Corporate Complicity Scorecard

An Assessment of U.S. Companies' Exposure to Military Modernization, Surveillance, and Human Rights Violations in the People's Republic of China

Nathan Picarsic and Emily de La Bruyère
Founders, Horizon Advisory

With contributions and peer review by
Dr. Adrian Zenz
Senior Fellow in China Studies
Victims of Communism Memorial Foundation

VICTIMS OF COMMUNISM MEMORIAL FOUNDATION

HORIZON ADVISORY

VICTIMS OF COMMUNISM
MEMORIAL FOUNDATION

HORIZON ADVISORY

ACKNOWLEDGMENTS

The authors would like to thank the Victims of Communism Memorial Foundation (VOC) for their support and partnership on this project, and especially Dr. Adrian Zenz, VOC's Senior Fellow in China Studies, for his contributions to this report's findings and thoughtful peer review of the manuscript.

DISCLAIMERS

This report was prepared as part of a joint and independently funded project between the Victims of Communism Memorial Foundation and Horizon Advisory. The report was prepared in accordance with a rigorous internal and external review process to ensure its objectivity. Collection of information in an area where companies are not particularly transparent about their activities is a laborious undertaking, and every effort was made to ensure statements were supported from public sources deemed to be reliable, including citations to those sources contained in over 300 footnotes. Both western and Chinese sources were consulted. Any corrections or updates that may be required will be posted on https://victimsofcommunism.org/publication/corporate-complicity-scorecard/. Lastly, there are numerous U.S. laws and international agreements which govern business activity with and in the People's Republic of China. Nothing in this report should be construed to be an allegation of a violation of such laws or agreements.

Table of Contents

Executive Summary

The US private sector increasingly finds itself at the heart of US-China geopolitical tension. In their endeavor to capture Chinese markets and boost their bottom lines, American corporations have increasingly supported Beijing's military modernization, surveillance state, domestic securitization, and attendant human rights violations. As a result of this growing dependency, some corporations engage in political lobbying in the US in ways that ultimately serves Beijing's interests while potentially undermining the values and principles that undergird the western democratic order.

Until now, scrutiny of US industrial actors' complicity with problematic actions of the Chinese state has been scattered and *ad hoc*, without comprehensive or comparative assessments across players. This report fills this important gap: it presents broad-ranging assessments of the nature of American corporations' involvement in China, and then grades them based on a transparent and replicable new methodology.

This research does not assume that doing business in China is inherently wrong. However, support for Beijing's military modernization, surveillance state, and human rights violations may contradict professed corporate ethics, mislead consumers, and risk violating relevant laws in the US and elsewhere. Many US companies began their relationships with China well before China revealed itself as an aggressive international player. Companies which do substantial business with China need to reassess their role—not just the benefit they receive, but the degree to which they could be said to facilitate China's abusive domestic and international policies.

Based on both existing and new research findings, the report seeks to systematically put together all the pieces of a company's involvement in China and assigns each a grade from A to F. Each company profile represents an examination that is much more comprehensive than what has been published to-date and turns the findings into a grade that allows readers to compare how they perform.

The authors reviewed eight well-known firms—Amazon, Apple, Dell, Facebook, GE, Google, Intel, and Microsoft—for potentially problematic linkages that may directly or indirectly support China's state surveillance, military modernization, and human rights violations. Hundreds of primary and secondary sources were fed into 12 indicator categories related to operations and partnerships, leading to a final grade. While the development of such a transparent rating methodology is the key innovation of this report, it also features a substantial number of previously unreported facts.

The research findings are wide-ranging and invite further scrutiny of how US companies' engagement with China relate to US-sanctioned Chinese entities such as the Xinjiang Construction and Production Corps as well as US laws such as the US Trafficking Victims Protection Act. Overall, this project aims to inspire the development of new best practices for US industry. Rather than merely condemning the US private sector, the report develops a grading scorecard system in order to incentivize corporations to equally promote freedoms and rights everywhere.

Introduction

The US private sector increasingly finds itself at the heart of US-China geopolitical tension.[1] For decades American corporations—including major industrial players—have sought to capture not only US but also Chinese markets and political favor. In doing so, they have in many cases traded support for Beijing's military modernization, surveillance state, and human rights violations in exchange for access to China's market. In an environment where the private sector is the leading global source of innovation, capital, and influence, the stakes of this Faustian bargain are enormous.

This risk is increasingly recognized. Scrutiny of the ties between US industry and the Chinese Communist Party (CCP) has grown alongside attention to the normative, economic, and security threat of Beijing's global authoritarianism. *The New York Times* has investigated Apple's data localization program in China and the privacy risks it raises; the *Wall Street Journal* has covered Chinese propaganda on Facebook; and industry-specific media such as *The Information* increasingly document ties between US companies and human rights abusers in China.[2]

However, scrutiny of US corporate ties to China has tended to be *ad hoc*, without comprehensive or comparative assessments across players. This project seeks to begin filling that gap. It seeks to survey and assess major US technology firms' exposure to China's military, surveillance state, and human rights abuses in a uniform and replicable fashion, so that its analysis can be extended and inspire development of improved best practices for US industry.

The report examines and grades eight major US companies—Amazon, Apple, Dell Facebook, GE, Google, Intel, and Microsoft—on their exposure to China's military modernization, surveillance state, domestic securitization, and human rights violations. It leverages both secondary sources and newly collected, primary source Chinese-language material, accounting for direct operational ties as well as indirect partnerships. This project does not assume that doing business in China is inherently wrong. It does however assume that support for Beijing's military modernization, surveillance state, and human rights abuses is problematic, and that corporate leaders must recognize as much. This project finds that such support takes five primary forms:

Offshoring of manufacturing that exposes US industrial chains to forced labor and other human rights atrocities in China: For example, both *Dell* and *GE* maintain offices in Xinjiang, the site of the CCP's ongoing genocide against the Uyghur minority.[3] They do so despite increasing public awareness of the risks of such operations, as well as clear business advisories from the US State Department counseling that businesses not operate in or have supply chains dependent upon Xinjiang.

Offshoring of innovation, in partnership with Chinese government, surveillance, and military players that risks granting those players access to sensitive technologies: For example, *Dell* and *Intel* have established joint laboratories with the Chinese Academy of Sciences Institute of Automation, a leading Chinese government research entity that develops state and military surveillance technologies.[4] Those laboratories focus on surveillance-relevant technologies, such as biometric recognition and intelligent perception.

Partnerships and engagements with Chinese government entities that support military—and surveillance-relevant systems: For example, *Amazon*, *Dell*, *GE*, and *Microsoft* have all partnered with Chinese government entities to support China's smart city development. Smart cities are widely recognized as a core part of the CCP's surveillance program, domestically and internationally.[5]

Compliance with Beijing's regulatory system that makes US industry a conduit for the Chinese government's problematic information collection: For example, *Apple's* data storage and security protocols in China have been reported to potentially put user data at risk of CCP access.[6]

Dependencies on the Chinese market that make US industry a conduit for Chinese influence and propaganda abroad: For example, Chinese government entities spread disinformation about Beijing's human rights atrocities in Xinjiang via *Facebook* advertisements. *Apple* has reportedly lobbied to limit provisions of the Uyghur Forced Labor Prevention Act, a bill since passed into law that bans US imports of goods made in Xinjiang due to forced labor concerns.[7]

Several key themes emerged from this project's analysis that exemplify the problematic aspects of the profiled corporations' involvement in China:

- **TWO-FACED**: US corporate players have no problem saying one thing in the United States while doing (and saying) something different in China. Such hypocrisy is particularly flagrant when it comes to digital privacy: Companies like *Apple*, *Amazon*, *Dell*, and *Intel* that stress information security in the US also abide by Chinese regulatory requirements for storing and handling data. This jeopardizes the information, and therefore security, of users in China who oppose the regime, as well as of global users.

- **EMPOWERING A STRATEGIC COMPETITOR**: As the established story has it, US companies' involvement with China has hollowed out US industrial capacity. This project finds that major US companies *also* offshore research and development (R&D), in both legacy and emerging business sectors. This threatens to hollow out America's innovation edge as well.

- **KILLING WITH A BORROWED SWORD**: Key players in the US defense industrial base partner with Chinese government and military-tied partners—including in innovation and advanced technology—in explicitly military-relevant domains. These US players include legacy actors like *GE*, *Dell*, and *Microsoft* as well as emerging defense vendors like *Amazon*.

- **BRIGHT SPOTS**: While every company reviewed in this initial set has some degree of exposure to and risk of supporting Beijing's problematic activities, two stand out as relatively less dependent and exposed: *Facebook* and *Google*.

A selection of the most potentially problematic company-specific anecdotes from this project that have not previously been reported in coverage of these eight industrial champions includes:

- *Dell* and *GE* appear to have offices in the Xinjiang Uyghur Autonomous Region that risk contributing to Beijing's mass surveillance and internment campaign overseen by the US-sanctioned paramilitary colonial entity Xinjiang Production and Construction Corps (XPCC).

- *Amazon*, *Dell*, *GE*, and *Microsoft* all support China's smart city development. Smart cities are a core part of both the CCP's intrusive domestic surveillance program and that program's global proliferation.

- *Dell* operates an artificial intelligence and computing architectures laboratory in partnership with the state-run Chinese Academy of Sciences Institute of Automation (CASIA), which specializes in developing surveillance technologies for the Chinese government and that could potentially be used to oppress Uyghurs in Xinjiang.

- *Amazon* operates at least six innovation centers in China in partnership with Chinese companies, including a state-controlled firm bankrolled by China Telecom, an entity the US Department of Defense has identified as a

military company. These centers likely result in significant transfer of technology and know-how that may be enabling China's surveillance state and military capability at home and abroad.

- *Intel* co-invests in, supplies, and engages in technological cooperation with a Chinese high-performance processor and integrated chip design company called Lanqi Technology (Montage Technology) alongside China Electronics Corporation (CEC), a state-owned defense conglomerate that the US Department of Defense has identified as a military entity.

- *Apple* and *Intel* leadership have met multiple times with top brass at the Ministry of Industry and Information Technology (MIIT), a leading Chinese state entity charged with implementing Beijing's military-civil fusion strategy, which channels technological innovations developed or acquired in the private sector toward the Chinese military.

The project's objective is to advance a transparent, replicable corporate grading system that can be extended and inspire the development of new best practices for US industry to proactively protect against identified risks. The goal is not to condemn the US private sector, but rather to inspire action to defend US corporate, US national, and global interests, grounded in the rights-based values and principles that undergird the liberal democratic order. Industry is the backbone of America. It should be incentivized to uphold those principles, not to fuel Beijing's adversarial geopolitical offensive.

Methodology

Just as this project urges transparency from American businesses operating in China, it seeks to display transparency in the methodology by which it assesses those companies. In this way, readers can evaluate for themselves the significance of the grades assessed.

Subject Companies

This project's initial installment has reviewed eight corporations:

- **Amazon** (Amazon.com, Inc.)
- **Apple** (Apple Inc.)
- **Dell** (Dell Inc.)
- **Facebook** (Meta Platforms, Inc.)
- **GE** (General Electric Company)
- **Google** (Alphabet Inc.)
- **Intel** (Intel Corporation)
- **Microsoft** (Microsoft Corporation)

Companies were selected for analysis based on a potential impact assessment informed by two criteria: Company size in terms of market capitalization, and operational alignment with CCP industrial priorities (e.g., Strategic Emerging Industry domains).

Grading Overview

Companies reviewed in this effort are graded on the familiar A-to-F scale. Generation of grades proceeded in two steps.

- First, companies were reviewed against a set of binary tests that generate an "auto-fail" result (e.g., if the company appears to operate a facility in Xinjiang).

- Second, the aggregate grade is determined by assessment of exposure in two primary dimensions: Operations and Partnerships. Those categories are separated in order to capture both direct and indirect exposures. Scores in these two categories are averaged to produce a company grade on the A-to-F spectrum.

"Operations" refers to the nature of companies' activities in the Chinese market and their direct ties to noted risk factors (e.g., China's military, surveillance, and human rights abuses). For example, does a company share information with the Chinese government, or censor information for the Chinese government? Does the company's technology or capital support military-relevant Chinese programs? Does the company lobby the US government to prevent competitive industrial policy *vis-à-vis* China?

"Partnerships" refers to the nature of a companies' partners in China and their indirect ties to noted risk factors (e.g., China's military, surveillance, human rights abuses) and the influence that these relationships have in China and abroad. For example, does the company source goods from suppliers associated with forced labor risks?[8] Has it formed strategic cooperation agreements with Chinese military companies?

Importantly, this distinction helps identify *where* exposure to a risk indicator takes place, not *what* that indicator is. For example, technology transfer to the military could fall within either Operations (e.g., if undertaken at the US company's operation in China) or Partnerships (e.g., if undertaken in the interactions between the US company's Chinese strategic partner and the Chinese military).

Data Sources

To assess exposure in those categories, this report uses the best available public data. It surveys existing secondary source analyses of profiled company operations in China, as well as original primary-source material. Primary-source collection for this project included extensive identification of the reviewed actors' strategic partnerships and supply-chain relationships in China. Source materials range from company filings to Chinese-language press coverage to Chinese central, provincial, and municipal government documents.

Scoring Rubric

Companies have been scored on two dimensions: Operations and Partnerships. The aggregate grade assigned to a company is an average of those two scores. In cases where a grade average falls between two letter grades, the average is rounded down to the nearest whole letter.

Those scores in turn are measured based on a series of variables that begin with binary, "auto-fail" tests and move into relative scoring of both quantitative and qualitative material.

Auto-Fail Tests

As outlined in the chart below, companies receive automatic failing grades for Operations or Partnerships with exposure to risk indicators in six criteria areas: the genocide of the Uyghur ethnic minority (e.g., via operations in Xinjiang); support for entities designated by the US government or international regulatory bodies as human rights, surveillance, or security threats (three criteria); and lobbying the US government to counteract China-specific human rights legislation.

Binary Test Chart

Indicator	Sources
Operations in Xinjiang	Company filings; Business registries; Baidu maps; Secondary reporting
Direct Indicators of Forced Labor	Company filings; Central, provincial, municipal government subsidies and announcements re: transfer of labor; Secondary reporting
Direct Support to Military or State Security	Company filings; Counterparty company filings; Primary press coverage and secondary reporting
Active Support to Designated Surveillance/Threat Actors	Sanction Listings; Company filings; Counterparty company filings; Primary press coverage and secondary reporting
Lobbying on China-specific Human Rights Legislation	Company filings; Lobbying disclosures; Secondary reporting

Of the eight companies reviewed, four engaged in activities that prompted auto-fail grades.

Company Auto-Fail Grades (red indicates activities that prompted auto-fail grades)

Indicator	Amazon	Apple	Dell	Facebook	GE	Google	Intel	Microsoft
Operations in Xinjiang								
Direct Indicators of Forced Labor								
Direct Support to Military or State Security								
Active Support to Designated Surveillance/ Threat Actors								
Lobbying on China-specific Human Rights Legislation								

Aggregate Grading

The eight companies were next assessed on two non-binary aggregate metrics, one for Operations and one for Partnerships. Each aggregate metric is based on six input indicators with three possible values: positive (0.33), neutral (0.00), and negative (-0.33). For each indicator, a positive value reflects *no finding* of evidence of problematic operations or partnerships and confirmation of policies and practices intended to prohibit and prevent such linkages. A neutral value reflects a) a balance of positive and negative findings, b) uncertainty over the relationship between rhetorical policies and corporate practices, or c) null findings. A negative value reflects documented exposure, whether directly (in the operations category) or indirectly (in the partnerships category), to China's military modernization, surveillance state, or human rights abuses. The category score for Operations or for Partnerships is the sum of the six component variables, conveyed as a total number score that can range from 2 to negative 2. That aggregate sum corresponds to an Operations or Partnership letter grade as follows.

Aggregate Grading (from 2 to negative 2)

Input Aggregate	Grade
2	A
1	B
0	C
-1	D
-2	F

Breakdown and Explanation of Indicators

Operations category scores are based on an assessment of six input metrics. Where uncertainty remains over a given input metric, it is scored as neutral. Otherwise, determinants of positive, neutral, and negative input scores are itemized as follows:

Indicators	Positive Score	Neutral Score	Negative Score
Subsidiaries	A positive score would feature no subsidiaries in China operating in the security, military, surveillance, or military-civil fusion sectors, as well as documented corporate policy and practice that would defend against operating in those fields.	A neutral score would feature subsidiaries operating in China in sectors under the umbrella of military-civil fusion, but not explicitly military, and with documented corporate policy and practice that ensure guardrails against potential support for China's military or surveillance apparatus.	A negative score would feature subsidiaries operating in China in sectors under the umbrella of military-civil fusion sectors but *without* documented corporate policy and practice that protects against potential support for China's military or surveillance apparatus *and/or* subsidiaries operating in China in the security, military, or surveillance sectors.
Investments	A positive score would feature no investments in Chinese entities in the public security, military, surveillance, or military-civil fusion sectors or those engaged in human rights abuses, as well as documented corporate policy and practice that monitor corporate investments to protect against human rights, military, and surveillance risks.	A neutral score would feature investments into Chinese entities in fields relevant to military-civil fusion—but not explicitly military—paired with documented corporate policy and practice to protect against human rights, military, and surveillance risks.	A negative score would feature investments into entities in the security, surveillance, or military-civil fusion sectors in China without documented corporate policy and practice protecting against human rights, military, and surveillance risks.
Data, information, research, and innovation centers	A positive score would feature no data, information, research, or innovation facilities in China and documented corporate policy and practice that actively protects corporate data from Chinese government access.	A neutral score would feature no data, information, research, or innovation facilities in China, but without documented corporate policy and practice that actively protects corporate data from Chinese government access.	A negative score would feature data, information, research, or innovation facilities operated in China and compliance with the Chinese government data policy regime that makes those vulnerable to government access or influence.
Compliance with Chinese data regimes, domestic or extra-territorial, that grant the Chinese government access to or influence over cross-border data flows and content controls.	A positive score would feature documented corporate policy and practice opposed to the Chinese government data policy regime, domestic and extra-territorial, and its applicability to foreign and cross-border data flows.	A neutral score would feature no declaratory policy or practice.	A negative score would feature active compliance with the Chinese government data policy regime's extra-territorial application and/or related content controls.
Direct customer relationships with official Chinese government and military entities.	A positive score would feature no direct customer relationships with Chinese government or military entities that might grant them access to resources (e.g., technology, legitimacy, information) able to bolster the CCP's military or surveillance system and documented corporate policy and practice protecting against such ties.	A neutral score would feature no direct customer relationships with Chinese government or military entities that might grant them access to resources (e.g., technology, legitimacy, information) able to bolster the CCP's military or surveillance system, but also no documented protections against indirect exposure to Chinese government or threat actor customers.	A negative score would feature direct customer relationships with Chinese government or military entities that might grant them access to resources (e.g., technology, legitimacy, information) able to bolster the CCP's military or surveillance system.
Participation in official fora of the Chinese Communist Party and Chinese government that help boost Chinese government propaganda, legitimacy, and influence on global narratives.	A positive score would feature no participation in official CCP and Chinese government narrative events, dialogues, or discourses as well as documented corporate policy and practice that opposes CCP and Chinese government propaganda and influence operations in China and abroad.	A neutral score would feature limited participation (e.g., individual attendance rather than corporate attendance, sponsorship, or advertised keynote participation) in official CCP and Chinese government narrative events, dialogues, or discourses in China or abroad.	A negative score would feature corporate attendance, sponsorship, or advertised keynote participation in official CCP and Chinese government narrative events, dialogues, and discourses in China or abroad.

