024, <https://www.bit-cctv.com/2024-global-top-50-security-companies.html>.

117 Conor Healy, “Shanghai Launches New ‘Uyghur Ethnicity’ Detection,” *IPVM*, 2024, <https://ipvm.com/reports/filtering-for-uyghurs>

118 Charles Rollet, “Hikvision Markets Uyghur Ethnicity Analytics, Now Covers Up,” *IPVM*, 2019, <https://ipvm.com/reports/hikvision-uyghur>

119 Omer Kanat and Peter Irwin, “Hikvision and Dahua Facilitating Genocidal Crimes in East Turkistan,” Uyghur Human Rights Project, 2023, <https://uhrp.org/statement/hikvision-and-dahua-facilitating-genocidal-crimes-in-east-turkistan/>

120 Drew Harwell and Eva Dou, “Huawei Tested AI Software That Could Recognize Uighur Minorities and Alert Police, Report Says,” *The Washington Post*, December 8, 2020, <https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uyghur-minorities-alert-police-report-says/>

121 Conor Healy, *Uyghur Surveillance & Ethnicity: Detection Analytics in China*, expert report presented to the Uyghur Tribunal (August 20, 2021), <https://uyghurtribunal.com/wp-content/uploads/2021/09/Conor-Healy.pdf>

122 Victims of Communism Memorial Foundation, *Xinjiang Police Files Fact Sheet*, May 23, 2022, <https://www.xinjiangpolicefiles.org/wp-content/uploads/2022/05/Xinjiang-Police-Files-Fact-Sheet-220523c.pdf>

123 Almost 100 % of China’s Public Spaces Under Watch: Here Is How China Turned Neighbours into Agents of the Chinese Communist Party,” *Turkistan Times* (Arabic edition), March 6, 2021, <https://turkistantimes.com/ar/news-14406.html>

124 Human Rights Watch, “China’s Algorithms of Repression,” May 1, 2019, <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass>.

125 Ambarella, Inc., Annual Report on Form 10-K for the Fiscal Year Ended January 31, 2019, SEC Accession No. 0001564590-19-010114, filed March — 2019, https://www.sec.gov/Archives/edgar/data/1280263/000156459019010114/amba-10k_20190131.htm

- 126 Nikita Ermolaev, “Hikvision Embedded Open Platform (HEOP) 2.0 Examined,” IPVM, February 10, 2023, <https://ipvm.com/reports/heop-2>
- 127 Dahua Technology, “Together with NVIDIA, Dahua Promotes Video+ with ‘Deep Sense’ Smart Video Structure Server,” Dahua Technology press release, March 23, 2017, <https://www.dahuasecurity.com/nl/newsEvents/pressRelease/751>
- 128 Brian Dipert, “Intel Movidius Helps Bring Artificial Intelligence to Video Surveillance Cameras,” Edge AI and Vision Alliance, April 6, 2017, <https://www.edge-ai-vision.com/2017/04/intel-movidius-helps-bring-artificial-intelligence-to-video-surveillance-cameras/>.
- 129 Charles Rollet, “WSJ Reporters on How China Built the World’s Biggest Surveillance State,” IPVM, September 5, 2022, <https://ipvm.com/reports/china-surv-book>
- 130 Ibid.
- 131 Karen Freifeld, “Seagate to Pay \$300 Million Penalty for Shipping Huawei 7 Million Hard Drives,” Reuters, April 19, 2023, <https://www.reuters.com/legal/seagate-settles-with-us-shipping-11-bln-hard-drives-huawei-2023-04-19/>
- 132 Charles Rollet, “WD and Seagate Stop Selling to Dahua,” IPVM, November 7, 2022, <https://ipvm.com/reports/seagate-wd-dahua.>
- 133 Dake Kang and Yael Grauer, “Silicon Valley Enabled Brutal Mass Detention and Surveillance in China, Internal Documents Show,” Associated Press, September 9, 2025, <https://www.apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-8e000601dad6aea230f18170ed54e88>
- 134 IPVM Team, “Hikvision Uyghur Recognition, NVIDIA-Powered, Sold to PRC China Authorities,” IPVM, July 25, 2023, <https://ipvm.com/reports/hikvision-uyghur-nvidia?code=fsdcyedb321>
- 135 U.S. House, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, Selling the Forges of the Future, 119th Cong., 1st sess., October 7, 2025, <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/selling-the-forges-of-the-future.pdf>
- 136 Conor Healy, “Hikvision and AGM Analyzed,” IPVM, March 24, 2025, <https://ipvm.com/reports/agm-hikvision-examined>
- 137 Dahua Technology, “Dahua Announces Joint Venture with Alat to Develop Its First Overseas Manufacturing Hub in Saudi Arabia,” Dahua Technology press release, February 20, 2024, <https://www.dahuasecurity.com/newsEvents/pressRelease/9661>
- 138 Marion Halftermeyer and Mackenzie Hawkins, “Saudi Arabia’s \$100 Billion AI Fund Will Divest From China If U.S. Asked, CEO Says,” Bloomberg, May 7, 2024, <https://www.bloomberg.com/news/articles/2024-05-07/saudi-ai-fund-would-divest-from-china-tech-if-us-asked-ceo-says>
- 139 Krystal Hu and Jeffrey Dastin, “Exclusive: Amazon Turns to Chinese Firm on U.S. Blacklist to Meet Thermal Camera Needs,” Reuters, April 29, 2020, <https://www.reuters.com/article/us-health-coronavirus-amazon-com-cameras/exclusive-amazon-turns-to-chinese-firm-on-u-s-blacklist-to-meet-thermal-camera-needs-idUSKBN22B1AL/>
- 140 John Scanlan and Conor Healy, “Honeywell Hides OEMing PRC China Sunell,” IPVM, August 19, 2024, <https://ipvm.com/reports/honeywell-oems-sunell>