Partnerships category scores are based on an assessment of six input metrics that feed into a letter-graded score. As in the Operations category, Partnerships input metrics are assessed on a positive-neutral-negative spectrum. Instances with uncertainty or limited information are scored as neutral. Otherwise, determinants of positive, neutral, and negative input scores are itemized as follows:

Indicators	Positive Score	Neutral Score	Negative Score
Interactions with Chinese government officials	A positive score would feature no interactions with Chinese Communist Party or Chinese government officials with mandates associated with human rights abuses, non-market economic behaviors, or military modernization.	A neutral score would feature limited official interactions with Chinese government officials and organs with mandates associated with human rights abuses, non-market economic behaviors, or military modernization.	A negative score would feature significant and frequent interactions with Chinese government officials or organs that carry explicit mandates associated with human rights, security, or surveillance risks.
Strategic partnerships with Chinese government and designated academic and commercial players that carry human rights, security, and surveillance risks.	A positive score would feature *no active* strategic partnerships with Chinese actors implicated in human rights, security, or surveillance activities.	A neutral score would feature *only past* strategic partnerships that have been terminated with Chinese actors implicated in human rights, security, or surveillance activities.	A negative score would feature *active* strategic partnerships with Chinese actors implicated in human rights, security, or surveillance activities.
Research partnerships with Chinese government, academic, and designated commercial players that carry human rights, security, and surveillance risks.	A positive score would feature corporate policy and practice that explicitly protects against and vets to prevent direct collaborative research with entities associated with human rights, security, and surveillance risk in the Chinese research ecosystem.	A neutral score would feature only past research relationships that have been terminated with entities associated with human rights, security, and surveillance risks in the Chinese research ecosystem.	A negative score would feature active research partnerships with entities associated with human rights, security, and surveillance risks in the Chinese research ecosystem.
Supply chain exposure to forced labor risk	A positive score would feature no connections to forced labor risk indicators in a company's supply chain in China as well as documented corporate policy and practice that vets vendors for direct and indirect exposure to forced labor indicators.	A neutral score would feature no connections to forced labor risk indicators, but also no explicit corporate policy and practice that vets vendors for direct and indirect exposure to forced labor indicators.	A negative score would feature connections to forced labor risk indicators either directly or indirectly with no declaratory mitigation measures.
Supply chain exposure to security and surveillance risk	A positive score would feature no connections to documented security and surveillance risks throughout a company's supply chain in China, as well as documented corporate policy and practice that vets vendors for direct and indirect exposure to security and surveillance risks throughout a supply chain.	A neutral score would feature no connections to security and surveillance risks, but also no explicit corporate policy and practice that vets vendors for direct and indirect exposure to security and surveillance risks throughout a supply chain.	A negative score would feature connections to documented security and surveillance risks in a company's supply chain.
Additional partnership ties to sectors relevant to military-civil fusion in China where such partnerships might legitimize China's security and surveillance apparatus, as well as its human rights abuses.	A positive score would feature corporate policy and practice that actively vets for and mitigates against partnerships that might legitimize China's security and surveillance apparatus, as well as its human rights abuses.	A neutral score would feature no active support or endorsement that constitutes a legitimizing force for China's security and surveillance apparatus, as well as its human rights abuses but no explicit corporate policy or practice protecting against such support or endorsement.	A negative score would feature active partnerships that serve to legitimize China's security and surveillance apparatus as well as its human rights abuses.

Auto-fail companies can, at best, receive a D grade based on their Operations and Partnerships scores. Those companies that do not register an auto-fail can score anywhere from A to F in both categories. The average of those two scores yields the company's overall grade. Companies that auto-fail any of the binary tests may still receive a D (rather than an F) if they also obtain either an Operations and Partnerships category score of C or above.

It is important to note that none of these variables assume that doing business in China or with Chinese partners is inherently negative. Rather, these variables isolate—and attempt to quantify in a relative fashion—the negative externalities associated with human rights, surveillance, and security risks present in the Chinese business ecosystem. Those risks stem from the Chinese Communist Party's and Chinese government's industrial policy program, which has been documented to disenfranchise and abuse minority groups and to undermine individual human rights, proliferate surveillance protocols that violate international norms, and fuel the fusion of civilian and military research and production to benefit the modernization of the People's Liberation Army.

International businesses, including those reviewed in this effort, bear responsibility to institute policies that protect against complicity with problematic aspects of the Chinese business environment by adopting and implementing widely recognized corporate social responsibility (CSR) and environmental, social and corporate governance (ESG) standards, as well as relevant US laws and government "business advisory" notices. Pleading ignorance is no longer an option. Failure to develop a robust approach to protecting against such risks through appropriate CSR/ESG policies and other measuers increases the risk of supporting malign behavior of what is increasingly recognized as an authoritarian and even criminal state.[9]

Summary Findings

This initial report provides profiles of eight companies assessed according to the above methodology. Their final grades are as follows:

Company Grades

Amazon	Apple	Dell	Facebook	GE	Google	Intel	Microsoft
D	D	F	B	F	B	F	F

Four of the companies failed at least one of the five binary "auto-fail" tests concerning their ties to China, resulting in four F grades.

Binary Auto-Fail Tests (red indicates activities that prompted auto-fail grades)

Indicator	Amazon	Apple	Dell	Facebook	GE	Google	Intel	Microsoft
Operations in Xinjiang								
Direct Indicators of Forced Labor								
Direct Support to Military or State Security								
Active Support to Designated Surveillance/ Threat Actors								
Lobbying on China-specific Human Rights Legislation								

Following these binary tests, all companies were scored against a set of separate Operations and Partnerships criteria, yielding two input metric grades that were averaged to calculate each company's final grade.

Company Final Grades

	Amazon	Apple	Dell	Facebook	GE	Google	Intel	Microsoft
Binary Tests	PASS	PASS	FAIL	PASS	FAIL	PASS	FAIL	FAIL
Operations	D	C	F	B	D	B	F	F
Partnerships	D	D	D	B	F	B	F	D
Overall Grade	**D**	**D**	**F**	**B**	**F**	**B**	**F**	**F**

A breakdown of the scoring input indicators is detailed in the charts that follow.

Legend	
Red	negative score (-0.33)
Yellow	neutral score (0.00)
Green	positive score (0.33)

Operations Grades

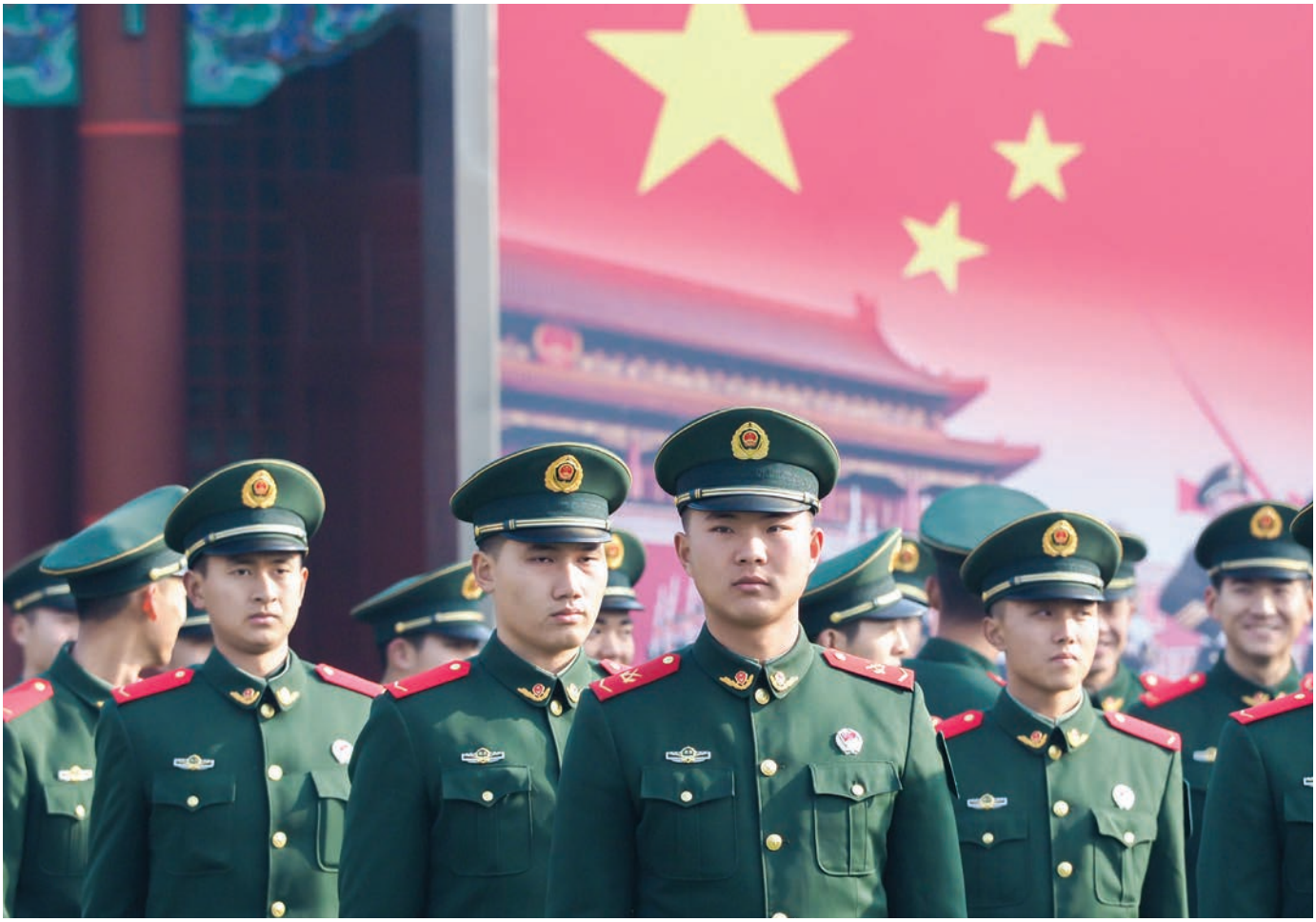
Indicator	Amazon	Apple	Dell	Facebook	GE	Google	Intel	Microsoft
Subsidiaries	0	0	-0.33	0	-0.33	0	-0.33	-0.33
Investments	0	0	-0.33	0.33	-0.33	0	-0.33	-0.33
Centers	-0.33	-0.33	-0.33	0.33	0.33	0.33	0	-0.33
Data and content controls	-0.33	-0.33	-0.33	0	0	0	-0.33	-0.33
Customers	0	0	-0.33	-0.33	-0.33	0	-0.33	-0.33
Narrative	-0.33	0	-0.33	0	-0.33	0	-0.33	-0.33
Total numeric score	-1	-0.66	-2	0.33	-1	0.33	-1.66	-2
Grade	**D**	**C**	**F**	**B**	**D**	**B**	**F**	**F**

Partnerships Grades

Criteria	Amazon	Apple	Dell	Facebook	GE	Google	Intel	Microsoft
Interaction with government	0	-0.33	-0.33	0	-0.33	0.33	-0.33	-0.33
Strategic partnerships	0	0	-0.33	0	-0.33	0.33	-0.33	-0.33
Research partnerships	-0.33	0	-0.33	0	-0.33	0	-0.33	0
Forced labor exposure	-0.33	-0.33	-0.33	0	0	0	0	-0.33
Security/surveillance exposure	-0.33	-0.33	-0.33	0	-0.33	0	-0.33	-0.33
Legitimizing endorsements	0	-0.33	-0.33	0.33	-0.33	-0.33	-0.33	-0.33
Total numeric score	-1	-1	-2	0.33	-1.66	0.33	-1.66	-1.66
Grade	**D**	**D**	**F**	**B**	**F**	**B**	**F**	**F**

The evidence collected and analyzed to produce these company-specific assessments ranged from corporate records and primary-source Chinese government documents and media reports to secondary analyses that have been assessed, to the best of the project's ability, for their credibility and relevance to this project's aggregate scoring methodology. The company profiles that follow provide a narrative justifying the indicator values determined for each of the reviewed companies, with references and citations to the determinative behaviors and relationships that have informed company grades. The profiles are not formulaic. Rather, they are meant to provide context and validation for the determinations outlined in the company grades.

The profiles are also meant to convey the need to develop a new framework for corporations doing business in China. Companies should recognize the operational and reputational risks associated with engagement with the Chinese government and its state-driven industrial system, even when their engagement seems limited to the private sector. US investors must also recognize these risks and internalize them as they consider the long-term prospects of companies with significant exposure to China and the CCP. And US consumers should vote with their purchases.



Amazon

In 2014, Amazon (China) Investment Co., Ltd.—a China-based Amazon subsidiary—signed a memorandum of understanding (MoU) with the Shanghai Free Trade Zone and Shanghai Information Investment Co. The three parties agreed to develop a cross-border e-commerce platform, designed to fuel the internationalization efforts of Chinese e-commerce companies in the free trade zone (FTZ). Amazon committed to assist its two partners in developing channels for Chinese products to reach overseas markets, as well as to build the Amazon China International Trade Headquarters in the FTZ.[10] Shanghai Information Investment is a state-owned entity invested in by China Telecom, which the US Department of Defense (DoD) more recently has identified as tied to the Chinese military.

Four years later, the same year that Amazon announced it was closing its e-commerce business in China, Amazon launched another partnership with the Shanghai government.[11] In 2018, Amazon Web Services (AWS) joined with the Shanghai Municipal Commission of Economy and Information, Jing'an District Government, and Shibei High-Tech Park to launch the Shanghai-AWS Joint Innovation Center (SHA-JIC).[12] SHA-JIC, part of a larger network of Amazon innovation centers in China, supports local start-ups, including players with ties to Beijing's military-civil fusion program. The center offers technological support as well as Amazon AWS resources. Focused on smart cities, big data, and cloud computing, the SHA-JIC describes itself as "an international technology innovation platform built under the guidance and with the support of the Shanghai Economic and Information Commission and the Jing'an District Government." [13]

The SHA-JIC draws on a similar set of partnerships to those behind the Shanghai FTZ cooperation. The center is operated by Shanghai Tuneful Cloud Computing Technology Co., Ltd (Shanghai Tongfu), which is majority-owned by Chinese government-backed Shanghai North High Tech Co. and Shanghai Information Investment Co—the same company with which Amazon signed the 2014 MoU, and which is invested in by China Telecom Corporation.[14]

The smart city, big data, and cloud computing technologies that SHA-JIC supports have direct applications to Chinese domestic and international military and surveillance programs. And there is evidence to suggest that the companies with which SHA-JIC partners contribute to China's military-civil fusion and surveillance programs. SHA-JIC's "settled" companies have included, among others, Silong Intelligence.[15] Silong Intelligence's website describes it as "committed to the customized R&D, integration, and service of command systems and smart community management and control systems in the field of public safety and emergency rescue in China."[16] Products on its website include "portable face-recognition forensics" that "can quickly import the image data of fugitives/key personnel from the Ministry of Public Security, collect face photos in concealment, and input them into the comparison system in real time to identify and compare data" and that "can be widely used in public security, national security, customs, major security activities, and other government agencies."[17] Silong's products also include a "mobile multi-channel face recognition system" for front-line police officers and guard patrols as well as a "mobile multi-channel video feature forensics system" designed to analyze public security footage in support of "public security, criminal investigation, anti-terrorism, intelligence" and other applications.[18]

SHA-JIC's broader network of relationships suggests additional exposure to the Chinese government, military, and surveillance apparatus. For example, SHA-JIC's "co-construction and implementation units"[19] include the Shanghai Data Exchange Center (SDEC), a state-owned data project supervised and guided by national ministries and commissions as well as the Shanghai Municipal Government.[20] The SDEC describes itself as promoting the large-scale aggregation of data across the government and commercial domains, data services and circulation built on top of that aggregation, and data interconnection and cooperation across regions.[21] SDEC's backers are primarily state-owned or state-supported actors.[22] They include China Telecom, China Electronics Corporation, and China United Network Communications Group.[23] DoD has identified all three as tied to the Chinese military. SDEC has also cooperated or engaged in dialogues with the Chongqing Municipal Public Security Bureau, Municipal Party Committee Propaganda Department, and Municipal Party Committee Cyberspace Affairs Office on data security;[24] with the Social Credit Promotion Division of the Shanghai Development and Reform Commission (SDRC) on data aggregation and monitoring, and applications to urban management and public safety;[25] and with the United Front Work Department of the Shanghai Municipal Party Committee.[26] These are Chinese government, security, and surveillance entities. Their mandates cover the China's social credit system, the surveillance state underlying it, and the dissemination of Chinese propaganda at home and abroad.[27]

Amazon AWS also appears to partner with SDEC.[28] In June 2019, the AWS Global Vice President visited the SDEC. There he discussed strengthening exchange and cooperation between AWS and the SDEC, as well as plans for AWS to provide the center with cloud service support.[29]

Despite having closed its e-commerce business in 2019, Amazon AWS maintains an extensive technological footprint in China, with ties to Beijing's military-civil fusion and surveillance systems. Amazon has expanded that footprint over the past five years, even as tensions between the US and China escalate and the risks of Beijing's technology-enabled authoritarianism have become increasingly evident. Amazon also relies heavily on China-based production, including production exposed to forced labor risks. This profile seeks to map Amazon's Chinese production footprint, as well as particularly glaring cases of potential forced labor exposure in Amazon's supply chain, focusing on:

- Amazon's network of six innovation centers, including SHA-JIC, in China and their ties to Beijing's military and surveillance programs;
- Amazon's data centers in China, launched in conjunction with Chinese government entities and co-located with military and military-civil fusion actors; and
- Exposure to forced labor in Amazon's supply chain.

Amazon receives a D for its operations in China: Through a network of innovation centers and the Chinese business of Amazon's cloud offerings, Amazon supports the cultivation of China's military and surveillance systems and the innovation underlying those. Amazon receives a D for its partnerships in China: The company has a myriad of exposures to the CCP's forced labor regime.

Supporting Chinese Government Information Architectures

Innovation Centers

Amazon Web Services (AWS) maintains a network of six innovation centers and at least two data centers in China. These have been launched in partnership with Chinese government and government-backed entities. They also bring Amazon into direct interaction with Chinese government, military, and domestic surveillance entities, and serve as a channel for technological and informational support to them.[30]

The first of Amazon's joint innovation centers, the Qingdao-Amazon AWS Joint Innovation Center, was launched in March 2017. The center was jointly established by the Qingdao Licang District People's Government, Amazon Connect Technology Services (Beijing) Co., Ltd,[31] and Qingdao Wanguo Cloud Business Internet Industry Co., Ltd.[32] Press coverage at the

Amazon Web Services expo in China, 2018. Image Credit: ImagineChinaLimited/Alamy Stock Photo.

time explained that its goal was to "cultivate and support local start-ups and transport them overseas," including through technology cooperation with foreign players; to help foreign start-ups open up the market in China; and "with the help of AWS's experience…to help traditional Qingdao enterprises realize Internet transformation."[33] It was projected that by 2021, the center would incubate a total of 750 start-ups and upgrade 120 traditional companies.[34]

The innovation center model was quickly replicated. In 2018, Amazon and the Xi'an Municipal Government and Xi'an Management Committee of Chanba Ecological District launched the Xi'an-AWS Joint Innovation Center.[35] In 2019, Amazon partnered with the Nanjing Municipal Government and Jiangning District to launch the Nanjing-AWS Joint Innovation Center.[36] The same year, Amazon established the SHA-JIC with the Shanghai Municipal Commission of Economy and Information, Jing'an District Government, and Shibei High-Tech Park.[37] In 2020, Amazon and the Chengdu High-Tech Industrial Development Zone set up the Chengdu-AWS Joint Innovation Center.[38]

These centers have been launched in partnership with Chinese government entities. They are operated, in part or in full, by Chinese commercial entities. They seek the same goals as the first, Xi'an innovation center: to support Chinese start-ups, with capital and technological support, and to connect them with overseas players and financial resources. Accordingly, the centers offer a range of types of support. The joint innovation centers also provide additional programming, including road shows, talent training, and "demo days" to incubated companies as well as the broader Chinese innovation ecosystem.[39]

These innovation centers also expose Amazon to, and provide a channel for support of, China's military-civil fusion and surveillance ecosystem. This is evident in the already-discussed example of SHA-JIC and Silong Intelligence.

Data Centers

Amazon AWS has also established at least two data centers in China. These are operated by local partners, seemingly in accordance with Chinese regulations forbidding foreign companies from owning or operating specific technologies or providing cloud services.[40] These data centers risk exposing Amazon's technology or data to the Chinese military and surveillance programs—albeit less directly than do the innovation centers—both because they involve compliance with China's digital regulatory regime and because they are subordinate to or operate in partnership with Chinese government and military-linked entities.