- 141 Raffaele Huang and Liza Lin, “Chinese AI Companies Dodge U.S. Chip Curbs by Flying Suitcases of Hard Drives Abroad,” The Wall Street Journal, June 12, 2025, https://www.wsj.com/tech/china-ai-chip-curb-suitcases-7c47dab1?gaa_at=eafs&gaa_n=AWEtSQeQ0t8oVC3Zm5TPdgcIGG7KAaESgtJEggS17nROJneRqIO61NmvnRbJN8gLwvw%3D&gaa_ts=6940543b&gaa_sig=fOS-kUjTf3xgL0szre05toCS0TANbjTyFltYlktGV5dQtvzCpqRQytz7tg1RbPjfoZkeNPSHAKLI5iR80WG73g%3D%3D
- 142 Jiang, Kun, Wolfgang Keller, Larry Qiu, and William Ridley. 2019. “China’s Joint Venture Policy and the International Transfer of Technology.” February 6, 2019. <https://voxchina.org/show-3-115.html>.
- 143 Huld, Arendse. 2025. “China’s 2025 Negative List for Market Access.” China Briefing News. May 5, 2025. <https://www.china-briefing.com/news/chinas-2025-negative-list-for-market-access/>.
- 144 Ibid.
- 145 Cory, Nigel. 2021. “Nigel Cory Associate Director, Trade Policy Information Technology and Innovation Foundation before the United States-China Economic and Security Review Commission’s Panel on China’s Cloud Market as Part of Its Hearing ‘a Net Assessment of the Chinese Communist Party’s Economic Ambitions, Plans, and Metrics of Future Success.’” <https://www2.itif.org/2021-china-cloud-market.pdf>.
- 146 “Azure in China Datacenters.” 2023. Microsoft.com. May 30, 2023. <https://learn.microsoft.com/en-us/azure/china/overview-datacenter>.
- 147 “AWS in China.” Amazon Web Services, Inc. <https://www.amazonaws.cn/en/about-aws/china/>.
- 148 Levine, Mike. 2024. “Top US Official Warns of ‘Large Uptick’ in Foreign Spies Targeting Tech Companies, Threatening National Security.” ABC News. October 29, 2024. <https://abcnews.go.com/US/top-us-official-warns-large-uptick-foreign-spies/story?id=115229723>.
- 149 CSIS. 2023. “Survey of Chinese Espionage in the United States since 2000 | Strategic Technologies Program | CSIS.” 2023. <https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000>.
- 150 “A Comprehensive Analysis of I-Soon’s Commercial Offering.” 2024. HarfangLab. March 2024. <https://harfanglab.io/insidethelab/isoon-leak-analysis/>.
- 151 Ibid.
- 152 “Attributing I-SOON: Private Contractor Linked to Multiple Chinese State-Sponsored Groups.” 2024. Recordedfuture.com. March 20, 2024. <https://www.recordedfuture.com/research/attributing-i-soon-private-contractor-linked-chinese-state-sponsored-groups>.
- 153 Ibid.
- 154 Kaaviya. 2025. “US Charges 12 Chinese Hackers for Hacking National Security Infrastructure.” Cyber Security News. CybersecurityNews. March 13, 2025. <https://cybersecuritynews.com/us-charges-12-chinese-hackers/>.
- 155 Fedasiuk, Ryan. 2020. “The China Scholarship Council: An Overview CSET Issue Brief.” <https://cset.georgetown.edu/wp-content/uploads/China-Scholarship-Council-Overview.pdf?ref=stanfordreview.org>.
- 156 “Brief Report on Chinese Overseas Students and International Students in China 2017 - Ministry of Education of the People’s Republic of China.” 2018. En.moe.gov.cn. March 31, 2018. http://en.moe.gov.cn/documents/reports/201901/t20190115_367019.html.
- 157 Molloy, Garret, and Elsa Johnson. 2025. “INVESTIGATION: Uncovering Chinese Academic Espionage at Stanford.” The Stanford Review. May 7, 2025. <https://stanfordreview.org/investigation-uncovering-chinese-academic-espionage-at-stanford/>.