Take, for example, Amazon's data center in the Zhongwei Industrial Park. AWS launched the center in 2015, through a cooperation agreement with the Ningxia government.[41] A 2019 article on the Zhongwei City People's Government Portal suggests that Amazon is developing the second phase of that project.[42] The local government and Party Committee appear to have been engaged in the construction of the data center, including through visits to observe and discuss development.[43]

The Zhongwei Industrial Park hosts a number of other data center and cloud projects belonging to Chinese government and military entities. China Mobile and China Unicom, which the US DoD has identified as connected to the PLA, have data centers in the same industrial park.[44] The industrial park also cooperates with the China Meteorological Administration and the China Resources Satellite Application Center (CRESDA).[45] The China Meteorological Administration, an entity operating under the State Council, is connected to China's military and military-civil fusion apparatus.[46] CRESDA is a part of the state-owned China Aerospace Science and Technology Group,[47] a company designated as affiliated with the Chinese military by the US Department of Defense.[48] Amazon's local operating partner for this data center—Ningxia West Cloud Data Technology Co., Ltd—supports the Zhongwei Municipal Government in developing data projects, likely including these, in the industrial park.[49]

Military Company Partnerships

Over the past decade, Amazon has also directly formed partnerships with Chinese military companies. In 2013, Amazon and China Telecom established a strategic partnership.[50] The next year, Amazon and China Unicom established a strategic partnership in 4G telecommunications.[51] And in 2017, Amazon and China Mobile signed a strategic cooperation memorandum. In doing so, they discussed cooperation in Shanghai's smart city construction.[52]

In 2019 AWS invited leadership from Beijing Aerospace Long March Science and Technology to the company's technology summit in Beijing. Representatives from the two companies discussed AI, big data, and architecture design. China's government portal for military-civil fusion news noted that "by participating in this technical summit…. Beijing Aerospace Long March Science and Technology Information Institute technical staff were able to deepen their knowledge of computing, enhance informatization construction capabilities…and provide a strong foundation for the continued advancement of aerospace+ work."[53]

Exposure to Forced Labor Indicators

Amazon sources a broad array of apparel, home furnishings, and electronics from hundreds of Chinese producers for its expansive e-commerce operation. Amazon's 2019 list of Amazon Basics suppliers revealed that almost half (487) were based in China.[54] Chinese production introduces risk of direct and indirect exposure to forced labor and to the industrial policy system and players that perpetuate abuses related to genocide in Xinjiang.

A 2019 report by the Australian Foreign Policy Institute (ASPI) identified Amazon among 83 major foreign and Chinese companies that are potentially benefiting from "the use of Uyghur workers outside Xinjiang through abusive labor transfer programs," namely through Amazon's supply relationship with O-Film.[55] In response to the ASPI report, Amazon released a statement confirming that the offending suppliers were removed from their supply chain.[56] But one external group that tracks these companies on their actions (or non-action) to eradicate forced labor from textile and apparel supply chains has listed Amazon among those companies "that have not taken all credible steps" to prevent the risk of supply chain exposure to the forced labor campaign in Xinjiang.[57]

Amazon's supply chains outside of Xinjiang have also been criticized for exposure to inhumane working conditions. In 2019, it was reported that Amazon Alexa production facilities managed by Foxconn violated labor regulations concerning young workers.[58] It was suggested at the time that some young workers worked 10 hours a day, six days a week, in violation of labor laws.[59] Foxconn claimed these roles "provid[ed] students…with the opportunity to gain practical work experience."[60]

Apple

In 2019, Apple launched the construction of its second data center in China, this one in Ulanqab, Inner Mongolia.[61] This choice of location was likely informed by regional Chinese industrial policies in the region that prioritize the digital sector. Huawei set up shop in the same area for the same reasons.[62] At the groundbreaking ceremony for Apple's Ulanqab facility, a representative from Apple participated and delivered remarks. So did Han Jun, a deputy secretary of the Ulanqab Municipal Party Committee and United Front Work Minister.[63] United Front Work refers to CCP efforts to disseminate Chinese propaganda and expand the Party's influence, domestically and internationally, to and through the co-optation of non-party entities.[64]

Several weeks after the ground-breaking ceremony, a different type of risk surfaced in the neighborhood. On April 27th of 2019, the Ulanqab Human Resources Development Company and the Labor and Employment Bureau of Jining District hosted a job fair targeting "poor labor" and "transferring employment" for poor families.[65] The Ulanqab People's Government would subsequently report in February 2021 that its goals for the year ahead included the "transfer" of 1,600 "rural laborers."[66] In other regions of China that, like Inner Mongolia, have significant ethnic minority populations (e.g., Tibet, Xinjiang), such transfer of labor programs could be interpreted as red flags for exposure to forced labor risks. While such risk is less established in the case of Inner Mongolia than in Uyghur regions of Xinjiang, it should still be considered.

Apple's operations in China have been the subject of significant public concern in recent years. Its data storage and censorship practices were the subject of a wide-ranging *New York Times* investigation in 2021; both *The Information* and the Australian Strategic Policy Institute have raised alarms over forced labor indicators in Apple's supply chain.[67] As those cases suggest, Apple—which relies on China for almost half of its production and seeks to sell in the Chinese market—faces both upstream and downstream exposure to risk factors within the Chinese system, including:

- Data compromises with the CCP: Exposing data to CCP access, censoring, content at the CCP's behest, granting Chinese government requests for customer data, and hosting applications that allow the CCP government to track the Chinese population;
- Indicators of forced labor in China-based supply chains; and
- Engagement in elite fora that increase the legitimacy and "discourse power" of Beijing's digital system abroad.

Activities on such fronts constitute normative and security risks. However, Apple's ties to the Chinese government, its human rights abuses, and its military and surveillance systems are not outsized in comparison to other companies surveyed in this report, despite the widespread public attention to them.

Apple receives a C for its China operations grade based on compliance with data and censorship regimes in the Chinese market that might grant the Chinese government access to user information—even as Apple positions itself as a vocal advocate for privacy. The company does not score worse because, unlike other companies surveyed in this report, no evidence suggests that Apple is outright sharing technology or information with known Chinese bad actors (e.g., military players). Apple also appears to advocate in other markets, including in the United States, in a manner consistent with Chinese preferences and inconsistent with the defense of human rights.

Apple receives a D in its partnerships because of forced labor risks throughout its supply chain as well as extensive cooperation at an elite level with the Chinese government that helps to legitimize Beijing's global technological ambitions.

Poisoned Fruit: Collaboration with the Chinese Government's Data Regime

In 2020, 42 percent of Apple's manufactured products were produced in China.[68] And China represents not only one of Apple's largest markets, but also one of its fastest growing: In Q1 2021, Apple reported 87 percent year-over-year growth in Greater China.[69] Apple appears intent on securing a strong position in the Chinese market, and on guaranteeing reliable Chinese production. This has forced, or at least led, the company to cooperate with Beijing's coercive information regime—including censoring apps on the app stores at Beijing's request and localizing data in China according to practices that risk granting the Chinese government access to personal information.

In 2017, China passed a data law requiring that all personal information collected in China be stored in China. In January 2018, Apple responded by transferring its iCloud services to a Chinese company, state-owned Guizhou-Cloud Big Data (GCBD). "In other words," explained Chinese media, "Guizhou-Cloud Big Data will be responsible for the operation of iCloud in mainland China and will have legal and financial relationships with iCloud users in mainland China."[70] In addition, Apple began the process of setting up data centers in China to store information—the first in Guiyang, the second in Inner Mongolia.[71]

In an interview with *People's Daily* about the changes, Apple reportedly said that "we hope to be transparent to customers."[72] A 2021 *New York Times* investigation suggested otherwise. That report found that "in its data centers, Apple's compromises have made it nearly impossible for the company to stop the Chinese government from gaining access to the emails, photos, documents, contacts and locations of millions of Chinese residents." Those compromises include providing Apple's state-owned operating partner in China the encryption keys for private data in Apple's iCloud service and granting GCBD employees control over the servers on which data is stored.[73]

Apple appears to have exposure to risks of content control, as well as information access, related to the Chinese government. Censorship of Apple-managed platforms in China seems to be a viable risk: A popular Quran app, for example, was removed from the Apple App Store "because it includes content that requires additional documentation from Chinese authorities."[74] According to Apple's self-published transparency figures, the company complied with more than 95 percent of requests from the Chinese government for customer data between July and December 2019.[75]

Those are cases of Apple seemingly restricting information on behalf of the Chinese government. The reverse dynamic is also a risk: Apple may enable dissemination of information platforms that can support Chinese government surveillance efforts. For example, Chinese Police Network reports that in 2020, Bayingoleng Mongolian Autonomous Prefecture Government in Xinjiang launched an app called Smart Eye Fraud.[76] The app is described on Chinese sites as in the Apple environment and downloadable from the App store.[77]

Apple's IT-related research and development (R&D) efforts in China may also contribute to China's military-civil fusion

Tim Cook, CEO of Apple Inc., speaks during the opening ceremony for the China Development Forum 2019 in Beijing, China. Image credit: Imaginechina Limited / Alamy Stock Photo.

program. In 2018, Apple announced a joint research center at Tsinghua University focused on machine learning and computer vision, unveiled as the Joint Research Center for Intelligent Mobile Technology of Tsinghua University.[78] Given the nature of Beijing's interest in the dual-use relevance of artificial intelligence and related fields—as well as the Chinese government's ties to the university research ecosystem—this type of commercial R&D is at risk of transfer to military-relevant actors in China. In fact, Chinese sources explicitly connect intelligent mobile technology to military applications. A 2017 article in *China News* headlined "China autonomous and controllable mobile phone operating system will take the road of military-civil fusion" describes the establishment of the China (Zhongguancun) Intelligent Terminal Operating System Industry Alliance's military-civil fusion professional committee, and the relevance of the technology to China's military program. "For a long time," explains the article, "many member units of China (Zhongguancun) Intelligent Terminal Operating System Industry Alliance have actively participated in important national, party, government and military projects."[79]

Elite Capture

Apple has reportedly lobbied to limit certain provisions in proposals for American policies intended to counteract China's domestic human rights abuses, such as the Uyghur Forced Labor Prevention Act.[80] At the same time, Apple's leadership contributes to a range of Chinese-organized fora meant to elevate Beijing's global image and add a gloss of business legitimacy to the CCP's narrative about its international technological ambitions. Participation in such fora is, for many, considered business as usual. It is by no means necessarily motivated by ambitions to support China's authoritarian agenda. However, the Chinese government organizes these events in order to burnish its global image and claim legitimacy, internationally, for its global economic and technological agenda. A player with the global weight of Apple should take that into account in its framing of business as usual.

Apple's Tim Cook has met multiple times with top brass at the Ministry of Industry and Information Technology (MIIT), a

leading Chinese government entity charged with implementing Beijing's military-civil fusion strategy.[81] At a 2016 meeting, the MIIT Minister, Miao Wei, praised the "extensive cooperation" between Apple and Chinese industry, and expressed hope that "Apple will further expand its business in China, deepen R&D and industrial chain cooperation, and provide Chinese consumers with a convenient and safe user experience."[82]

In 2017, Apple's Tim Cook delivered a keynote speech at the World Internet Conference in China, hosted by the Cyberspace Administration of China (CAC) and Zhejiang Provincial People's Government.[83] The conference was dedicated to promoting the Chinese "way" of the internet. Other notable companies participating included Microsoft, IBM, China Telecom, China Electronics Technology Group, Huawei, and Qihoo 360.[84]

In 2021, Cook returned to China to attend the Chinese Development Conference. Organized by the Development Research Center of the State Council, the conference's focus is encouraging elite interactions around the topic of the future of China's economy. The theme of the 2021 session was "China on a New Journey Toward Modernization." Other attendees included business and investment luminaries like Elon Musk of Tesla and Ray Dalio of Bridgewater Associates.[85] This was the second time Cook had attended the conference; he co-chaired it in 2018. Notably, at that session he advocated for stronger privacy regulation.[86]

These examples are largely consistent with business as usual for American corporates engaged in China. Apple's role is representative rather than anomalous. However, there are real-world implications and consequences that, arguably, a company with Apple's clout has a responsibility to guard against: its participation lends legitimacy and international influence to Beijing's efforts to shape a problematic emerging digital system.

In addition, Apple's reported domestic lobbying efforts in the US also could stymy a normative response: Apple reportedly lobbied to limit provisions of the Uyghur Forced Labor Prevention Act, a bill that passed in December 2021 and bans imports of goods tied to forced labor in Xinjiang.[87]

Far From the Tree: Apple's Chinese Partnerships

A host of sources have found significant exposure to forced labor in Apple's supply chain. A 2019 report by the Australian Strategic Policy Institute (ASPI) identified indicators of forced labor associated with four Apple suppliers in China: O-Film, Foxconn, Hubei Yihong, and Fuying Photoelectric Co., Ltd.[88] Apple's 2020 supplier list also included Goertek Inc., a leading Chinese electro-acoustic device manufacturer.[89] ASPI has identified Goertek's supply chain as potentially exposed to forced labor risks.[90] Goertek also does business with Huawei, has close ties to the Chinese government, and receives significant government subsidies. [91] Goertek operates military-civil fusion projects in China, including the Beihang Qingdao Research Institute, which has a dedicated center for military-civil fusion, as well as others for virtual reality, microelectronics, precision instruments, and optoelectronics.[92]

According to the World Uyghur Congress and reporting conducted by *The Information*, an additional seven companies in Apple's supply chain feature indicators of participation in forced labor programs.[93]

Having such an extensive list of suppliers that have reported connections to a range of indicators of forced labor is problematic. It features both direct and indirect exposure to the atrocities that the CCP inflicts upon its minority populations. And this proximity to forced labor indicators suggests a deficiency in supply-chain vetting that sharply contrasts with Apple's self-proclaimed ambition to serve as a positive influence in the world.

Dell

SCORECARD

F

In July 2020, China's state-owned Xinhua News Agency broadcast Dell's "new product conference" across China.[94] At the event, Dell showcased its product portfolios in edge computing, data centers, and cloud computing. Dell also shared, according to Xinhua, its "unswerving support for the Chinese government's policies and close following of the government's strategic development direction."[95] According to a Xinhua News account of remarks by the President of Dell China, he said that "for more than 20 years, Dell has always been a firm supporter and executor in the process of the Chinese government's economic development. Dell … has used practical actions to support the country's strategic decision making."[96] To underline the point, the conference coincided with the joint publication of a Dell-Chinese Academy of Sciences (CAS) book on next-generation digital architectures.[97]

CAS is the Chinese government's national academy for natural sciences. It also contributes to Beijing's military and surveillance programs. Dell is a Texas-headquartered American multinational that is also an active US government contractor.[98]

Yet Chinese media describes Dell as a "foreign-owned local enterprise."[99] Dell's leadership in China agrees: Dell leadership has described Dell as "a real 'local enterprise'" in China "that has "achieved local research and development, local production, and local services."[100] Seventy-five percent of Dell's global production capacity and 85 percent of its supply chain are in China.[101] In 2017, Dell's annual procurement from China totaled approximately 35 billion USD.[102] In January 2021, Dell's Sohu Account reported that Dell had provided, directly or indirectly, one million employment opportunities in China, adding that "Dell Technology Group has truly fulfilled the social responsibility of a brand enterprise."[103]

In other words, Dell is deeply enmeshed in the Chinese industrial and government system. This engagement comes at a price. **Dell supports Chinese government entities developing Beijing's national surveillance programs and cutting-edge data tools. Dell also partners with the Chinese military-civil fusion apparatus. And Dell's extensive supply chain in China is riddled with indicators of forced labor, at the same time as Dell maintains a regional office in Urumqi, Xinjiang.** The account that follows is intended to illuminate only the most glaring examples that the project was able to uncover of Dell's contributions to Chinese government, military, and surveillance programs, as well as exposure to indicators of human rights abuses. Dell's extensive footprint, partnerships, and investments in China suggest there may be more examples not yet uncoverd. Examples of such problematic activity found by this project include:

- Dell has assisted some of China's leading government institutions, including the Development Research Center of the State Council, in defining Beijing's industrial policy.

- Dell and the Chinese Academy of Sciences's Institute of Automation (CASIA) have a joint laboratory dedicated to AI and cloud computing. That laboratory focuses on research and applications of AI and new computing architectures in the field of brain information processes, in particular video big data, biometric recognition, and voice recognition. CASIA develops surveillance technologies for the Chinese government and supports the Chinese military. CASIA also has ties to the Chinese surveillance state's operations in Xinjiang.

- Dell's partners and suppliers in China are associated with indicators of exposure to forced labor, as well as of support for surveillance activities in Xinjiang.

Dell receives an F for operations because its ties to the Chinese government directly support the technologies and applications of a modern surveillance state. Dell receives an F for partnerships for similar reasons, as well as because of human rights exposures in its value chain. Past analyses have not found any suppliers with greater exposure to forced labor than Dell's value chain. Dell's footprint in Xinjiang raises additional red flags.

In China, For China

Dell established its first production base in China in 1998.[104] According to aggregated recent press coverage, today, the company operates eight research and development centers in China;[105] 32 global offices, including one in Xinjiang;[106] three manufacturing plants;[107] joint projects with 10 Chinese universities—thanks to which Dell has received the Chinese Ministry of Education's Best Partner Award;[108] and a host of other projects. Dell has committed to support China's Belt and Road Initiative (BRI),[109] the Internet+ national strategy,[110] and the Made in China 2025 program.[111] In 2015, Dell launched a new corporate strategy of "In China, For China," committing to help China's digital competitiveness, boost the development of new infrastructure, and advance China's digital transformation—and to invest 125 billion USD in China by 2020.[112] In 2018, Dell initiated a new phase of that strategy: Dell China 4.0+, oriented around fueling China's "Smart+" construction. The Dell China President cited localization of procurement and manufacturing in China as an example of this new phase of engagement bearing fruit.[113] As of January 2020 Dell's China R&D Group had applied for more than 1,400 Chinese and foreign patents.[114]

In developing this footprint, Dell has engaged extensively with core players in the Chinese government. This engagement extends to the highest levels of Chinese government: In 2018, Dell partnered with the State Council to produce an in-depth report on digital industrialization and China's industrial policy.[115] The report focused on China's ambitious Made in China 2025 program—and strengthening capabilities in emerging technologies , including cloud computing, big data, and artificial intelligence.[116] These technologies are relevant to China's military-civil fusion program. At the launch event, the President of Dell China declared that "Dell Technology Group is committed to becoming the most trusted partner of Chinese enterprises."[117] The State Council is the chief administrative authority of the People's Republic of China; Made in China 2025 and digital industrialization among Beijing's top priorities. In other words, Dell's localization in China has led it to support the industrial policy that Beijing sees as a core lever in today's geopolitical competition with the United States.