158 Levine, Mike. 2024. "Top US Official Warns of 'Large Uptick' in Foreign Spies Targeting Tech Companies, Threatening National Security." ABC News. October 29, 2024. <https://abcnews.go.com/US/top-us-official-warns-large-uptick-foreign-spies/story?id=115229723>.

159 "Ding_indictment.pdf | United States Department of Justice." 2025. Justice.gov. 2025. <https://www.justice.gov/opa/media/1388341/>.

160 Portman, Rob, and Tom Carper. n.d. "United States Senate Permanent Subcommittee on Investigations Committee on Homeland Security and Governmental Affairs Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans Staff Report Subcommittee on Investigations United States Senate." https://www.govinfo.gov/content/pkg/GOVPUB-Y4_G74_9-PURL-gpo128826/pdf/GOVPUB-Y4_G74_9-PURL-gpo128826.pdf.

161 Jia, Hepeng. 2018. "China's Plan to Recruit Talented Researchers." Nature 553 (7688): S8–8. <https://doi.org/10.1038/d41586-018-00538-z>.

162 Ibid.

163 Shi, Dongbo, Weichen Liu, and Yanbo Wang. 2023. "Has China's Young Thousand Talents Program Been Successful in Recruiting and Nurturing Top-Caliber Scientists?" Science 379 (6627): 62–65. <https://doi.org/10.1126/science.abq1218>.

164 Ibid.

165 Zegart, Amy, and Emerson Johnston. 2025. "A Deep Peek into DeepSeek AI's Talent and Implications for US Innovation." https://www.hoover.org/sites/default/files/research/docs/Zegart_DeepSeekAI_Talent_July1.pdf.

166 "Applying for an 'R' Visa- 国际学者在线服务平台英文." 2021. Peking University 2021. <https://www.oir.pku.edu.cn/gjxzzxfwpten/info/1011/1072.htm>.

167 Jeyaretnam, Miranda. 2025. "China Tries to Woo STEM Talent with New K Visa as Trump Tightens H-1B: What to Know." TIME. Time. October 2025. <https://time.com/7322223/china-k-visa-tech-stem-immigration-h1b-fee-trump-explainer/>.

168 Ibid.

169 Ibid.

170 Proclamation No. 10043, "Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China," Federal Register 85, no. 106 (June 1, 2020): 34353–34355; National Security Presidential Memorandum 33, "United States Government-Supported Research and Development National Security Policy," January 14, 2021; CHIPS and Science Act of 2022, Pub. L. No. 117-167, 136 Stat. 1366 (2022).

171 "From Innovation to Weaponization." <https://content.striderintel.com/wp-content/uploads/2025/09/From-Innovation-to-Weaponization.pdf>.

172 "From Ph.D. To PLA." 2025. Select Committee on the CCP. September 19, 2025. <https://chinaselectcommittee.house.gov/media/reports/from-phd-to-pla>.

173 "CCP on the Quad: How American Taxpayers and Universities Fund the CCP's Advanced Military and Technological Research." 2024. Select Committee on the CCP. September 23, 2024. <https://selectcommitteeontheccp.house.gov/media/reports/ccp-quad-how-american-taxpayers-and-universities-fund-ccps-advanced-military-and>.

;"Joint Institutes, Divided Loyalties." 2025. Select Committee on the CCP. September 11, 2025. <https://chinaselectcommittee.house.gov/media/reports/joint-institutes-divided-loyalties>.

174 Ibid.

- 175 Saul, Stephanie, and Steven Rich. 2025. "How Harvard's Ties to China Helped Make It a White House Target." The New York Times, July 7, 2025. <https://www.nytimes.com/2025/07/07/us/harvard-china-white-house-funding.html>.
- 176 "Fox in the Henhouse." 2025. Select Committee on the CCP. September 5, 2025. <https://chinaselectcommittee.house.gov/media/reports/fox-in-the-henhouse>.
- 177 Tiffert, Glenn. 2020. "Global Engagement: Rethinking Risk in the Research Enterprise." Hoover Institution. July 30, 2020. <https://www.hoover.org/global-engagement-rethinking-risk-research-enterprise>.
- 178 Chen, Shu-Ching Jean. 2018. "These Are the Faces behind China's Video Surveillance Tech." ForbesIndia.com. ForbesIndia. April 3, 2018. <https://www.forbesindia.com/article/cross-border/these-are-the-faces-behind-chinas-video-surveillance-tech/49845/1>.
- 179 "Interview with Dr. Zhou Xi: Cloudwalk | Synced." 2017. Synced | AI Technology & Industry Review. April 5, 2017. <https://syncedreview.com/2017/04/05/interview-with-dr-zhou-xi-cloudwalk/>.
- 180 "Treasury Identifies Eight Chinese Tech Firms as Part of the Chinese Military-Industrial Complex." 2021. U.S. Department of the Treasury. December 16, 2021. <https://home.treasury.gov/news/press-releases/jy0538>.
- 181 Ibid
- 182 Gibson, Jean Philippe. 2017. "Inquisitr News." Inquisitr News. December 12, 2017. <https://www.inquisitr.com/dragonfly-eye-artificial-intelligence-machine-can-identify-2-billion-people-in-seconds>.
- 183 Cheung, Sunny. 2024. "Scientist at Forefront of US Army Research Selected to Lead PRC's Strategic Chip Production Line - Jamestown." Jamestown.org. August 8, 2024. <https://jamestown.org/scientist-at-forefront-of-us-army-research-selected-to-lead-prcs-strategic-chip-production-line/>.
- 184 "Wide Bandgap Semiconductor Laboratory." 2024. Archive.ph. August 5, 2024. <https://archive.ph/G6QRc#Research>.
- 185 John Honovich, "Hikvision Exec Shiliang Pu Is PRC Ministry of Public Security (MPS) Leader," IPVM, April 27, 2016, <https://ipvm.com/reports/hikvision-cetc-mps>
- 186 Harvey, Adam. "Exposing.ai: Duke MTMC." Exposing.ai. https://exposing.ai/duke_mtmc/.
- 187 Council on Foreign Relations. 2020. "Assessing China's Digital Silk Road Initiative." Council on Foreign Relations. 2020. <https://www.cfr.org/china-digital-silk-road/>.
- 188 Ibid; Cheney, Clayton. 2019. "China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism." Council on Foreign Relations. September 26, 2019. <https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political>.
- 189 Feldstein, Steven. 2020. "Testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Strategic Aims in Africa." https://www.uscc.gov/sites/default/files/Feldstein_Testimony.pdf.
- 190 Ibid.
- 191 Ibid.
- 192 Jili, Bulelani. 2022. "China's Surveillance Ecosystem and the Global Spread of Its Tools." Atlantic Council. October 17, 2022. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/>.
- 193 Bartholomew, Carolyn. 2020. "China and 5G | Issues in Science and Technology." Issues in Science and Technology. February 24, 2020. <https://issues.org/china-and-5g/>.