Dell and the Chinese Academy of Sciences

Dell is also directly involved in more explicitly problematic areas of Chinese government programming, including military modernization and surveillance. In 2016, Dell and the Chinese Academy of Science's Institute of Automation (CASIA) unveiled a joint laboratory, the AI and Advanced Computing Joint Laboratory.[118] That laboratory focuses on research and applications of AI and new computing architectures in the field of brain information processes, in particular video big data, biometric recognition, and voice recognition. At the unveiling, the President of Dell Greater China declared that via "cooperation with CASIA, we will combine computing resources and scientific research resources to promote the leapfrog development of AI to seize the commanding heights of the new round of scientific and technological revolution."[119]

CASIA develops surveillance technologies and applications for the Chinese government.[120] For example, between 2012 and 2016, the Institute undertook a project for the National 973 Program, the PRC's leading basic research program, on developing "Social Perception Data Processing for Public Safety."[121] As its official description puts it, the project was designed to "meet the major needs of national security… for social perception intelligence, [and] provide technical

Michael Dell, founder and chairman of Dell Inc., holds a news conference in Shanghai, China, on March 21, 2007.
Image Credit: REUTERS / Alamy Stock Photo.

support and decision-making support for real-time monitoring, early warning and forecasting, and emergency handling of public security."[122] CASIA's Intelligent Video Surveillance and Face Recognition Technology systems have been used in Chinese government security applications.[123] CASIA-linked surveillance systems have likely been deployed in Xinjiang: As early as 2007, a delegation from the Institute visited the Xinjiang Institute of Physics and Chemistry to discuss cooperation in "Xinjiang minority speech and language processing technology."[124]

In addition, CASIA contributes to China's military and military-civil fusion programs. The Institute runs dedicated military projects, evident and advertised in its hiring documents.[125] Examples of CASIA's past such projects include developing space cameras for the Shenzhou V and a vehicle-mounted ground illuminator detection system that won China's second prize for military scientific and technological progress.[126] CASIA also maintains a Military-Civil Fusion Innovation Center.[127]

The technologies, like biometric monitoring and voice recognition, on which the Dell-CASIA joint laboratory focuses are relevant to a range of potential surveillance and military applications. And the cooperation between Dell and CASIA appears to be ongoing. In 2016, the Dell-CASIA collaboration developed a deep learning computing and service platform, known as Zhuge Shenzhi.[128] In 2017, the two parties signed a tri-party agreement with SDIC Innovation to develop an AI solution service platform.[129] In 2020, *People's Daily*, a major Chinese state-owned newspaper, awarded the joint CASIA-Dell laboratory the title of "AI Industry Application Research Base" and reported on the launch of a new project, the "Intelligent Research Base Strategic Cooperation."[130]

The Dell partnership with CASIA also involves cooperation on standards development—a core part of China's international technological offensive.[131] For example, in 2020, CASIA, Dell China, and the China Computer Users Association jointly released a PRC standard on requirements and evaluation for AI computer vision specialists.[132]

Nor is CASIA the only Chinese Academy of Sciences entity with which Dell collaborates. A 2020 article in China's *Science and Technology Daily* reported that the Institute of Physics of CAS had adopted a Dell high-performance computing system based on Intel technologies for its Material Genomics Research Platform: "A few days ago, the Institute of Physics of the Chinese Academy of Sciences joined hands with Dell and Intel to build its Huairou material genome high-performance computing platform, which has attracted widespread attention in scientific research and industry." In an interview on the subject, a representative from the CAS Institute of Physics said that the Institute had "worked with Dell and Intel to build this high-performance computing platform."[133] China's high-performance computing ecosystem is a contributor to a range of military and military-civil fusion efforts, including in testing necessary for hypersonic and nuclear-armed weapons platforms.[134]

Dell and Local Governments

Dell also cooperates with local Chinese government entities. In 2015, Dell signed a memorandum of understanding with the with Guiyang Municipal Government, outlining partnership in big data and cloud computing as well as construction of cloud joint laboratories and intelligent manufacturing platforms.[135] The next year, the two companies signed an agreement to "deepen cooperation." Chinese media coverage of the event cited Dell reporting – and it is unclear whether this is paraphrasing or quoting – that, "as a company rooted in China for 21 years, Dell is committed to carrying out strategic cooperation with the Chinese government and local partners in the field of big data and cloud computing." The same coverage then quotes the President of Dell China saying, "the memorandum on deepening strategic cooperation signed this time reflects that Dell actively integrates into the local economy and fully supports and embraces the Internet+ national strategy."[136]

Also in 2016, Dell became a smart city government partner of Wuhou District in Chengdu and announced that it intended to invest more broadly in relevant technologies across Sichuan.[137] Dell also partners with other Chinese companies that support smart city development: For example, the 2019 IPO prospectus of Zhejiang Daily Interactive Network Company, which provides big data solutions for smart cities, listed Dell alongside Inspur and Huawei as a supplier.[138] China's smart city program is a core part of its domestic and international surveillance efforts.

Military-Civil Fusion

As the above example suggests, Dell's potential contributions to China's military and surveillance programs do not end with government ties. The company has also partnered with commercial entities that support those programs, including players that the US government has identified as bad actors. For example, as part of the launch of the "In China, For China" program in 2015, Dell signed a series of cooperation agreements with Chinese military-tied entities, including China Electronics Corporation, a state-owned conglomerate that the US Department of Defense (DoD) would later identify as tied to the Chinese military, and Tsinghua Tongfang, an information technology company that was placed on the US Department of Commerce's Entity List in 2021.[139] In 2019, Dell committed to a strategic partnership in 5G and Internet of Things technologies with China Unicom.[140] This was less than a year before DoD identified China Unicom as tied to the Chinese military. No public documentation found by this project suggests that any of these agreements has been terminated.

In 2016, Dell participated in China's International Science and Technology Expo, held in Sichuan Province. That event's theme was Science and Technology Innovation, Military-Civil Fusion, Open Cooperation. Chinese media described it as being held in service of "the national innovation-driven development and military-civil fusion strategy."[141]

At the 2021 China Cyber Information Security Summit, hosted by the China Information Association, Dell was awarded the title of "2020–2021 China Cyber Information Security Industry Innovative Enterprise." It was the only multinational company to receive this recognition.[142]

Human Rights Risks

Surveillance

A 2021 report from *Top10VPN* found that two Chinese companies that identify Dell as a partner have assisted in development of surveillance and censorship systems in China, including in Xinjiang.[143] **Xiamen Dragon Information Technology**, which reportedly describes Dell as a partner, is a public security information company. It has used a combination of facial recognition and "QQ" information to label and tag citizens as Uyghur, Han, or Tibetan. In addition, Dell and **Bluedon Information Security Technology** reportedly signed an agreement in 2017 in the context of Dell's China 4.0 Strategy, wherein Dell stated that it intended to draw on Bluedon's information security expertise. Bluedon's services include blocking of anti-censorship tools, as well as its Sharp Eyes (Xueliang) Project, a state-backed project aimed at achieving 100% surveillance coverage of China's public spaces.[144]

Forced Labor

In addition, a 2019 report by the Australian Strategic Policy Institute (ASPI) identified potential indicators of forced labor associated with at least three Chinese suppliers of Dell: Foxconn, Sichuan Mianyang Jingweida, and Hibroad Technology Co., Ltd.[145] Another Chinese company that the ASPI report identified as exposed to forced labor risks, Hefei Bitland, notes Dell, alongside Microsoft, as one of its partners on its website.[146]

The risks suggested by these reports are exacerbated, first, by the extent of Dell's supply relationships in China and, second, by Dell advertising operations in Xinjiang with an office in Urumqi, the capital of the Xinjiang Uyghur Autonomous Region (XUAR).[147]

Dell store in Tianjin, China. Image credit: Imaginechina Limited / Alamy Stock Photo.

Facebook

SCORECARD
B

In March 2021, China's state-owned Xinhua News Agency purchased, for under 100 USD, an ad on Facebook featuring a video of the mayor of Urumqi, the capital city of Xinjiang. In the video, the mayor declared that the "peace and stability that people from all ethnic groups in Xinjiang once longed for has become a reality." He also described a "plot" on the part of Western countries to smear China's reputation by fabricating stories of genocide.[148] That advertisement was seen some 200,000 times in two days. Last year, a Facebook ad purchased by state-owned CCTV featuring students in a Xinjiang boarding school describing themselves as well-fed and taken care of was shown over a million times in four days.[149] These are not isolated cases: In 2020, the Chinese government's messaging on Facebook about its treatment of ethnic minorities in Xinjiang hit a new high.[150]

Facebook is blocked in China. But that doesn't stop Beijing from using the platform as a propaganda channel to influence foreign audiences—and also, as *Wall Street Journal* reporting has documented, to track them. Three of the world's 20 most popular Facebook pages are run by Chinese state-controlled media outlets.[151] Facebook has also acknowledged the presence of China-based hacking accounts on its platform, used to disseminate malware that enables surveillance of journalists and dissidents overseas.[152]

Facebook has removed hacking accounts it was able to identify. And it removes Xinjiang-related ads when the advertisers violate current Facebook policies (e.g., not labeling them as relevant to social and political issues). Facebook does not appear to have instituted policies against ads purchased by Chinese government entities or their proxies—including ads concerning Xinjiang that may be channels for Chinese state propaganda—or publicly resolved to treat Chinese government entities on the platform any differently than it does other users.[153] It is possible that profit influences consideration of these risks: Facebook makes some 5 billion USD annually from advertisements sold in China.[154]

Blocked in China since 2009, Facebook's footprint in the country is minimal. Nonetheless, this project has found that:

- Facebook continues to sell ads in China, including to Chinese government entities, creating an international channel for Beijing's propaganda; and
- The one concrete physical product that Facebook does make, the Oculus headset, relies on Chinese suppliers with reported exposure to indicators of forced labor.

Facebook receives a B for operations. The company has a minimal presence in China and—despite a history of friendly overtures to the Chinese Communist Party (CCP)—has recently taken a firm, exemplary narrative stance *vis-à-vis* Beijing's authoritarian regime. Ad sales to Chinese government entities, and failure to limit their role on the platform, leave Facebook in a position as a channel for Beijing's international propaganda campaign.

Facebook receives a B for partnerships. The company's minimal footprint in China also translates to a limited network of partners in the country. However, Facebook's commercial partnerships around the Oculus headset expose it to indicators of forced labor risks.

It's Complicated

Facebook entered the Chinese market in 2005 under the domain facebook.cn. Four years later—following a sequence of anti-government uprisings in Xinjiang during which activists coordinated on the platform—the Chinese government blocked access to Facebook.[155] Instagram, which Facebook owns, was likewise blocked in 2014.[156]

Facebook has since tried, and for the most part failed, to re-enter the Chinese market. In 2015, Beijing authorities granted Facebook a three-month license to open offices in the city. These were never opened.[157] The next year, reports surfaced that Facebook had developed location-based censorship software through which it might be able to operate in the Chinese market. The software would suppress posts from news feeds within certain geographic areas—not through Facebooks' direct censorship, but rather through a third party, likely intended to be a China-based partner.[158] In 2018, Facebook announced that it would establish an Innovation Center in Hangzhou via a China-based subsidiary. However, Facebook failed to obtain final government approval for the operation. The innovation center did not open.[159]

Since 2018, Facebook leadership has begun to criticize the CCP, including its human rights abuses. At a Senate hearing in 2018 its chief operating officer, Sheryl Sandberg, said that China failed to meet Facebook's normative standards and it would not operate there; in 2019, CEO Mark Zuckerberg announced that Facebook would not establish a data center in China because the country violated privacy and free speech.[160]

Advertising Bonanza

However, while Facebook remains blocked in China, and although leadership has begun to take a hardline narrative stance against the CCP, the firm continues to operate a robust advertising business in China. In 2017, the company launched a China Advertising Partner Program. By the next year, revenue from ad purchases in China was estimated at 5 billion USD, about 10 percent of Facebook's total sales.[161] And Facebook appears to have continued to build out its ad business in China. In 2020, Facebook set up a new engineering team in Singapore reportedly to further develop its China advertising business, including by refining ad-buying tools for Chinese customers.[162]

Get in Where You Can

Facebook is primarily an internet platform company. However, it does have tangible products, of which one of the most well-known is its Oculus virtual reality headset. Facebook works with Chinese manufacturing to make that product: its primary Chinese manufacturing partner for the Oculus is Goertek Inc.,[163] a leading electro-acoustic device manufacturer that also does business with Huawei (a company sanctioned by the US government), has close ties to the Chinese government, and receives significant Chinese state subsidies.[164] Goertek also operates military-civil fusion projects in China, including the Beihang Qingdao Research Institute, which has a dedicated center for military-civil fusion, as well as others for virtual reality, microelectronics, precision instruments, and optoelectronics.[165] Cooperation with Facebook on the Oculus VR headset runs the risk of contributing to Goertek's efforts to develop military-relevant capabilities. Goertek's supply chain is also exposed to forced labor risks. A 2019 Australian Strategic Policy Institute report found that Hubei Yihong Manufacturing Co lists Goertek as one of its customers.[166] Hubei Yihong has received transferred Uyghur workers from Keriya County, Xinjiang, at its manufacturing center in Xianning, Hubei.[167]

GE

SCORECARD

F

"For GE, China is not only a market, but also an important part of GE's global supply chain and innovation base. As GE's global strategic market and its largest market outside of the United States, China's development is crucially important to GE's global development."

— Xiang Weiming, GE China CEO, 2020[168]

At the 2016 China International Aviation and Aerospace Expo, the Aviation Industry Corporation of China (AVIC) and General Electric Company (GE) won the "Joint Cooperation Award." They were commended for their "outstanding cooperation in promoting the development of China's civil aircraft avionics technology and industry"—most notably via their joint venture, Aviage Systems, a civil avionics systems solution provider.[169]

AVIC is one of China's largest aerospace and defense companies. The US Department of Defense (DoD) has identified it as tied to the People's Liberation Army (PLA). GE and AVIC inaugurated Aviage in 2012. Before the company had been formally launched, Aviage was selected by COMAC, another leading Chinese state-owned aerospace manufacturer, to provide core avionics systems, integrated services, and maintenance systems for the Chinese C919 airliner.[170] The DoD has also identified COMAC as tied to the PLA. Aviage's global headquarters are in the AVIC Civil Avionics Industrial Park. That park's press materials describe it as "relying on the agglomeration capabilities of AVIC in military-civilian fusion, innovation-driven, transformation and upgrading."[171]

The Aviage partnership—and the advanced aerospace technologies that Beijing has obtained through it—have been documented: A 2011 *New York Times* article wrote that "no Western company has been more aggressive in helping China pursue that [jet technology] dream" than GE. [172] After DoD identified AVIC as a military company in 2020, *Bloomberg* reported that the company's ties to GE were raising concerns in the United States.[173]

Even so, existing coverage risks understating the degree to which the Aviage case is representative, rather than anomalous, when it comes to GE's presence in China. This joint venture is just one of many partnerships GE has cultivated in China over the past two decades. Those partnerships appear to involve technology-sharing, including with core players in China's military, military-civil fusion, and surveillance system. Those partnerships have also granted military-tied Chinese players positions of leverage in GE's supply chains, critical to both America's national security and its manufacturing base. And GE's operations and partnerships in China systemically expose it to risks associated with forced labor and other human rights atrocities in the country. Moreover, GE continues to develop its presence in China, despite the increasingly clear security risks, normative dangers, and threats that Beijing's industrial ambitions pose to GE's core business interests. These lines of exposure are particularly troubling because GE is a major contractor for the US Department of Defense, including in technologies and products similar to those with which it partners with the Chinese military system.

This report does not seek to offer a comprehensive portrait of GE's presence in and partnerships with China. Instead, it focuses on certain illustrative examples that may only scratch the surface of GE's partners, technology cooperation, government ties, and exposure to human rights risks in China. These examples are intended to provide a representative picture of the *types* of exposure GE exhibits, and the implications of this for an American manufacturing company that is currently attempting to reinvent itself as a digital champion. Illustrative examples include:

- GE maintains a host of subsidiaries in China, as well as joint ventures with Chinese state-owned entities, that entail technology-sharing with Chinese military-tied actors in security-relevant fields.

- GE maintains innovation centers that put its technology at risk of use by the Chinese government and military, and has partnered with Chinese government-led entities to help them develop research hubs abroad through which they might acquire foreign technology.

- GE has collaborated with Chinese local government entities in developing smart cities, a core part of China's intrusive surveillance program.

- GE has an office in Xinjiang and partners with players implicated in China's human rights abuses in the region.

GE is often seen as a champion of American manufacturing. Yet it is perhaps more integrated into the Chinese system, including the Chinese government system, than any other major American company surveyed in this report.

GE receives a D in operations because of its extensive footprint in China that entails joint ventures and research projects with Chinese government and military actors, as well as entities tied to human rights abuses. While these operations are large, the technological and industrial capabilities that they involve—and that they risk providing to Chinese military and government actors—are less advanced than other companies profiled in this report. That reality is one of the few factors preventing a more aggressively failing grade.

GE receives an F in partnerships for similar reasons. Even if the specific projects GE undertakes in China are less technologically advanced, the players with which it partners are major contributors to China's military and surveillance programs.

Joint Ventures and Technology Sharing

GE's presence in China is extensive. The company has dozens of subsidiaries or joint ventures in China. At a first level, these underline the degree to which GE has shifted production to China: in 2011, GE healthcare moved its global X-Ray machine headquarters from Wisconsin to China, the first time GE had offshored a branch business headquarters to China.[174]

At a next level, the nature of these joint ventures and subsidiaries underlines GE's degree of engagement with Chinese government entities, in fields relevant to military-civil fusion. At least five are partnerships with state-owned entities: in addition to the Aviage Systems partnership with AVIC, GE operates General Electric-Harbin Power-Nanjing Turbine Energy Service with Harbin Electric as well as Nanjing Steam Turbine Motor (Group) Co., Ltd.; Huadian General Light Gas Turbine Equipment Co., Ltd. in partnership with state-owned Huadian Distributed Energy Engineering

Technology; NARI General Electric Intelligent Monitoring and Diagnosis (Wuhan) Co., Ltd. in partnership with State Grid Electric Power Research Institute Wuhan Nanrui Co., Ltd; Xidian General Electric Automation Co., Ltd. in partnership with China Xidian Electric; and General Electric (Wuhan) Automation Co., Ltd. in partnership with Baosteel-invested Baosight Software.

Select GE Subsidiaries and Joint Ventures in China

Name	GE Stake
General Electric Wind Power Equipment Manufacturing (Shenyang) Co., Ltd.	100
General Electric Medical System (Tianjin) Co., Ltd.	100
General Electric Energy Conversion Technology (Shanghai) Co., Ltd.	100
General Electric-Harbin Power-Nanjing Turbine Energy Service (Qinhuangdao) Co., Ltd.	51
Huadian General Light Gas Turbine Equipment Co., Ltd.	49
General Electric Medical (China) Co., Ltd.	100
General Electric Technology Transmission (Shenyang) Co., Ltd.	75
General Electric Power Conversion Technology (Shanghai) Co., Ltd.	100
General Electric (China) Energy Development Co., Ltd.	100
General Electric Medical Systems (China) Co., Ltd.	100
General Electric Energy (Shenyang) Co., Ltd.	100
General Electric Medical System Trade Development (Shanghai) Co., Ltd.	100
NARI General Electric Intelligent Monitoring and Diagnosis (Wuhan) Co., Ltd.	50
General Electric Power Generation Electronics (Shenyang) Co., Ltd.	100
Shenzhen Branch of General Electric (China) Co., Ltd.	–
GE Healthcare (China) Co., Ltd	100
General Electric Medical System Trade Development (Shanghai) Co., Ltd.	100
Beijing General Electric Hualun Medical Equipment Co., Ltd.	100
Xiamen Taikoo Engine Service Co., Ltd.	9.90
General Electric Renewable Resources (Tianjin) Co., Ltd.	100
Xidian General Electric Automation Co., Ltd.	41
General Electric (Wuhan) Automation Co., Ltd.	50
Aviage Systems	50

General Electric X-ray simulator at the World Expo Park in Shanghai, China, on May 3, 2010. Image credit: Imaginechina Limited / Alamy Stock Photo.

GE's joint ventures in China feature varying degrees of technology transfer. GE China documents describe an "in China, for China" innovation program.[175] GE reports having seven R&D centers, more than 60 laboratories, more than 30 manufacturing bases, and 34 joint ventures across 40 cities in China.[176] Concretely, when General Electric, the Shanghai Minhang District People's Government, and state-owned Huadian Distributed Energy Engineering Technology Co., Ltd (Huadian) launched their joint venture in 2011, GE's Chinese-language press release on the subject announced that "the cooperation will be a perfect combination of [GE's] global advanced technology and [Huadian's] rich local experience."[177] The press release also declared that "GE will transfer some of the core technology for the production of some components and gradually increase the localization rate of products." In a speech at the signing ceremony, the President of GE Energy Group China projected that the joint venture would "make positive contributions to the realization of China's infrastructure construction."[178]

GE has also partnered with Chinese government-led entities to help them develop international footholds through which they might acquire foreign technology. In 2012, Shanghai Jiaotong University and the GE China Research and Development Center cooperated to establish an advanced manufacturing joint laboratory at the University of Michigan.[179]

Military Ties

GE's joint venture partners—the players with which it is sharing technology—are not only state-owned entities. Some are also key figures in China's military and military-civil fusion programs. Besides AVIC, one potentially illustrative example is GE's long-standing partnership with Harbin Electric Group, one that conveys both the technology transfer and human rights risks that accompany GE's China presence.

The Chengdu Wing Loong II Chinese high-altitude strike military unmanned aerial vehicle. Image credit: Andrey 69 / Shutterstock.