- 194 Woodruff, Judy, and Nick Schifrin. 2019. "Chinese Tech Makes Cities 'Smart,' but Critics Say It Spreads Authoritarianism." PBS NewsHour. October 1, 2019. <https://www.pbs.org/newshour/show/is-this-chinese-technology-a-trojan-horse-for-spreading-authoritarianism>.
- 195 Council on Foreign Relations. 2020. "Assessing China's Digital Silk Road Initiative." Council on Foreign Relations. 2020. <https://www.cfr.org/china-digital-silk-road/>.
- 196 Ibid.
- 197 Feldstein, Steven. 2020. "Testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Strategic Aims in Africa." https://www.uscc.gov/sites/default/files/Feldstein_Testimony.pdf.
- 198 Warner, Jason, and Toyosi Ajibade. 2024. "China's Smart Cities in Africa: Should the United States Be Concerned?" Csis.org. October 18, 2024. <https://www.csis.org/analysis/chinas-smart-cities-africa-should-united-states-be-concerned>.
- 199 Bartholomew, Carolyn. 2020. "China and 5G | Issues in Science and Technology." Issues in Science and Technology. February 24, 2020. <https://issues.org/china-and-5g/>.
- 200 Ibid.
- 201 Council on Foreign Relations. 2020. "Assessing China's Digital Silk Road Initiative." Council on Foreign Relations. 2020. <https://www.cfr.org/china-digital-silk-road/>.
- 202 Bartholomew, Carolyn. 2020. "China and 5G | Issues in Science and Technology." Issues in Science and Technology. February 24, 2020. <https://issues.org/china-and-5g/>.
- 203 Ibid.
- 204 Council on Foreign Relations. 2020. "Assessing China's Digital Silk Road Initiative." Council on Foreign Relations. 2020. <https://www.cfr.org/china-digital-silk-road/>.
- 205 "The Impact of China's National and Cyber Security Laws on Global Encryption - DataLocker Inc." 2024. DataLocker Inc. October 3, 2024. <https://datalocker.com/blog/the-impact-of-chinas-national-and-cyber-security-laws-on-global-encryption/>.
- 206 Segal, Adam. 2020. "China's Alternative Cyber Governance Regime Hearing on a 'China Model?' Beijing's Promotion of Alternative Global Norms and Standards." https://www.uscc.gov/sites/default/files/testimonies/March%202013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf.
- 207 Ruser, Nathan, and Samantha Hoffman. 2019. "Mapping More of China's Tech Giants: AI and Surveillance." Australian Strategic Policy Institute (ASPI). November 28, 2019. <https://www.aspi.org.au/report/mapping-more-chinas-tech-giants/>.
- 208 Jili, Bulelani. 2022. "China's Surveillance Ecosystem and the Global Spread of Its Tools." Atlantic Council. October 17, 2022. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/>.
- 209 Bartholomew, Carolyn. 2020. "China and 5G | Issues in Science and Technology." Issues in Science and Technology. February 24, 2020. <https://issues.org/china-and-5g/>.
- 210 Ibid.
- 211 Ibid.
- 212 Ingram, Ruth. 2023. "Uyghurs in Afghanistan Fear Taliban Buying Huawei Surveillance Tech." The China Project. October 19, 2023. <https://thechinaproject.com/2023/10/19/uyghurs-in-afghanistan-fear-taliban-buying-huawei-surveillance-tech/>.
- 213 Ibid.
- 214 Cave, Danielle. 2021. "Mapping China's Tech Giants | Australian Strategic Policy Institute." Mapping China's Tech Giants | Australian Strategic Policy Institute. 2021. <https://chinatechmap.aspi.org.au/#/map/f2-Huawei>.

- 215 Zhou, Viola. 2025. "Banned in the U.S. And Europe, Huawei Aims for the Developing World's AI." Rest of World. September 18, 2025. <https://restofworld.org/2025/huawei-us-ban-ai-cloud/>.
- 216 Uyghur Human Rights Policy Act of 2020, Pub. L. No. 116-145, 134 Stat. 648 (2020).
- 217 Ibid.
- 218 U.S. Department of Commerce, Bureau of Industry and Security, "Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification," Federal Register 87, no. 197 (October 13, 2022): 62186–62240.
- 219 Executive Order No. 14032, "Addressing the Threat From Securities Investments That Finance Certain Companies of the People's Republic of China," Federal Register 86, no. 105 (June 3, 2021): 30145–30150.; U.S. Department of Commerce, Bureau of Industry and Security, "Addition of Certain Entities to the Entity List," Federal Register 84, no. 196 (October 9, 2019): 54002–54017.
- 220 Garance Burke, Dake Kang, and Byron Tau, "U.S. Government Allowed and Even Helped U.S. Firms Sell Tech Used for Surveillance in China, AP Finds," Associated Press, October 29, 2025, <https://apnews.com/article/chinese-surveillance-silicon-valley-trump-administration-congress-21c5f961b1fd22f9a9e563ebe64e5582>
- 221 U.S. Congress, House, Uyghur Forced Labor Prevention Act, H.R. 6256, 117th Cong., Congressional Record 167, no. 217 (December 14, 2021): H7877 (passed 428-1).; U.S. Congress, Senate, Uyghur Forced Labor Prevention Act, S. 65, 117th Cong., Congressional Record 167, no. 219 (December 16, 2021): S9356 (passed by unanimous consent).
- 222 NVIDIA Corporation, Form 8-K: Current Report, April 9, 2025, U.S. Securities and Exchange Commission, <https://www.sec.gov/Archives/edgar/data/1045810/000104581025000082/nvda-20250409.htm>.
- 223 Flacks, Marti, and Madeleine Songy. The Uyghur Forced Labor Prevention Act Goes into Effect. Center for Strategic and International Studies, June 27, 2022. <https://www.csis.org/analysis/uyghur-forced-labor-prevention-act-goes-effect>.
- 224 Uyghur Forced Labor Prevention Act, Pub. L. No. 117-78, 135 Stat. 1525 (2021).
- 225 Section 307 and Imports Produced by Forced Labor. Congressional Research Service, Library of Congress, updated 2025. <https://www.congress.gov/crs-product/IF11360>.
- 226 Satariano, Adam. "Has the U.S. Campaign Against Uyghur Forced Labor Been Successful?" Foreign Policy, August 21, 2023. <https://foreignpolicy.com/2023/08/21/china-us-forced-labor-uyghur-xinjiang-uflpa/>.
- 227 Murphy, Laura T., and Charlotte Tate. Assessing the Impact of the Uyghur Forced Labor Prevention Act After Three Years. Center for Strategic and International Studies, August 29, 2025. <https://www.csis.org/analysis/assessing-impact-uyghur-forced-labor-prevention-act-after-three-years>.
- 228 Uyghur Forced Labor Prevention Act: Overview and Implementation. Congressional Research Service, updated 2025. <https://www.congress.gov/crs-product/R48642>.
- 229 Reuters. "Nvidia May Be Forced to Shift Out Some Countries After New U.S. Export Curbs," October 17, 2023. <https://www.reuters.com/technology/nvidia-may-be-forced-shift-out-some-countries-after-new-us-export-curbs-2023-10-17/>.
- 230 Uyghur Forced Labor Prevention Act: Overview and Implementation. Congressional Research Service, updated 2025. <https://www.congress.gov/crs-product/R48642>.
- 231 Lindblom, Charles E. The Science of "Muddling Through." Public Administration Review 19, no. 2 (1959): 79–88.