The relationship between GE and Harbin Electric dates back two decades, when they established their joint venture.[180] In March 2014, the two companies launched an innovation center in Harbin, GE's third innovation center in China. At the center's opening ceremony, GE leadership described the innovation center as a "comprehensive platform for localized cooperation" between "strategic partner" Harbin Electric and GE.[181] In a press release, GE framed the innovation center as part of GE's "In China, for China" innovation strategy; "an important measure for GE to strengthen its localized technology collaboration." [182]

Harbin Electric Group is a state-owned entity. It also participates in Beijing's military-civil fusion program, including through a dedicated company department.[183] That participation draws on turbine technologies, also the domain involved in the partnerships with GE. For example, in 2017, Harbin Electric visited China's Second Naval Submarine Base to unveil a ship power maintenance center. The company described this as a "major move thoroughly to implement the military-civil fusion development strategy." Representatives from the People's Liberation Army Navy's (PLAN's) Naval Equipment Department, the Second Submarine Base, the PLAN's military representative office in Harbin, and military-related enterprises attended the inauguration ceremony.[184] Coverage of the event in *Sina Finance* noted that "as an important state-owned backbone enterprise related to national security, Harbin Electric Group has devoted itself to China's national defense construction since its birth."[185] The same year, Harbin Electric leadership met with counterparts from the China Aviation Engine Group to discuss cooperation in gas turbines.[186]

Harbin Electric is also exposed to indicators of forced labor in Xinjiang. For example, the state-owned enterprise undertakes projects for the Xinjiang Production and Construction Corps (XPCC).[187] The US government has sanctioned XPCC for connections to human rights abuses in the Xinjiang Uyghur Autonomous Region.[188]

Supporting China's Domestic Authoritarianism and International Offensive

GE's technological partnerships also risk directly supporting China's surveillance state: In 2016, GE and the Tianjin municipal government launched a smart-city project. In the memorandum of understanding for the project, GE committed to provide Internet of Things application software development.[189] China's smart city program is a core part of its domestic surveillance efforts, elements of which could be replicated abroad. Having honed smart city capabilities at home, Beijing is also now exporting them—and in the process, developing new levels of access to, and control of, detailed data and information on municipal infrastructure as well as individual households and consumers in rights-respecting countries.[190]

GE also espouses support for high-level industrial policies, including the Belt and Road Initiative (BRI) and Made in China 2025, intended to extend Beijing's footprint and influence internationally.[191] Such support brings GE into partnership with Chinese military-tied entities. helping Beijing to expand its footprint internationally. For example, in 2017, GE and China Telecom announced a strategic cooperation agreement in industrial Internet technology, including in developing and deploying "services in China through technical cooperation in the industrial Internet field to help implement the Made in China 2025 strategy."[192] China Telecom has since been identified by the US DoD as affiliated with the Chinese military.

Exposure to Human Rights Risks

GE's operations in China also expose it directly, as well as through its partners, to human rights risks and indicators of forced labor. GE itself appears to have an office in Urumqi, Xinjiang.[193] The US Departments of State, Treasury, Commerce, and Homeland Security have issued joint business advisories warning companies against operating in Xinjiang because of forced labor and oppression of the Uyghur ethnic minority in the region.[194]

A number of GE's major partners are associated with indicators of forced labor and connected to known bad actors. Harbin Electric's ties to XPCC offer one example. China Huadian, GE's joint venture partner in Huadian General Light Gas Turbine Equipment Co., Ltd., provides another case. Huadian Electric has a Xinjiang-based subsidiary.[195] In 2021, the Chairman of China Huadian attended the Central Enterprise Aid Xinjiang Work Conference in Urumqi. Other attendees included the Secretary of the Party Committee of the Xinjiang Uyghur Autonomous Region (XUAR), the Political Commissar of the XPCC, and leaders of the state-owned Assets Supervision and Administration Commission of the State Council (SASAC). At the conference, China Huadian signed a strategic cooperation agreement with the XUAR government as well as a project cooperation agreement with the Kashgar Administrative Office. China Huadian's Chairman affirmed that the company would always "thoroughly study and implement General Secretary Xi Jinping's important expositions on Xinjiang work, and fully and accurately implement the Party's strategy of governing Xinjiang in the new era"—and also that China Huadian was committed to "practicing the spirit of the XPCC" and implementing the spirit of the "Fifth Central Ethnic Work Conference."[196]

Google

SCORECARD
B

On January 6, 2016, the Xiamen Google AdWords Experience Center launched. The Center was established by the local district government; a China-based Google subsidiary, Google Advertising (Shanghai) Co., Ltd; and Google's domestic operating partner, Xiamen First Page Network Technology Co., Ltd (First Page). Local Chinese Communist Party leaders and government officials attended the opening ceremony alongside a host of Google China executives. They celebrated the role the center would play in furthering China's international commercial ambitions, fueled by Google's technology and influence. The General Manager of First Page explained that the center would "rely on the influence of Google's international platform and its absolute advantage in global advertising" to help Chinese companies succeed in the international market. "With the support and joint efforts of the government, we will jointly promote the upgrading and transformation of small- and medium-sized cross-border e-commerce enterprises."[197] First Page reiterated the point the next year, at the Google Greater China Partner Summit in Xiamen: "We have a better understanding of Google's rules…. It is inevitable that Chinese foreign trade companies will Go Global through Google."[198]

Google Experience Centers in China[199]

Archived map of Google Experience Centers in China. Image credit: Google.

Neither that language nor the Xiamen center is anomalous. Over the past decade, Google has launched at least 27 so-called "Experience Centers" in China. They are designed to help Chinese companies expand their international market through digital advertising and technological support.[200] All the Experience Centers are jointly established by Google, a local government entity, and a local operator.[201] The Experience Centers serve as bases through which Google sells advertisements and marketing to Chinese entities. They also offer technological, commercial, and training support. For example, the Guangxi Experience Center features a cross-border e-commerce talent training center; an entrepreneur incubation center for cross-border e-commerce companies; and a Google Big Data Mining and Application Center.[202]

The Chinese government blocked Google's search engine in 2010.[203] Since then, the company's footprint in the PRC has remained minimal. However, that does not mean that Google has left the country entirely. Nor does it mean that Google has not attempted to expand its footprint. In 2019, for example,

Google stopped carrying advertisements in China for sites that allowed China-based users to evade censorship laws, a move that reportedly appeared to be part of an attempt to reclaim ground in China's market, and corresponding favor with the Chinese government.[204] More concretely, other Alphabet subsidiaries operate in China, the company continues to invest directly into Chinese companies, and Google relies on suppliers in China. For the most part, these constitute commercial relationships with limited connection to the Chinese government, Chinese military players, or Beijing's surveillance state. However, they do create certain risks. In surveying the history and current state of Google's operations in China, this report finds ever since:[205]

- Google's investments in China as well as its Experience Centers risk supporting Chinese industrial policy, its internationalization, and may indirectly contribute to China's military-civil fusion and surveillance ecosystems; and

- Google's supply chain in China exposes it to indicators of potential security and human rights risks.

Google receives a B in operations. While the company's presence in China is minimal, what operations Google does maintain in the country lead it to support China's distortive industrial policy, and to fuel that policy's internationalization. Google receives a B in partnerships for similar reasons, as well as because the company maintains supply relationships with Chinese entities that expose it to both human rights and security risks.

The Disappearing Act

In 2006, Google made a deal with Chinese authorities: If it agreed to censor search results shown to Chinese users, it could enter the Chinese market with google.cn.[206] By 2009, Google had acquired a 30 percent share of the Chinese search market. But the next year, the Chinese government launched an extensive hacking attack targeting Google's intellectual property as well as Gmail accounts belonging to Chinese human rights activists. In response, Google announced that it would stop censoring search results. In response, the Chinese government blocked Google's websites. Google retreated to a Hong Kong-based search engine.[207] "Google Shuts China Site in Dispute over Censorship," read *The New York Times* headline.[208]

However, as Chinese internet commentators explain, "Google has never given up the big cake of the Chinese market."[209] A *Zhihu* post from 2016 points to the experience centers as evidence:

In the past years, dozens of Google experience centers have opened in China. These are jointly established by Google, local governments, and operators…This shows that the government encourages and supports the experience center model, even though you are not allowed to visit Google.[210]

The experience centers are just one example. Over the past decade, various reports have suggested that Google and its parent company, Alphabet, have attempted to re-enter segments of the Chinese market. Some of those projects have failed. Launched in 2017, the Google AI China Center fizzled out within a few years. Dragonfly, an attempt to re-brand and launch a new search engine for the Chinese market, faltered amid US outcry and regulatory concern that it would censor according to Beijing's preferences, and also share data with the Chinese government about individuals searching terms that Beijing deemed sensitive, which it could then use for further surveillance and repression.[211] Other projects have been more successful: Google released its machine-learning framework, TensorFlow, in China in 2017.[212] The next year, Waymo, Alphabet's self-driving car company, established an office in the Shanghai Free Trade Zone.[213]

Google's experience centers in China provide a platform for Beijing to advance its Belt and Road Initiative, Go Out program, and other national strategies designed to secure, through state support, Chinese leverage in critical value chains. Google's investments in the Chinese start-up scene dovetail with similar efforts. The company's portfolio features darlings of Beijing's industrial policy, subsidized by the Chinese government as part of a larger effort to leapfrog into strategic domains. In 2018, Alphabet's CapitalG invested in Manbang, China's truck-hailing giant.[214] Manbang's other investors include Tencent and state-owned Sinopec Group

Capital. Manbang's corporate documents acknowledge that its profit relies on Chinese government subsidies, a core feature of the industrial policy behind Beijing's "State led, Enterprise driven" economic model.[215]

Supply Relationships

Google relies on suppliers in China, including suppliers that expose it to forced labor and to security risks. A 2019 report by the Australian Strategic Policy Institute (ASPI) found indicators of forced labor associated with at least three Chinese suppliers of Google: Hubei Yihong Precision, Foxconn, and Hefei Bitland Information.[216] Goertek's LinkedIn account also suggests that it is a Google supplier.[217] Goertek is a leading Chinese electro-acoustic device manufacturer. ASPI has identified its supply chain as exposed to forced labor risks. Goertek also does business with Huawei, has close ties to the Chinese government, and receives significant government subsidies. [218] Goertek operates military-civil fusion projects in China, including the Beihang Qingdao Research Institute, which has a dedicated center for military-civil fusion. Other Goertek military-civil fusion activities focus on virtual reality, microelectronics, precision instruments, and optoelectronics.[219]

Google has also partnered with Feitian, a Beijing-based supplier of two-factor authentication products, to develop security keys. Feitian is a player in China's security ecosystem.[220] A 2021 report by *Top10VPN* found that Feitian had supplied USB keys for China's police and potentially the PLA.[221] In 2017, Feitian acquired Hongsi Electronics, which delivers security chips in conjunction with China's Office of State Commercial Cryptography Administration (OSCCA).[222] Feitian's role in Beijing's industrial and technology policy is evident in the subsidies that it receives. The company's 2021 semi-annual report more than 3 million RMB in subsidies for the first half of the year. Those include subsidies for a project on "Intelligent Network Identity Authentication System Engineering" run by the Beijing Academy of Science and Technology, and a project funded by the National Development and Reform Commission (NDRC) project on encryption algorithms supporting the SM2 and SM4 algorithms of OSCCA, as well as "project funds for foreign trade companies to improve their international business capabilities."[223]

In May 2019, Google replaced Bluetooth Titan Security Keys made by Feitian because of security vulnerabilities.[224] As recently as December 2020, Chinese industry analysis reported that Feitian had supplied Google with the Titan Security Key.[225] Feitian's website continues to advertise Titan Security Keys for Google Advanced Protection programs.[226] Feitian's corporate documents also emphasize that in 2016, it became a member of the board of the Fast Identity Online (FIDO) alliance, a standard-setting organization for authentication protocols, whose members include Google, Microsoft, Apple, Intel, PayPal, and MasterCard.[227]

Intel

SCORECARD

F

On October 1, 2021, Intel's chief government affairs officer published a piece on the company website: "US competitiveness is at stake for chip manufacturing." He described plummeting US semiconductor manufacturing in face of growing Asian control of the industry. The commentary framed Intel as a patriotic US national champion and a contributor to efforts to revitalize American industry, technology, and competitiveness. "At Intel," the piece explained, "we are significantly expanding our US manufacturing operations […] Intel looks forward to working with our federal partners to help maintain America's position as the world's top technological innovator."[228] Intel has followed through on this narrative with announcements of significant investment in US-based manufacturing.[229]

These announcements contrast with the reality that Intel also manufactures—and operates research and development, innovation, and artificial intelligence centers—in China. They also belie Intel's collaborations with China's major tech players, including those tied to the Chinese military and surveillance systems, on technologies relevant to military and surveillance capabilities. Intel may be working to help maintain America's position as the world's top technological innovator. But it also risks supporting China's efforts to acquire and deploy that innovation in ways that may contribute to Beijing's surveillance state, military modernization, and human rights abuses.

Intel has a major presence in China, from production and supply relationships to technological cooperation, research and development centers, innovation sharing, and investment. With this presence comes extensive ties to the Chinese government—in terms of elite contact as well as research and technological collaboration—including to government entities leading surveillance and military development programs.

Amid Intel's extensive footprint in the Chinese system, some representative and troublesome examples include:

- An extensive production, research, and development footprint in China, featuring partnerships with government and military-tied entities;
- Long-standing ties to the Chinese government, including research collaborations with government research institutions (e.g., CASIA) developing surveillance technologies and elite-level relationships with the institutional players (e.g., MIIT) charged with implementing Beijing's military-civil fusion strategy;
- Investments in and alongside Chinese military-civil fusion and surveillance-relevant companies; and
- Intel technology potentially being incorporated into surveillance efforts in Xinjiang.

Intel Operations Score: F: Even as the company positions as a champion of American competitiveness, Intel also manufactures and shares innovation in China. In addition, Intel invests in Chinese high-tech and military-civil fusion companies, potentially fueling them with both capital and access to technology. And Intel's technology is used by Xinjiang's public security authorities. On all these fronts, Intel's exposure exceeds that of other companies surveyed in this effort.

Intel Partnerships Score: F: The company's extensive, and long-standing, technological partnerships with government-, military-, and surveillance-tied Chinese entities have contributed to the development of Beijing's military and surveillance capabilities over the past decade. Moreover, this project found no evidence that Intel has taken action to curb or terminate such problematic relationships, even as the US government warns, and increasingly regulates, against maintaining them. On all these fronts, Intel's exposure exceeds that of other companies surveyed in this report.

An American Champion with a Chinese Footprint: Intel China

Intel set up an office in Beijing in 1985 and established Intel (China) Co., Ltd in 1994.[230] Since, Intel's China footprint—in manufacturing, research, development, and innovation—has grown consistently. Today, Intel's website lists 17 campuses in China,[231] the company has at least two production sites in China, and it operates a series of innovation and R&D centers across the country.[232]

The Intel China Research Institute, also known as Intel Labs China, was launched in 1998 to research and develop cutting-edge technologies in the intelligent Internet of Everything environment. Today it focuses on artificial intelligence algorithms, autonomous system platforms, intelligent infrastructure, and 5G. The Institute has five centers: The robot innovation laboratory, cognitive computing laboratory, intelligent driving laboratory, communication architecture laboratory, and new technology center.[233] The Intel China Research Institute cooperates with Chinese players ranging from the China Academy of Sciences to Baidu and Tencent.[234] The Dean of the Institute described its model in a June 2021 interview, focused on quantum technology efforts: "The Intel China Research Institute follows the development trend of global cutting-edge technologies in real time and brings some technologies to China for localized innovation and application. Intel also makes good use of the advantages of China's local industry, academia, and research to open up and break through in technology."[235]

In 2002, Intel established the **Asia Pacific Application Design Center (Shenzhen**) to provide advanced product development and technical support services for OEM and ODM manufacturers in China's computing and communications industry.[236] At its launch, Intel's chief technology officer described the new center as a "concrete manifestation of Intel's long-term commitment to supporting the development of China's information industry." Representatives from Huawei and Tsinghua Tongfang, among others, attended the launch.[237]

In 2003, Intel established **Intel Products (Chengdu) Limited**, which packages and tests Intel semiconductor products. As of 2014, Intel had invested 600 million USD in the facility. In 2014, the company announced that over the next 15 years, it would invest 1.6 billion USD to introduce the latest high-end testing and fully upgrade the facility.[238] In its recruitment information for the Chengdu operation, Intel declares that its "Chengdu production plant has become Intel's important global production engine and new mobile device trial production base. It is also an important move by Intel to respond to the Chinese government's Western Development Policy."[239] In 2019, Intel announced that the Chengdu plant had completed certification and achieved full-process manufacturing across assembly, testing, and completion. The plant's products reportedly do not enter the US market because of US trade policy.[240]

In 2005, Intel established the **Intel Asia Pacific R&D Center** in Shanghai's Zhizhu Science Park. Intel's recruitment information describes this as Intel's largest and most

comprehensive R&D base in the Asia Pacific. It focuses on operating systems, virtualization technology, big data, deep learning, basic input output systems and firmware, cloud computing and data center platform development, and Internet of Things and video technology.[241] According to Chinese media, the center has supported specific collaborations between Intel and Huawei, Tencent, Alibaba, and Baidu.[242]

In 2007, Intel announced a 2.5 billion USD investment to build a 12-inch wafer manufacturing in **Dalian**, China's first wafer plant in Asia. Intel has announced that it is in the process of selling the plant to South Korea's SK Hynix.[243]

Intel has continued to launch new projects in China even as tensions with the US escalate. In 2018, Baidu and Intel announced the establishment of a joint **AI 5G innovation lab** to support new user experiences, IoT, and automotive development goals.[244] In 2018, Intel held the grand opening for its **FPGA China Innovation Center**, Intel's largest FPGA innovation center in the world.[245] And in May 2020, Intel's China Research Institute and the Lishui Development Zone, a provincial development zone established by the Jiangsu Provincial People's Government, jointly launched the "**Intelligent Transportation Technology Research**" project. That project aims to build an open technology and industry exchange platform, help the construction of intelligent transportation standards, and promote advances in intelligent transportation technology.[246]

Partnering with the Chinese Government

In 2012, Intel partnered with **the Chinese Academy of Sciences Institute of Automation (CASIA)** in jointly establishing the "China-Intel Internet of Things Technology Research Institute" to focus on intelligent perception, transmission technology, and big data processing technology.[247] In 2018, Intel, CASIA, and Tsinghua University established the Intel Intelligent Connected Automotive University Cooperative Research Center, designed to promote research on autonomous driving and networked automobiles.[248]

The technologies on which these joint programs focus (e.g., intelligent perception) are directly relevant to a variety of military and surveillance use cases. CASIA develops surveillance technologies and applications for the Chinese government.[249] For example, between 2012 and 2016, the Institute undertook a project for the National 973 Program, the PRC's leading basic research program, on developing "Social Perception Data Processing for Public Safety."[250] According to its official description, that project was designed to "meet the major needs of national security…for social perception intelligence [and] provide technical support and decision-making support for real-time monitoring, early warning and forecasting, and emergency handling of public security."[251] CASIA's Intelligent Video Surveillance and Face Recognition Technology systems have been used in

Intel exhibit at the China International Import Expo in Shanghai, on November 6, 2018. Image credit: REUTERS / Alamy Stock Photo.