- 232 Lawrence Berkeley National Laboratory. Export Control Considerations for Entities on the BIS Entity List. <https://exportcontrol.lbl.gov/training/export-control-considerations-for-entities-on-bis-entity-list/>.
- 233 Additions to the Entity List; Amendment to Confirm Basis for Adding Certain Entities to the Entity List, 88 Fed. Reg. 2023-06663 (March 30, 2023). <https://www.federalregister.gov/documents/2023/03/30/2023-06663/additions-to-the-entity-list-amendment-to-confirm-basis-for-adding-certain-entities-to-the-entity>.
- 234 National Bureau of Statistics of China. “Press Release,” February 28, 2024. https://www.stats.gov.cn/english/PressRelease/202402/t20240228_1947918.html
- 235 ASML. EUV Lithography Systems. ASML. Accessed December 16, 2025. <https://www.asml.com/en/products/euv-lithography-systems>.
- 236 Solís, Mireya, and Mathieu Duchâtel. “The Renaissance of the Japanese Semiconductor Industry.” Brookings Institution, June 3, 2024. <https://www.brookings.edu/articles/the-renaissance-of-the-japanese-semiconductor-industry/>.
- 237 Council on Foreign Relations. “The Consequences of Exporting Nvidia’s H200 Chips to China.” Council on Foreign Relations. <https://www.cfr.org/expert-brief/consequences-exporting-nvidias-h200-chips-china>
- 238 Cornell Law School, Legal Information Institute. “International Traffic in Arms Regulations (ITAR).” Wex Legal Dictionary / Encyclopedia. https://www.law.cornell.edu/wex/international_traffic_in_arms_regulations_itar
- 239 U.S. Department of Commerce, Bureau of Industry and Security. “Guidance on End-User and End-Use Controls and U.S. Person Controls.” Bureau of Industry and Security. <https://www.bis.gov/licensing/guidance-on-end-user-and-end-use-controls-and-us-person-controls>.
- 240 U.S. Department of the Treasury, Office of Foreign Assets Control. Sanctions List. <https://sanctionssearch.ofac.treas.gov/>
- 241 Addressing the Threat from Securities Investments That Finance Certain Companies of the People’s Republic of China, 86 Fed. Reg. 30507 (June 7, 2021). U.S. Federal Register. <https://www.federalregister.gov/documents/2021/06/07/2021-12019/addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples>
- 242 U.S. Department of Commerce, Bureau of Industry and Security. Penalties. <https://www.bis.gov/enforcement/penalties>
- 243 U.S. Congress. Remote Access Security Act, H.R. 2683, 119th Cong., introduced in House (2025). <https://www.congress.gov/bill/119th-congress/house-bill/2683>
- 244 U.S. Congress. Export Control Reform Act of 2018, H.R. 5040, 115th Cong., introduced in House February 15, 2018. <https://www.congress.gov/bill/115th-congress/house-bill/5040>
- 245 Internal Revenue Service. Rev. Rul. 2003-29, 2003-1 C.B. Washington, DC: IRS. <https://www.irs.gov/pub/irs-drop/rr-03-29.pdf>
- 246 Human Rights Watch. “China: Alarming New Surveillance, Security in Tibet.” Human Rights Watch, March 20, 2013. <https://www.hrw.org/news/2013/03/20/china-alarming-new-surveillance-security-tibet>
- 247 TABLE Media. “Hong Kong: 56,000 More CCTV Cameras by 2028.” TABLE Media. <https://table.media/en/china/news-en/hong-kong-56000-more-cctv-cameras-by-2028>.
- 248 Foundation for Defense of Democracies. “Iran Seeks Purchase of Advanced Spy Satellites from China.” FDD, August 19, 2024. <https://www.fdd.org/analysis/2024/08/19/iran-seeks-purchase-of-advanced-spy-satellites-from-china/>
- 249 Center for Strategic and International Studies. “China’s Smart Cities in Africa: What Should the United States Be Concerned About?” CSIS. <https://www.csis.org/analysis/chinas-smart-cities-africa-should-united-states-be-concerned>