Chinese government security applications.[252] CASIA-linked surveillance systems have likely been deployed in Xinjiang: As early as 2007, a delegation from the Institute visited the Xinjiang Institute of Physics and Chemistry to discuss cooperation in "Xinjiang minority speech and language processing technology."[253]

In addition, CASIA is a core contributor to China's military and military-civil fusion programs. The Institute runs dedicated military projects, evident and advertised in its hiring documents.[254] Examples of CASIA's past such projects include developing space cameras for the Shenzhou V and a vehicle-mounted ground illuminator detection system that won China's second prize for military scientific and technological progress.[255] CASIA also maintains a Military-Civil Fusion Innovation Center.[256]

Intel's technological engagement with the Chinese Academy of Sciences extends beyond CASIA, too. In 2012, Intel established a joint laboratory with the **Institute of Computing Technology of the Chinese Academy of Sciences** (CASICT), focused on using Intel microprocessors, chipsets, software, and computing products to fuel research and applications in field programming and optimization, data center server architectures, corresponding hardware and software systems, and research on gene sequencing.[257]

It is unclear whether either laboratory is still in operation or has been terminated. Regardless, there are recent indicators that Intel continues to cooperate with the China Academy of Sciences (CAS). In January 2021, Intel China representatives visited the Center of High Performance Computing of the Shenzhen Institute of Advanced Technology, under CAS, to discuss research, progress of major national and provincial projects, and the efficient analysis of biomedical big data.[258]

Intel has partnerships with China's surveillance apparatus outside of CAS, too. In 2015, Intel China and the Guiyang Municipal People's Government signed a memorandum of strategic cooperation on smart city construction. Intel committed to providing "leading big data technology" for Guiyang's "China Data Valley" project.[259] In 2017, Intel China partnered with the Guiyang Municipal Government and China's AI Industry Innovation Alliance—spearheaded by the Ministry of Industry and Information Technology—to launch the China Artificial Intelligence Open Innovation Platform.[260]

Similarly, Intel China describes local Chinese governments using its technologies to implement digital monitoring systems. For example, a case study on the company's website about Intel's technology fueling video surveillance in Zhejiang Province begins by describing a "challenge:"

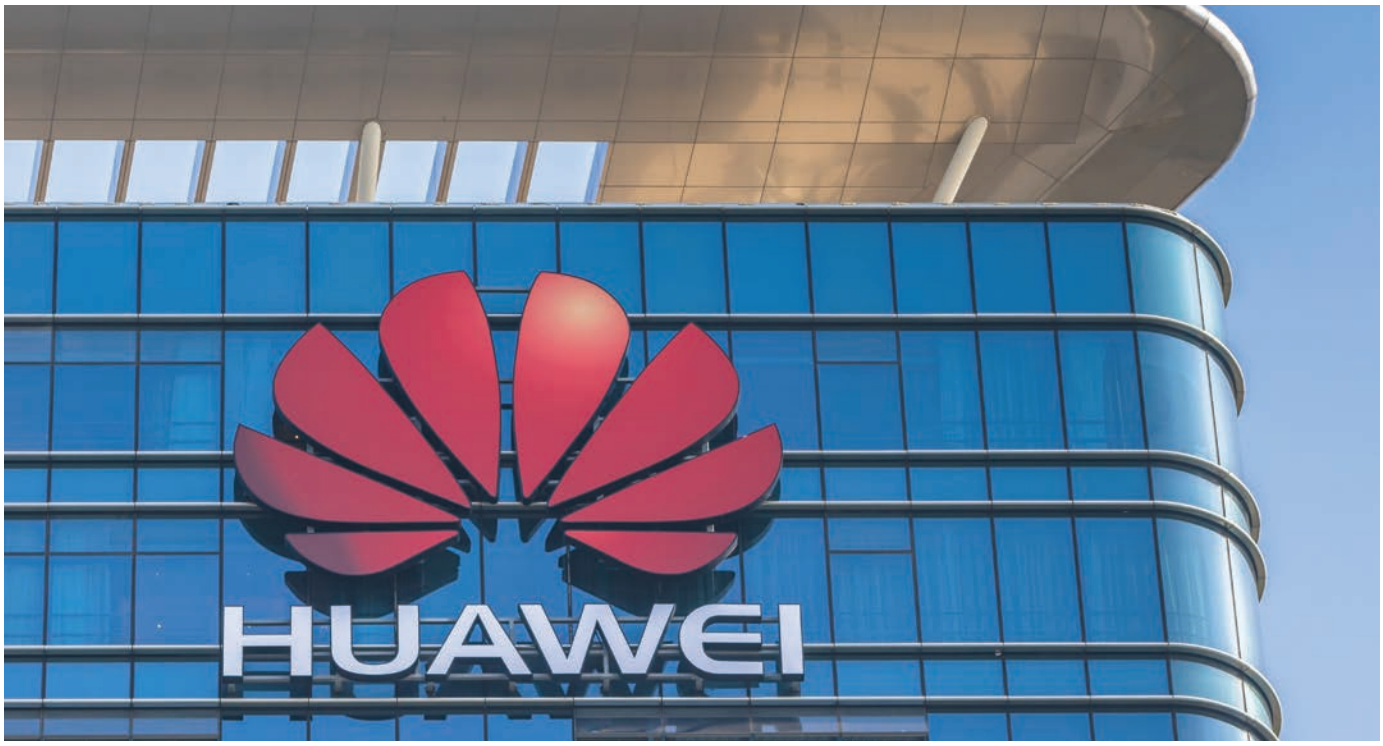
Thousands of digital surveillance equipment systems have been installed at important checkpoints in the city [in Zhejiang Province]. These systems capture images and video data 24 hours a day, with a monthly data volume of terabytes. Now, the local transportation department is facing the challenge of how to improve traffic management through effective use of this ever-increasing data.[261]

It then speaks of the solution: "22 servers based on the Intel Xeon processor E5 series… to form a traffic data center in this [Zhejiang Province] city…[and] Leverage the advantages of Intel Open Data Analysis Platform to realize the mining and analysis of massive amounts of data."

Chinese Government Ties

As that example indicates, Intel's footprint in China entails cooperation with the Chinese government—including, notably, the Ministry of Industry and Information (MIIT), a leading state entity charged with implementing China's military-civil fusion national strategy. Some of this engagement appears run-of-the-mill and necessary for doing business in China, also to pre-date widespread recognition of accompanying risks: In 2011, Intel and MIIT's Electronic Intellectual Property Center signed a strategic cooperation agreement committing to partner in intellectual property and related fields.[262]

However, Intel executives continue to engage with MIIT representatives in fields relevant to military-civil fusion, even as tensions between the US government and China escalate and risks posed by Beijing's military-civil fusion strategy become more evident. Even if these meetings are considered normal or even necessary business practices, they constitute



Main building of Huawei Base in Songshan Lake District of Dongguan city, Guangdong Province, China. Image credit: Peter Stein / Shutterstock.

elite-level engagement—in fields relevant to military and surveillance applications—between a company intended to be a champion of US competitive industrial development, and a Chinese government entity charged with acquiring and applying industrial capacity for military and surveillance uses. In December 2017, the Vice Minister of MIIT met with Intel's then-CEO to discuss cooperation in China and the development of intelligent networked vehicles.[263] In 2019, the Vice Minister and then-CEO met again, this time to discuss the integrated circuit industry.[264] The same year Intel hosted a sub-forum at the China International Information and Communication Exhibition organized by MIIT. Intel's sub-forum focused on 5G and relevant applications.[265] At the event, China Mobile and ZTE showcased 5G-enabled technologies (e.g., intelligent edge computing, autonomous driving, intelligent image identification) fueled by Intel products. In response, Intel leadership declared that the company would continue to work closely with China's 5G industry ecological partners.[266]

Intel is also a technical advisor of China's Data Center Alliance overseen by MIIT. Its governing units include China Telecom and China Mobile, which have been identified by the US Department of Defense as tied to the Chinese military, as well as Huawei and ZTE.[267]

Footholds and Circumvention: Intel's Investments in China

Intel further develops its footprint in China through investments—including into high tech and military-civil fusion relevant companies.[268] These investments risk providing capital that could fuel China's surveillance and military capabilities. They also often accompany technological partnerships. For example, Intel owned a more than 12 percent stake in UNISOC, a Chinese state-invested fabless semiconductor company, as recently as 2020.[269] Intel's investments in China also illustrate potential tensions between Intel's

overseas stakes and US geopolitical interests. In 2018, Intel and UNISOC announced a strategic cooperation in 5G. The next year, they announced an end to the partnership. Many analysts assumed the break-up stemmed from uncertainty around Sino-US relations, and the regulatory or reputational risk that might accompany cooperation with a Chinese state-owned entity operating in 5G technology development. However, Chinese sources have suggested that the break-up of technological ties may have been superficial. Intel remained a shareholder in UNISOC. And in 2019, Intel subsidiary Mobileye announced the establishment of a joint venture with UNISOC to develop autonomous driving technology. As Chinese press put it in 2019, "Intel broke up with UNISOC on the surface, then backchanneled to match UNISOC up with its Israeli branch. Israel's technology is not affected by US sanctions."[270] In other words, Chinese sources seem to interpret Intel's moves as converting its partnership with UNISOC to its Israeli subsidiary in order to reduce public attention to its support for Beijing's 5G ambitions.

Intel also invests alongside China Electronics Corporation—which the US Department of Defense has identified as tied to the PLA—in Lanqi Technology, a Chinese high-performance processor and integrated chip design company. Intel is the largest shareholder in the company after China Electronics Investment Holdings (中国电子投资).[271] In addition, Intel supplies and engages in technological cooperation with Lanqi: In 2020, Intel, Lanqi, and Tsinghua University jointly launched a 2 billion RMB project to carry out research and development of high-performance processors, data-protection memory modules, and their application software technologies.[272] Intel's Global Vice President attended the signing, as did the Chairman and Party Secretary of China Electronics.[273] In August 2021, Lanqi announced it intended to triple the volume of its transactions with Intel.[274] In October 2021, Lanqi participated in the Intel Innovation Summit.[275] Activity with and through Lanqi may provide an indirect route for Intel's innovation to support the state-backed ecosystem of Chinese corporates that may support military-civil fusion programming. Chinese media suggests as much: A 2019 article noted that Lanqi's Jintide server CPU "is an important path for Intel's architecture to continue to serve the needs of China's central enterprises."[276]

Partnerships

A similar patter holds for Intel's partnerships in China—which link it to military and surveillance-tied entities, relate to sensitive technologies, and appear to be ongoing despite US-China geopolitical tensions and increasing awareness of the atrocities that the Chinese surveillance state enables. Intel's partnership with Hikvision offers a prime example. Hikvision is a Chinese state-owned manufacturer and supplier of video surveillance equipment that the US government has placed on the US Department of Commerce's Entity List.[277] Intel has long been a core Hikvision supplier. The two companies launched their technological cooperation in 2006, when Hikvision began to develop products on Intel platforms. By 2014, Intel and Hikvision appear to have moved from back-end supply relationships to comprehensive cooperation, partnering in front-end cameras, machine vision, and other fields. In 2017, Intel and Hikvision launched a comprehensive partnership in artificial intelligence, committing to "strengthen the exploration of deep learning technology" and an artificial intelligence platform.[278] In 2018, Intel China advertised on its website having assisted Hikvision's development of the "Deep Eyes global camera" used in video surveillance.[279]

The next year, Hikvision was added to the Department of Commerce's Entity List and barred from buying restricted components from US sources.[280] Chinese press suggested that Intel might help to navigate those restrictions: According to a social media account of China's Semiconductor Investment Alliance, former Intel CEO Bob Swan said in an October 2019 interview—and it is unclear whether the post is paraphrasing or quoting—"regarding Hikvision being included in the Entity List…Intel is focusing on how to use its global operating capabilities to reduce the impact on customers… It also hopes to exert influence between the Chinese and American governments."[281] That notion appears to have taken at least some concrete form in encouraging stable trade dynamics: In 2019, technology firms including Dell, Microsoft, and Intel issued a joint statement calling for then-President Trump not to impose tariffs on Chinese laptops and tablets.[282] Hikvision and Intel appear not to have publicly launched any new cooperation projects since the Entity List inclusion.

Uyghurs at a re-education camp in Moyu County, China. Image credit: Azamat Imanaliev / Shutterstock.

Intel has launched partnerships with additional companies tied to the Chinese military. In 2018, Intel and China Unicom signed a strategic cooperation agreement in the field of connected PCs.[283] The same year, Intel and China Mobile signed a strategic cooperation agreement focused on 5G, cloud computing, and AI.[284]

Xinjiang

Intel's footprint in China also entails risks that its technology is supporting Beijing's surveillance and repression efforts in Xinjiang, directed against the Uyghur minority population. In 2019, the *Wall Street Journal* found that Intel technology was being used in surveillance systems in Xinjiang, and that Intel had invested in and provided technologies to a company embedded in Xinjiang and supported by the Chinese Ministry of Public Security.[285] A 2020 investigation by *The New York Times* found that the Urumqi Cloud Computing Center—a hub through which the Chinese government monitors "countless people in Xinjiang"—runs on chips manufactured by Intel and Nvidia.[286] And in December 2020, the chairs of the Congressional-Executive Commission on China sent a letter to Intel's CEO seeking information on the company's involvement in Xinjiang surveillance.[287]

Despite this public attention, Intel technology appears to still be used in Xinjiang surveillance applications. For example, the Chinese Ministry of Commerce website notes that the "Border intelligent control system of the Xinjiang Entry-Exit border inspection station" relies on Intel CPUs.[288] A 2020 procurement post from the Public Security Bureau of Shaya County, Xinjiang reports the purchase of Intel hard disks.[289] A similar 2021 report from the Public Security Bureau of Changji Hui Autonomous Prefecture in Xinjiang reports the purchase of Intel servers.[290]

Intel might not know about or be able to control those uses. However, Intel's Chinese website does advertise the use of its processors, adapters, and servers for Chinese government-run medical programs in Xinjiang.[291]

Microsoft

Microsoft established Microsoft Research Asia in 1998.[292] It is now the company's largest and most comprehensive R&D base outside the United States, with functions spanning basic research, technology incubation, product development, and strategic cooperation.[293] Chinese media describes it as the "Whampoa Military Academy for AI," a reference to the legendary military academy that produced the commanders who led China's forces in the Northern Expedition and Second Sino-Japanese War.[294] Two decades later, in 2017, Microsoft Research Asia launched the Innovation Hub, a new center that describes its goal as combining "Microsoft's leading AI research results with the rich industry experience of member companies" in China. Some 50 companies have joined, hailing from industries including finance, logistics, telecommunications, and manufacturing, and ranging from state-owned enterprises and investment arms to Chinese start-ups.[295]

Through the Innovation Hub, Microsoft supports Chinese companies, including state-owned entities, and their technological development, that are affiliated with the Chinese military and surveillance state. For example, China Telecom—state-owned telecommunications giant that the US Department of Defense has identified as tied to the Chinese military—is on the roster of the Innovation Hub's current members.[296]

The Innovation Hub is not an anomaly in Microsoft's presence in China. The company has an expansive technological and information footprint in China entailing significant cooperation with Chinese government entities, including in research and with players relevant to Beijing's military and surveillance programs. This report does not attempt to describe all of Microsoft's presence in China. Rather, it focuses on specific cases that underline the extent of that presence and associated risks. Those cases include:

- Microsoft has launched a network of innovation hubs in China in partnership with local government entities, as well as joint laboratories with central government entities. These collaborative efforts develop and apply technologies relevant to China's surveillance state (e.g., smart cities). Microsoft has continued to expand this network even as tensions between the United States and China have escalated, and Beijing's threat to global security and human rights norms has become more evident.

- Microsoft has a joint venture in China, in conjunction with a state-owned defense conglomerate on the US Commerce Department's Entity List, that tailors Microsoft products for government and state-owned enterprise (SOE) uses. That joint venture partners with a host of government and military players.

- Microsoft's partners and suppliers in China include companies implementing surveillance programs in Xinjiang, with indicators of forced labor in their supply chains, and that the US government has identified as tied to the Chinese military.

Microsoft receives an F in operations. Its technology support for Chinese government and military entities is more direct than those of most other companies surveyed in this effort. The applications to the surveillance and censorship programs of the CCP are also clearer.

Microsoft receives an F in partnerships. Its supply chain is exposed to forced labor risks, though not more so than other companies surveyed in this report that offend on this front. Rather, Microsoft's partnership exposure stands out for ongoing ties to entities that the US government has clearly identified as tied to the Chinese military.

Technology and Data Footprint

Microsoft has a significant, and growing, network of innovation centers, data centers, joint laboratories, and other technology hubs in China. Many of these have been established in partnership with Chinese government or government-tied entities. They focus on technologies, like smart cities, that are core to China's domestic surveillance efforts. And these technology hubs continue to be launched even as China's tech-enabled threats to human rights and global norms become apparent.

Government-Tied Innovation and Technology Centers

Microsoft boasts a broad network of innovation centers across China, all launched in conjunction with government entities, focused on information technology development relevant to military-civil fusion, ranging from artificial intelligence to advanced computing. In 2010, Microsoft established a cloud computing innovation center in Shanghai.[297] Microsoft leadership declared that the innovation center would "help the government…to improve their competitiveness," while the Shanghai Municipal government said the Microsoft innovation center would help Shanghai "accelerate the realization of strategic goals."[298] In 2013, Microsoft signed a memorandum of strategic cooperation with the Hainan Provincial government to launch an innovation center in Hainan. In that agreement, both parties committed to "all-around strategic cooperation" in information technology research and development, software talent training, and incubation of information technology applications.[299] In 2014, Microsoft launched the Jiangsu Microsoft Innovation Center with the Yangzhou Municipal Government and the Shaanxi Microsoft Innovation Center with the Shaanxi Provincial People's Government.[300] Microsoft has continued to develop innovation centers in China even as tensions between the US and China escalate—and Beijing's technological ambitions have become broadly recognized as posing risks for global human rights and security. In 2019, Microsoft built an Artificial Intelligence and Internet of Things Laboratory in Shanghai.[301] Also in 2019, Microsoft expanded its Suzhou innovation center (originally launched in 2013) with support from the local government, to include an AI Industry Innovation Center. Construction is intended to be complete in 2023.[302] And in 2021, Microsoft's Zhenjiang Digital Economy Innovation Center, a partnership with the Zhenjiang government, began operation.[303]

These projects all involve local government support. Microsoft also runs joint laboratories with central Chinese government entities. In 2009, Microsoft, the Ministry of Industry and Information Technology (MIIT), and Tianjin University of Technology established a joint laboratory, the Microsoft Embedded System and Hardware Platform of Tianjin University of Technology Laboratory (MIIT-MS Embedded Tianjin Laboratory). The laboratory is part of MIIT's National Software and Integrated Circuit Public Service Platform. Tianjin University describes it as "a supporting platform for government decision-making, a resource platform for enterprise innovation, a dissemination platform for the latest technology, and a convergence platform for information sharing."[304] In other words, this is a platform that can support China's data-enabled approach to authoritarian governance. MIIT is the chief Chinese government entity charged with implementing China's military-civil fusion national strategy. And Microsoft's collaboration with MIIT appears to be ongoing. As recently as September 2021, the Minister of MIIT met with Microsoft President Brad Smith by video. They discussed deepening Microsoft's exchange and cooperation in China.[305]

Shen Xiangyang, Microsoft Global Executive Vice President, at the Wuzhen Summit in China's Zhejiang province on November 7, 2018. Image credit: Imaginechina Limited / Alamy Stock Photo.

In 2013, Microsoft joined hands with the Urban Engineering Research Center of China's Ministry of Construction to establish a Joint Laboratory of Smart City Technology Solutions of the Digital City Engineering Center of the Ministry of Housing and Urban Rural development.[306] Through that joint laboratory, Microsoft has launched smart city cooperation programming with local governments across China.[307] And in 2016, Microsoft and China Development Bank Capital launched an innovation incubator and accelerator platform for smart city solutions based on the Azure smart cloud platform.[308] Chinese smart city development, at home and abroad, is broadly accepted as a core pillar of, and contributor to, Beijing's surveillance system.[309]

Data Centers

Microsoft is building out a system of data centers in China. In 2021, Microsoft announced plans to open four new such centers in the country, bring its total to 10.[310] These data centers are operated by a local Chinese partner, 21Vianet, China's leading third-party independent data operator.[311]

As the case of Apple has shown, compliance with China's regulatory regime for storing data can make corporate and user information accessible to the Chinese government. 21Vianet's ties to the Chinese government make this possibility particularly concerning. 21Vianet assists MIIT in developing evaluation standards for government procurement cloud and is a member of the Chinese National Information Security Standardization Technical Committee, a rules-developing body falling under the China Electronics Standardization Institute—itself overseen by MIIT.[312] 21Vianet is also a governing unit of China's Data Center Alliance. That alliance is under the guidance of MIIT.[313] Its other governing units include Huawei, ZTE, China Telecom, China Mobile, and China Unicom, all of which the US Department of Defense as identified as tied to the Chinese military. The Alliance's full membership roster includes Microsoft, as well as Intel.

Ties to the Chinese Government

Microsoft also tailors its products in China for the Chinese government, in partnership with Chinese military-linked entities. In 2015, Microsoft and China Electronic Technology Company (CETC) launched C&M Information Technologies (神州网信技术有限公司), a joint venture dedicated to licensing Microsoft's operating system to Chinese government agencies and state-owned enterprises in the energy, telecommunications, and transportation sectors.[314] C&M describes its purpose as providing desktop operating system products for "Chinese government agencies and state-owned enterprise in the field of critical information infrastructure." Its long-term goal is to "help China create more world-class technologies so it can become a leader in technological innovation."[315] In 2017, Microsoft worked with China Electronic Technology Company (CETC) to launch a custom version of its Windows 10 software designed for exclusive use by the Chinese government. The software included local encryption adapted to target sensitive issues.[316]

CETC is a state-owned Chinese defense conglomerate specializing in dual-use electronics and information technologies. In 2020, the US Department of Defense explicitly identified CETC as tied to the Chinese military. Units of CETC and affiliated subsidiaries have been placed on the US Department of Commerce's Entity List, thereby restricting exports to them from US companies.[317] Not only is C&M a joint venture with a government and military entity that supports the Chinese government, but its supply and channel providers are also closely tied to the Chinese government and military systems. For example, the company's OEM partners include Tsinghua Tongfang, a Chinese state-owned software company that was placed on the US government's Military End-User List in 2021.[318] One of C&M's two channel partners is Chinasoft Cloud Technology Service, a subsidiary of China Electronics Corporation (CEC).[319] The first "security vendor" listed on C&M's website is Qi'anxin Technology, a Chinese government-invested cybersecurity company focused on serving central government departments and state-owned enterprises.[320] Its controlling shareholder is CEC. Qi'anxin not only supports Chinese government cyber capabilities, but also has partnered with at least one state-owned enterprise in Xinjiang to strengthen its network in the region.[321]

Though not necessarily a function of the CETC-Microsoft partnership, a 2021 report from *Top10VPN* found that Chinese government surveillance and censorship organs—including the Beijing Municipal Public Security Bureau, Fuzhou Public Security Bureau, Luoyang Public Security Bureau, and Zhongshan Public Security Bureau—use Windows products in their security and surveillance systems.[322] In 2014, Microsoft China leadership provided technical guidance for the construction of the public security cloud platform for Guangyuan City, Sichuan's Public Security Bureau.[323]

Microsoft also reportedly facilitates the Chinese government's efforts to control information. It has agreed to censor search results on its Bing search engine (e.g., Dalai Lama, Tiananmen Square), a commitment that has allowed Bing to be one of the few foreign search engines accessible in China.[324]

Partnerships

Microsoft's network of partnerships extends more broadly still. These further underline Microsoft's proximity to the Chinese military-civil fusion system, as well as to ongoing human rights abuses in China.

Surveillance Partners

A 2021 report from *Top10VPN* found that two Chinese companies that identify Microsoft as a partner have assisted in development of surveillance and censorship systems in China, including in Xinjiang.[325] **Haiyi Software** lists Microsoft—as well as other US companies IBM, HP, and Accenture—as a partner on its website.[326] The *Top10VPN* also reported that Haiyi provides products to public security bureaus across China and has participated in the first and second phases of the Golden Shield Project (also called the National Public Security Work Informational Project), a nationwide network-security project that includes a security management information system and a criminal information system. According to *Top10VPN,* Haiyi has also provided products to the Urban Multi-Dimensional Perception Monitoring Platform, which integrates data from multiple sources to

achieve 24/7 monitoring.[327] Bolstering those findings, Haiyi's website advertises "the most complete software product line in the field of domestic public security informatization."[328] **Beijing Zhongke Fuxing Information Technology** also lists Microsoft as a partner—alongside Intel and IBM—on its website.[329] According to *Top10VPN,* the company recently developed a detention center management information system to manage criminal information in prison databases. The company has worked on several projects in Xinjiang, including an information management center for Xinjiang Public Security Department and Xinjiang Production and Construction Corps (XPCC) detention centers.[330]

Forced Labor

A 2019 report by the Australian Strategic Policy Institute (ASPI) found indicators of forced labor associated with at least three Chinese suppliers of Microsoft: Hubei Yihong Precision, Foxconn, and O-Film Manufacturing Company.[331] Another potentially problematic link is Goertek Inc., a leading Chinese electro-acoustic device manufacturer that ASPI has identified as exposed to indicators of forced labor risks. Goertek's LinkedIn account suggests it is a Microsoft supplier.[332] Goertek also does business with Huawei, has close ties to the Chinese government, and receives significant government subsidies. [333] Goertek also operates military-civil fusion projects in China, including the Beihang Qingdao Research Institute, which has a dedicated center for military-civil fusion, as well as others for virtual reality, microelectronics, precision instruments, and optoelectronics.[334]

Military Partners

Microsoft has launched strategic cooperation agreements with other companies that the US government has identified as tied to the Chinese military or as an export restriction concern. In addition to its partnership with CETC discussed above, Huawei's 2016 annual report said it had launched "in-depth cooperation" with Microsoft.[335] Moreover, in 2018, Microsoft announced a strategic cooperation with Dajing Innovations (DJI), a leader in civilian drones and imaging technology. Microsoft stated that it would bring advanced AI/ML capabilities to DJI drones through its Azure platform.[336] In 2020, DJI was placed on the US Department of Commerce's sanctioned Entity List. This project was unable to uncover any evidence that the CETC joint venture or other relevant partnerships detaile here have been terminated.

Security Risks

Microsoft has also partnered with Feitian, a Beijing-based supplier of two-factor authentication products, to develop biometric security keys.[337] Feitian is a player in China's security ecosystem.[338] A 2021 report by *Top10VPN* found that Feitian had supplied USB keys for China's police and potentially the PLA.[339] In 2017, Feitian acquired Hongsi Electronics, which delivers security chips in conjunction with China's Office of State Commercial Cryptography Administration (OSCCA).[340] Feitian's role in Beijing's industrial and technology policy is evident in the subsidies that it receives. The company's 2021 semi-annual report more than 3 million RMB in subsidies for the first half of the year. Those include subsidies for a project on "Intelligent Network Identity Authentication System Engineering" run by the Beijing Academy of Science and Technology and a National Development and Reform Commission (NDRC)-funded project on encryption algorithms supporting the SM2 and SM4 algorithms of OSCCA, as well as "project funds for foreign trade companies to improve their international business capabilities."[341]

Endnotes

1 The authors are grateful for the guidance, feedback, and research support of a dedicated team of analysts led by Zoe R.

2 Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi, "Censorship, Surveillance, and Profits: A Hard Bargain for Apple in China," The New York Times, May 17, 2021, https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html; Eva Xiao, "China Used Twitter, Facebook More Than Ever Last Year for Xinjiang Propaganda," The Wall Street Journal, March 30, 2021, https://www.wsj.com/articles/china-used-twitter-facebook-more-than-ever-last-year-for-xinjiang-propaganda-11617101007; "Seven Apple Suppliers Accused of Using Forced Labor from Xinjiang," The Information, May 10, 2021. https://www.theinformation.com/articles/seven-apple-suppliers-accused-of-using-forced-labor-from-xinjiang

3 See: https://uyghurtribunal.com/wp-content/uploads/2022/01/Uyghur-Tribunal-Judgment-9th-Dec-21.pdf.

4 See, for example, "中科院自动化研究所与戴尔(中国)有限公司举行揭牌仪式 合作建立'人工智能与先进计算联合实验室' [The Institute of Automation of the Chinese Academy of Sciences and Dell (China) Co., Ltd. Held an Inauguration Ceremony to Jointly Establish the 'Artificial Intelligence and Advanced Computing Joint Laboratory']," it.people.com, March 8, 2016. http://web.archive.org/web/20220123172926/http://it.people.com.cn/n1/2016/0308/c403118-28182297.html; "北京市、英特尔和中国科学院联合成立'中国英特尔物联技术研究院' [Beijing, Intel and the Chinese Academy of Sciences Jointly Established the 'China Intel Institute of IoT Technology']," EEFocus, April 12, 2012. https://web.archive.org/web/20220123174014/https://www.eefocus.com/communication/298066..

5 See, for example, "广东省政府与微软公司签署战略合作协议 [Guangdong Provincial Government and Microsoft Signed a Strategic Cooperation Agreement]," People's Daily, October 14, 2014. https://web.archive.org/web/20211122145236/http://world.people.com.cn/n/2014/1014/c157278-25833273.html; "Shanghai-Amazon Web Services Joint Innovation Center," https://web.archive.org/web/20211119143738/https://www.amazonaws.cn/en/jib/shanghai/; "戴尔未来5年重点投资智慧城市 [Dell Will Focus on Investing in Smart Cities in the Next 5 Years]," IoT World, October 13, 2016. https://web.archive.org/web/20211119162230/http://www.iotworld.com.cn/html/News/201610/253a2fe108eccec9.shtml; "Ge与天津缔结战略合作共建智慧城市 [Ge and Tianjin Signed a Strategic Cooperation to Build a Smart City], GE, May 24, 2016. https://web.archive.org/web/20220124183707/https://www.ge.com/news/press-releases/ge%E4%B8%8E%E5%A4%A9%E6%B4%A5%E7%BC%94%E7%BB%93%E6%88%98%E7%95%A5%E5%90%88%E4%BD%9C%E5%85%B1%E5%BB%BA%E6%99%BA%E6%85%A7%E5%9F%8E%E5%B8%82 .

6 Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi, "Censorship, Surveillance, and Profits: A Hard Bargain for Apple in China," *The New York Times, May* 17, 2021. https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.

7 Ana Swanson, "Nike and Coca-Cola Lobby Against Xinjiang Forced Labor Bill," The New York Times, November 29, 2020. https://www.nytimes.com/2020/11/29/business/economy/nike-coca-cola-xinjiang-forced-labor-bill.html; Reed Albergotti, "Apple Is Lobbying against a Bill Aimed at Stopping Forced Labor in China," Washington Post, November 20, 2020. https://www.washingtonpost.com/technology/2020/11/20/apple-uighur/.

8 Supply chains are included within the partnerships category because the company is not in this case itself employing forced labor but rather sourcing from a separate actor exposed to this risk.

9 Uyghur Tribunal Judgment: https://uyghurtribunal.com/wp-content/uploads/2022/01/Uyghur-Tribunal-Judgment-9th-Dec-21.pdf.

10 “亚马逊与上海自贸区和信投的战略合作 [Strategic Cooperation Between Amazon and Shanghai Free Trade Zone and Xintou],” CNGold, August 20, 2014. https://web.archive.org/web/20211119135603/https://mip.cngold.org/forex/xw2713180.html.

11 Karen Weise, “Amazon Gives up on Chinese Domestic Shopping Business,” The New York Times, April 18, 2019. https://www.nytimes.com/2019/04/18/technology/amazon-china.html.

12 “上海-亚马逊AWS联合创新中心正式启用 [Shanghai-Amazon AWS Joint Innovation Center Officially Opened],” Sohu, June 29, 2018. https://www.sohu.com/a/238462194_185201; “上海-亚马逊AWS联合创新中心亮相2019上海静安国际大数据论坛 [Shanghai-Amazon AWS Joint Innovation Center at the 2019 Shanghai Jing’an International Big Data Forum],” Shanghai-Amazon AWS Joint Innovation Center Sohu Account, September 20, 2019. https://web.archive.org/web/20220123180754/https://www.sohu.com/a/342185736_120288603; “Shanghai-Amazon Web Services Joint Innovation Center,” https://web.archive.org/web/20211119143738/https://www.amazonaws.cn/en/jib/shanghai/.

13 Ibid. China’s smart cities are closely tied with its surveillance efforts. See, for example, Matthew Keegan, “In China, Smart Cities or Surveillance Cities,” US News and World Report, January 31, 2020.

14 “四月动态: SHA-JIC加入静安众创空间联盟，9家新入驻企业名单公布 [April News; SHA-JIC Joined the Jing’an Makerspace Alliance, and the List of 9 New Companies Announced],” Shanghai-AWS Joint Innovation Center Sohu Account, May 6, 2020. https://web.archive.org/web/20220123181349/https://www.sohu.com/a/393208189_120288603.

15 “2020年3月上海-亚马逊AWS联合创新中心入驻企业动态 [In March 2020, Shanghai-Amazon AWS Joint Innovation Center Settled in Enterprise Dynamics],” Shanghai-Amazon AWS Joint Innovation Center Sohu Account, March 28, 2020. https://web.archive.org/web/20220123182108/https://www.sohu.com/a/383907120_120288603.

16 “Company Profile,” Silong Intelligence. http://web.archive.org/web/20220201232003/http://www.soloai.com.cn/news-info/1175148.html.

17 Solutions, Silong Intelligence, Silong Intelligence. https://web.archive.org/web/20220123181655/http://www.soloai.com.cn/bxsznsbdb.

18 Solutions, Silong Intelligence, Silong Intelligence. https://web.archive.org/web/20220123181655/http://www.soloai.com.cn/bxsznsbdb.

19 As one press release puts it, “this means that the SDEC and other institutions are jointly responsible for various specific implementation tasks.” (“上海-亚马逊AWS联合创新中心启动将共同打造产业创新生态 [Shanghai-Amazon AWS Joint Innovation Center is Launched and Will Jointly Create an Industrial Innovation Ecosystem],” Shanghai Big Data Alliance, January 11, 2018. https://web.archive.org/web/20220123192022/https://www.sohu.com/a/216005191_468622) An example of a template Chinese “co-construction and implementation unit” agreement suggests that these partnerships can cover support in product design and research and development; provision of servers and server operation; development of software systems and technical architecture; joint intellectual property ownership and technology transfer agreements; and shared funding streams. (服务平台共建单位合作合同协议书范本 [Service Platform Co-Construction Unit Cooperation Contract Agreement Template]. https://web.archive.org/web/20220123192433/https://www.tspweb.com/key/%E5%B9%B3%E5%8F%B0%E6%9C%8D%E5%8A%A1%E5%90%88%E4%BD%9C%E5%90%88%E5%90%8C%E5%8D%8F%E8%AE%AE%E8%8C%83%E6%9C%AC.html).

20 上海数据交易中心介绍 [Introduction to the Shanghai Data Exchange Center], Shanghai Data Exchange Center, chinadep.com, https://web.archive.org/web/20220123192129/https://www.chinadep.com/#/.

21 “上海数据交易中心公共数据赋能普惠金融行业应用入选2019上海市大数据典型案例集 [Shanghai Data Exchange Center’s Public Data Empowerment of Inclusive Financial Industry Applications Was Selected into the 2019 Shanghai Big Data Typical Case Collection],” Shanghai Data Exchange Center Sohu Account, July 15, 2020. 2020. https://web.archive.org/web/20211119142147/https://www.sohu.com/a/407476891_622773.

22 “关于我们[About Us],” Shanghai Data Exchange Center. https://web.archive.org/web/20220123192129/https://www.chinadep.com/#/about.

23 “上海数据交易中心今日挂牌成立 剑指全球数据经济中心 [Shanghai Data Exchange Center Was Established Today, Aiming at the Global Data Economy Center],” Jiemian.com, April 1, 2016; 上海数据交易中心介绍 [Introduction to the Shanghai Data Exchange Center], Shanghai Data Exchange Center, chinadep.com, https://web.archive.org/web/20220123192129/ https://www.chinadep.com/#/ https://web.archive.org/web/20160403024414/http://www.jiemian.com/article/595764.html.

24 “2020数据安全高峰论坛在重庆举办 上海数据交易中心CEO汤奇峰发表主题演讲 [2020 Data Security Summit Forum is held in Chongqing, Shanghai Data Exchange CEO Tang Qifeng Delivers a Keynote Speech],” Shanghai Data Exchange Center Sohu Account, September 15, 2020. https://web.archive.org/web/20211119142600/https://www.sohu.com/a/418479761_622773.

25 “上海市发改委、上海市信用中心领导来访上海数据交易中心 [Leaders from Shanghai Development and Reform Commission and Shanghai Credit Center Visited Shanghai Data Exchange],” Shanghai Data Exchange Center Sohu Account, October 31, 2019. https://web.archive.org/web/20211119142705/https://www.sohu.com/a/350854798_622773.

26 “市委常委、市委统战部部长郑钢淼率队调研上海数据交易中心 [Zheng Gangmiao, Member of the Standing Committee of the Municipal Party Committee and Minister of the United Front Work Department of the Municipal Party Committee, Led a Team to Investigate the Shanghai Data Exchange Center],” Shanghai Data Exchange Center Sohu Account, May 13, 2019. https://web.archive.org/web/20211119142923/https://www.sohu.com/picture/313605153 For context on the United Front, see Alex Joske, *The Party Speaks for You: Foreign Interference and the Chinese Communist Party’s United Front System*, ASPI, June 2020. https://www.aspi.org.au/report/party-speaks-you.

27 See, for example, “China’s Overseas United Front Work and Implications for the United States,” US China Economic and Security Review Commission, August 24, 2018; “China’s Corporate Social Credit System,” Congressional Research Service, January 17, 2020. https://www.uscc.gov/files/000779.

28 “AWS全球副总裁Rudy Valdez莅临，上海大数据应用展示中心迎来第40000名来访者 [Rudy Valdez, AWS Global Vice President, Is Here, and Shanghai Big Data Application Exhibition Center Welcomes the 40,000th Visitor],” Shanghai Data Exchange Center Sohu Account, June 6, 2019. https://web.archive.org/web/20211119143141/https://www.sohu.com/a/318871133_622773.

29 Ibid.

30 Megha Rajagopalan and Alison Killing, “This Company Monitors Prisoners In Xinjiang. It Won An “Innovation” Award at An Event Sponsored by Amazon.,” Buzzfeed, April 19, 2021. https://www.buzzfeednews.com/article/meghara/amazon-xinjiang-prison-surveillance-award.

31 A wholly owned subsidiary of Amazon Technology Resources Co., Ltd that appears to serve as a Beijing-based operating company for AWS in China.

32 “青岛—亚马逊AWS联合创新中心正式运营 [Qingdao-Amazon AWS Joint Innovation Center Officially Operates],” Qingdao News, March 29, 2017. https://web.archive.org/web/20220124000429/https://news.qingdaonews.com/wap/2017-03/29/content_11986994.htm.

33 “亚马逊AWS布局：全球首个联合创新中心落户青岛 [Amazon AWS Layout: the World’s First Joint Innovation Center Settled in Qingdao],” Sohu, April 6, 2017. https://web.archive.org/web/20220124001510/https://www.sohu.com/a/132405738_117770.

34 Ibid.

35 西安与亚马逊AWS共建”西安联合创新中心” [Xi’an and Amazon AWS jointly build “Xi’an Joint Innovation Center”], China Business News, September 18, 2017: https://web.archive.org/web/20220124001704/https://www.sohu.com/a/192658660_351301. “Xi’an-AWS Joint Innovation Center,” https://web.archive.org/web/20220124001735/https://www.amazonaws.cn/en/jib/xian/.

36 “南京-亚马逊AWS联合创新中心正式启航 [Nanjing-Amazon AWS Joint Innovation Center Officially Set Sail], Zhihu, March 3, 2019. https://web.archive.org/web/20211119143530/https://zhuanlan.zhihu.com/p/58278774.

37 “上海-亚马逊AWS联合创新中心亮相2019上海静安国际大数据论坛 [Shanghai-Amazon AWS Joint Innovation Center unveiled at the 2019 Shanghai Jing’an International Big Data Forum],” Shanghai-Amazon AWS Joint Innovation Center Sohu Account, September 20, 2019. https://web.archive.org/web/20220123180754/https://www.sohu.com/a/342185736_120288603; “Shanghai-Amazon Web Services Joint Innovation Center,” https://web.archive.org/web/20211119143738/https://www.amazonaws.cn/en/jib/shanghai/.

38 “Chengdu-AWS Joint Innovation Center,” Amazon AWS China, https://web.archive.org/web/20211119143823/https://www.amazonaws.cn/en/jib/chengdu/.

39 See, for example, “Chengdu-AWS Joint Innovation Center,” https://web.archive.org/web/20211119143823/https://www.amazonaws.cn/en/jib/chengdu/.

40 “亚马逊宁夏项目困局：三年换了四任董事长，云业务仍飘在天上 [Amazon Ningxia Project Dilemma: After Three Years of Changing Four Chairman, Cloud Business Is Still Floating in the Sky],” Yicai, November 16, 2017. https://web.archive.org/web/20220124003851/http://tech.sina.com.cn/it/2017-11-16/doc-ifynwhww5335521.shtml.

41 Ibid.

42 “亚马逊云计算中卫合作项目二期推进会顺利召开 [The Second Phase Promotion Meeting of the Amazon Cloud Computing Zhongwei Cooperation Project was Successfully Held],” Zhongwei City Cloud Computing and Big Data Development Services Bureau, March 4, 2019. https://web.archive.org/web/20211119144503/http://www.nxzw.gov.cn/zjzw/xbyjd/201903/t20190304_1297214.html.

43 Ibid.

44 “云’聚中卫大境开 [‘Cloud’ Gathers in Zhongwei],” Xinhua, October 13, 2021. https://web.archive.org/web/20211014031845/http://finance.people.com.cn/n1/2021/1013/c1004-32252769.html; “李建华：把云基地打造成西部云产业高地 [Li Jianhua: Build the Cloud Base into a Cloud Industry Highland in the West],” Ningxia Daily, June 7, 2016. https://web.archive.org/web/20211119145251/http://www.cac.gov.cn/2016-06/07/c_1119005269.htm?from=singlemessage; DOD Releases List of Additional Companies, in Accordance with Section 1237 of FY99 NDAA, Department of Defense, August 28, 2020. https://www.defense.gov/News/Releases/Release/Article/2328894/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/.

45 “李建华：把云基地打造成西部云产业高地 [Li Jianhua: Build the Cloud Base into a Cloud Industry Highland in the West],” Ningxia Daily, June 7, 2016. https://web.archive.org/web/20211119145251/http://www.cac.gov.cn/2016-06/07/c_1119005269.htm?from=singlemessage.

46 See, for example, “中国气象局与战保局共商军民融合发展 [China Meteorological Administration and War Insurance Bureau Discuss Military-Civilian Fusion Development],” China Meteorological Network, February 5, 2016. https://web.archive.org/web/20211119145445/http://www.cma.gov.cn/2011xwzx/2011xqxxw/2011xqxyw/201602/t20160205_303802.html.

47 See, for example, “中国资源卫星应用中心：目前管理15颗在轨卫星_中国航天科技 [China Resources Satellite Application Center: Currently Manages 15 Satellites in Orbit],” Space China, May 15, 2017. https://web.archive.org/web/20211119145557/http://www.spacechina.com/n25/n148/n272/n4789/c1652372/content.html.

48 DOD Releases List of Additional Companies, in Accordance with Section 1237 of FY99 NDAA, Department of Defense, August 28, 2020. https://www.defense.gov/News/Releases/Release/Article/2328894/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/.

49 宁夏西云数据科技有限公司该公司所有职位民营公司 [Ningxia West Cloud Data Technology Co., Ltd. All Positions in the Company], 51Job. http://web.archive.org/web/20220125164644/https://jobs.51job.com/all/co4824077.html; “2021云天大会 云计算产业高质量发展’双碳’ 论坛在中卫举行 [2021 Yuntian Conference Cloud Computing Industry High-Quality Development ‘Double Carbon’ Forum Held in Zhongwei],” China Daily, October 17, 2021. https://web.archive.org/web/20220201233557/https://cn.chinadaily.com.cn/a/202110/17/WS616be29aa3107be4979f302c.html; “云计算技术与创新分论坛—— 宁夏西云数据科技有限公司助力中卫驾云逐梦 [Cloud Computing Technology and Innovation Sub-Forum - Ningxia West Cloud Data Technology Co., Ltd. Helps Zhongwei Drive the Cloud to Pursue Dreams]”, Zhongwei News Network, October 19, 2021. https://web.archive.org/web/20220125165207/http://news.nxtv.com.cn/nxnews/zwnews/2019-10-17/494484.html.

50 “中国电信与亚马逊建立战略合作关系 [China Telecom and Amazon Have Established a Strategic Partnership],” TVOAO, April 18, 2013. https://web.archive.org/web/20211119145826/https://www.tvoao.com/a/90425.aspx.

51 “亚马逊中国与中国联通建立4G业务战略合作伙伴关系 [Amazon China and China Unicom Establish a 4G Business Strategic Partnership],” TVOAO, March 21, 2014. https://web.archive.org/web/20211119150116/https://www.tvoao.com/a/160859.aspx.

52 “刘敏出席亚马孙中国移动战略合作发布会 [Liu Min Attended the Amazon China Mobile Strategic Cooperation Conference],” 360doc.cn, June 28, 2017. / web/20211119150006/http://www.360doc.cn/mip/667111859.html.

53 “刘敏出席亚马孙中国移动战略合作发布会 [Liu Min Attended the Amazon China Mobile Strategic Cooperation Conference],” 360doc.cn, June 28, 2017. https://web.archive.org/web/20211119150006/http://www.360doc.cn/mip/667111859.html.

54 “Amazon Supplier List,” https://d39w7f4ix9f5s9.cloudfront.net/cb/19/77dfc5b441c892cd6e2be166ba70/final-amazon-supplier-list-2019-11-14-updated-1005am.pdf.

55 Vicky Xiuzhong Xu et al., “Uyghurs for Sale,” Australian Strategic Policy Institute, March 1, 2020. https://www.aspi.org.au/report/uyghurs-sale.

56 “Amazon’s updated response to the Australian Strategic Policy Institute’s Report on Forced Labour of Ethnic Minorities from Xinjiang,” Business and Human Rights Resource Centre, October 2, 2020. https://www.business-humanrights.org/en/latest-news/amazons-updated-response-to-the-australian-strategic-policy-institutes-report-on-forced-labour-of-ethnic-minorities-from-xinjiang/.

57 Coalition to End Uyghur Forced Labour, “Brands,” https://enduyghurforcedlabour.org/brands/.

58 Gareth Chamberlain “Schoolchildren in China work overnight to produce Amazon Alexa devices,” The Guardian, August 8, 2019. https://www.theguardian.com/global-development/2019/aug/08/schoolchildren-in-china-work-overnight-to-produce-amazon-alexa-devices.

59 “Amazon’s Supplier Factory Foxconn Recruits Illegally: Interns Forced to Work Overtime,” China Labor Watch, August 8, 2019. https://chinalaborwatch.org/amazons-supplier-factory-foxconn-recruits-illegally-interns-forced-to-work-overtime/.

60 Ibid.

61 “苹果（乌兰察布）数据中心项目今日举行开工仪式 [Apple (Ulanchabu) Data Center Project Held a Groundbreaking Ceremony Today],” China IDC Circle News, March 15, 2019. https://web.archive.org/web/20220124010104/https://www.sohu.com/a/301450383_210640.

62 “Huawei Cloud,” baxtel.com, https://web.archive.org / web/20220124011232/https://baxtel.com/data-center/huawei-cloud.

63 “苹果（乌兰察布）数据中心项目今日举行开工仪式 [Apple (Ulanchabu) Data Center Project Held a Groundbreaking Ceremony Today],” China IDC Circle News, March 15, 2019. https://web.archive.org/web/20220124010104/https://www.sohu.com/a/301450383_210640.

64 For additional context, see, for example, Alex Joske, “The Party Speaks for You: Foreign interference and the Chinese Communist Party’s united front system,” Australian Strategic Policy Institute, June 9, 2020. https://www.aspi.org.au/report/party-speaks-you.

65 “‘2019年集宁区“就业扶贫’大型现场招聘会将于4月27日在集宁举行 [The 2019 Jining District ‘Employment Poverty Alleviation’ Large-Scale On-Site Job Fair Will be Held in Jining on April 27],” Sohu, April 23, 2019, https://web.archive.org/web/20220124010544/https://www.sohu.com/a/309784762_469808.

66 集宁区着力稳就业扩就业 [Jining District Strives to Stabilize Employment and Expand Employment], Xiaoxiang Morning News, February 26, 2021. http://www.wulanchabu.gov.cn/information/wlcbzfw11667/msg2849758338224.html.

67 Jack Nicas, Raymond Zhong, Daisuke Wakabayashi, “Censorship, Surveillance and Profits: A Hard Bargain for Apple in China,” *The New York Times,* May 17, 2021. https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html; Wayne Ma, “Seven Apple Suppliers Accused of Using Forced Labor from Xinjiang,” The Information, May 10, 2021. https://www.theinformation.com/articles/seven-apple-suppliers-accused-of-using-forced-labor-from-xinjiang; Vicky Xiuzhong Xu et al., “Uyghurs for Sale,” Australian Strategic Policy Institute, March 1, 2020. https://www.aspi.org.au/report/uyghurs-sale.

68 “Apple Diversifies Supply Chain But Keeps China at the Center,” The Verdict, June 18, 2021. https://www.verdict.co.uk/apple-supply-chain-china/.

69 Kif Leswing, “Apple Reports another Blowout Quarter with Sales up 54%, Authorizes $90 billion in Share Buybacks,” CNBC, April 28, 2021. https://www.cnbc.com/2021/04/28/apple-aapl-earnings-q2-2021.html.

70 “苹果:中国内地的iCloud服务将转由国内公司负责运营 [Apple: iCloud Services in Mainland China Will Be Transferred to Domestic Companies to Operate],” People’s Daily, January 10, 2018. https://web.archive.org/web/20220124012324/https://www.thepaper.cn/newsDetail_forward_1943524.

71 Ibid.

72 Ibid.

73 Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi, "Censorship, Surveillance, and Profits: A Hard Bargain for Apple in China," *The New York Times,* May 17, 2021. https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.

74 James Clayton, "Apple Takes Down Quran App in China," BBC, October 15, 2021. https://www.bbc.com/news/technology-58921230.

75 "Transparency Report: China Mainland," Apple, https://www.apple.com/legal/transparency/cn.html.

76 "巴音郭楞：上线'慧眼识诈' 即时发布高发案预警 [Bayinguo Leng: Launching 'Smart Eyes to Identify Frauds' Immediately Issue High-Risk Case Warnings]," China Police Network, September 12, 2020.

77 See, for example: http://web.archive.org/web/20220125145401/http://www.962.net/iossoft/550338.html.

78 "清华大学与苹果公司成立智能移动技术联合研究中心, [Tsinghua University and Apple Establish a Joint Research Center for Smart Mobile Technology]," QQ, September 4, 2018. https://web.archive.org/web/20220124013534/https://new.qq.com/cmsn/20180904/20180904086781.html?pc.

79 "中国自主智能手机将走军民之路 [China Autonomous and Controllable Mobile Phone Operating System Will Take the Road of Military-Civil Fusion]," China News Network, September 21, 2017. https://web.archive.org/web/20171126085540/http://cx.xinhuanet.com/2017-09/22/c_136629594.htm.

80 Ana Swanson, "Nike and Coca-Cola Lobby Against Xinjiang Forced Labor Bill," The New York Times, November 29, 2020. https://www.nytimes.com/2020/11/29/business/economy/nike-coca-cola-xinjiang-forced-labor-bill.html.

81 See, for example: Catherine Shu, "Apple CEO Tim Cook Met with China's Top Internet Regulator this Week," Tech Crunch, May 19, 2016. https://techcrunch.com/2016/05/19/apple-china-miit/.

82 "工信部部长苗圩会见苹果CEO库克 [Minister of Industry and Information Technology Miao Wei met with Apple CEO Cook]," QQ, May 19, 2016. https://web.archive.org/web/20160519102250/https://tech.qq.com/a/20160519/059431.htm.

83 Shannon Liao, "Apple's Tim Cook and Google's Sundar Pichai Were Surprise Guests at China's Internet Conference," The Verge, December 4, 2017. https://www.theverge.com/2017/12/4/16733202/china-apple-google-tim-cook-sundar-pichai-open-internet-surprise-guests.

84 "今年世界互联网大会将举行 设置5板块20分论坛 [This Year's World Internet Conference Will Hold 5 Sections and 20 Sub-Forums], Beijing News, November 17, 2017. https://web.archive.org/web/20220124014254/https://www.chinanews.com.cn/cj/2017/11-17/8378738.shtml.

85 "China Development Forum scheduled for later this month with largest foreign attendance," Global Times, March 15, 2021. https://web.archive.org/web/20220124014426/https://www.globaltimes.cn/page/202103/1218449.shtml.

86 Sami Fathi, "Tim Cook Attending Chinese Development Conference Later This Month," Mac Rumors, March 15, 2021. https://www.macrumors.com/2021/03/15/tim-cook-chinese-development-forum-2021/.

87 Ana Swanson, "Nike and Coca-Cola Lobby Against Xinjiang Forced Labor Bill," The New York Times, November 29, 2020. https://www.nytimes.com/2020/11/29/business/economy/nike-coca-cola-xinjiang-forced-labor-bill.html.

88 Vicky Xiuzhong et al, "Uyghurs for Sale," Australian Strategic Policy Institute, 2019. https://www.aspi.org.au/report/uyghurs-sale.

89 See: https://www.apple.com/supplier-responsibility/pdf/Apple-Supplier-List.pdf.

90 Vicky Xiuzhong et al, "Uyghurs for Sale," Australian Strategic Policy Institute, 2019. https://www.aspi.org.au/report/uyghurs-sale.

91 “元宇宙能否让千亿市值的歌尔股份再次起飞？[Can Metaverse Allow Goertek’s shares, Which Have a Market Value of 100 billion Yuan, to Take off Again?],” Xueqiu, March 10, 2021. https://web.archive.org/web/20211119164423/https://xueqiu.com/1608947171/200394447; “歌尔股份表示，华为是公司长期合作的战略客户 [Goertek Stated that Huawei Is the Company’s Long-Term Strategic Customer],” Xueqiu, June 16, 2021. https://web.archive.org/web/20211119164518/https://xueqiu.com/6985073409/183114612; “重磅！总书记主持召开企业家座谈会！海康威视、高德红外、歌尔股份董事长在列 [Heavy! The General Secretary Presided Over a Symposium for Entrepreneurs! The Chairmen of Hikvision, AutoNavi, and Goertek Are Listed],” EastMoney, July 21, 2020. https://web.archive.org/web/20200725013317/http://finance.eastmoney.com/a/202007211564092860.html; “歌尔股份2021年半年报分析 [Analysis of GoerTek’s 2021 Semi-Annual Report],” Zhihu, August 27, 2021. https://web.archive.org/web/20220124015437/https://xueqiu.com/1983721775/195662880.

92 “头部企业在青岛系列报道丨歌尔：投资青岛，打造全球研发中心 [Reports from Leading Companies in Qingdao | Goertek: Invest in Qingdao to Build a Global R&D Center],” Qingdao News Net, May 20, 2020. https://web.archive.org/web/20211119152801/https://baijiahao.baidu.com/s?id=1667221194266904864&wfr=spider&for=pc.

93 Wayne Ma, “Seven Apple Suppliers Accused of Using Forced Labor from Xinjiang,” The Information, May 10, 2021. https://www.theinformation.com/articles/seven-apple-suppliers-accused-of-using-forced-labor-from-xinjiang.

94 “助力新基建发展 戴尔科技集团打出组合拳 [Facilitating the Development of New Infrastructure, Dell Technology Group Hits a Combo Box],” Xinhua, July 10, 2020. https://web.archive.org/web/20211119153010/http://www.xinhuanet.com/tech/2020-07/10/c_1126221946.htm.

95 Ibid.

96 Ibid.

97 Ibid. This language, and similar language like it throughout this profile, reveals Dell representatives in China lauding their collaboration with the Chinese state or Chinese Communist Party in flowery terms. Flowery phrases like these can be common ways for companies to ingratiate themselves with the Chinese state—boilerplate ways of doing business in the country. However, the evidence on the ground, as this profile seeks to convey, suggests that these words may have been more than empty niceties.

98 See, for example, Jane Edwards, “Dell Technologies Wins $2.5B Navy BPA for Commercial Software Licenses,” GovconWire, June 7, 2021. https://www.govconwire.com/2021/06/dell-technologies-wins-2-5b-navy-bpa-for-commercial-software-licenses/.

99 “戴尔全球副总裁石峰：我们是’南极本地企业’ [Shi Feng, Global Vice President of Dell: We Are a ‘Local Enterprise’],” The Paper, November 6, 2020. https://web.archive.org/web/20220124154326/https://www.thepaper.cn/newsDetail_forward_9867412.

100 “坚持在中国为中国戴尔助力体育数字化转型 [Persist in China’s Support for China’s Dell in the Digital Transformation of Sports],” Zhongguancun Online, July 28, 2021. https://web.archive.org/web/20211119153459/http://app.myzaker.com/news/article.php?pk=6100ceb18e9f091fae2dc12b&f=normal.

101 Ibid.

102 “戴尔看好中国经济高质量发展助力产业升级 [Dell is Optimistic about the High-Quality Development of China’s Economy to Promote Industrial Upgrading],” Xinhua News, April 14, 2019. http://web.archive.org/web/20211119153930/https://baijiahao.baidu.com/s?id=1630798640578501374&wfr=spider&for=pc.

103 “戴尔科技：顺境逆境宠辱不惊 “在中国，为中国” [Dell Technology: Prosperity and Adversity Do Not Be Surprised],” Dell Technology Group Sohu account, January 5, 2020. https://web.archive.org/web/20220124155654/https://www.sohu.com/a/442560231_282720.

104 “戴尔的中国精神：日拱一卒，志存高远 [Dell’s Chinese Spirit: Achieving One’s Day, Aspiring High],” Sohu, August 19, 2020. http://web.archive.org/web/20211119153609/https://www.sohu.com/a/413846869_100182703.

105 “助力新基建发展 戴尔科技集团打出组合拳 [Facilitating the Development of New Infrastructure, Dell Technology Group Hits a Combo Box], Xinhua, August 21, 2020. /web/20211119154416/https://baijiahao.baidu.com/s?id=1672083700387309151&wfr=spider&for=pc.

106 “Dell Technologies Global Offices,” Dell Technologies. https://www.delltechnologies.com/en-us/office-locations.htm.

107 了解戴尔科技集团大中华区 [Learn about Dell Technology Group Greater China], Dell China Sohu Account, May 23, 2019. https://web.archive.org/web/20220124160628/https://www.sohu.com/a/315853316_120045008.

108 Including Peking University, Beijing Normal University, Fudan University, Shanghai Jiaotong University, and Southwest Jiaotong University. ("十三年前10年，十三微生物2000人，戴尔中国本地化个人研究是如何实践的？[Thirteen Years Ago, There Were 10 People; How Did Dell China's Localized Personal Research Work?]," Sohu, January 4, 2020. https://web.archive.org/web/20211119154736/https://www.sohu.com/a/364676022_117561).

109 "戴尔的中国精神：日拱一卒，志存高远 [Dell's Chinese Spirit: Achieving One's Day, Aspiring High]," Sohu, August 19, 2020. http://web.archive.org/web/20211119153609/https://www.sohu.com/a/413846869_100182703.

110 "戴尔'在中国 为中国'祭出6大招 [Dell's 'In China for China' Offers 6 Big Moves]," People's Daily, March 9, 2016. https://web.archive.org/web/20211119154917/http://finance.people.com.cn/n1/2016/0309/c1004-28185666.html.

111 "助力《中国制造2025》戴尔将大力帮助企业实现数字化转型 [Helping "Made in China 2025" Dell Will Vigorously Help Enterprises Achieve Digital Transformation]," Sohu, December 1, 2017. https://web.archive.org/web/20220124163051/https://www.sohu.com/a/207837354_468699; "中科院战略咨询院与戴尔发布研究报告 [Chinese Academy of Sciences Strategic Consulting Institute and Dell Release Research Report]," Zhongguancun Online, July 10, 2020. https://web.archive.org/web/20211119155114/https://new.qq.com/omn/20200710/20200710A0KB9700.html.

112 "戴尔的中国精神：日拱一卒，志存高远 [Dell's Chinese Spirit: Achievement and Aspiration]," Sohu News, August 19, 2020. http://web.archive.org/web/20211119153522/https://www.sohu.com/a/413846869_100182703.

113 "戴尔看好中国经济高质量发展助力产业升级 [Dell is Optimistic about the High-Quality Development of China's Economy to Promote Industrial Upgrading]," Xinhua News, April 14, 2019. http://web.archive.org/web/20211119153930/https://baijiahao.baidu.com/s?id=1630798640578501374&wfr=spider&for=pc.

114 "十三年前10年，十三微生物2000人，戴尔中国本地化个人研究是如何实践的？[Thirteen Years Ago, There Were 10 People; How Did Dell China's Localized Personal Research Work?]," Sohu, January 4, 2020. https://web.archive.org/web/20211119154736/https://www.sohu.com/a/364676022_117561.

115 "国务院发展研究中心与戴尔共同发布一份重要报告 [The Development Research Center of the State Council and Dell Jointly Released an Important Report], Dell China, March 30, 2018. https://web.archive.org/web/20211119155552/https://baijiahao.baidu.com/s?id=1596330109354809740&wfr=spider&for=pc.

116 Ibid.

117 Ibid.

118 "中科院自动化研究所与戴尔(中国)有限公司举行揭牌仪式合作建立'人工智能与先进计算联合实验室' [The Institute of Automation of the Chinese Academy of Sciences and Dell (China) Co., Ltd. Held an Inauguration Ceremony to Jointly Establish the 'Artificial Intelligence and Advanced Computing Joint Laboratory']," it.people.com, March 8, 2016. http://web.archive.org/web/20220123172926/http://it.people.com.cn/n1/2016/0308/c403118-28182297.html.

119 Ibid.

120 For a thorough overview of CASIA and implications for international research collaborations, see: Jeff Stoff and Glenn Tiffert, "Eyes Wide Open: Ethical Risks in Research Collaboration with China," Hoover Institution, December 2021. https://www.hoover.org/research/eyes-wide-open-ethical-risks-research-collaboration-china.

121 "973计划项目 '面向公共安全的社会感知数据处理'课题验收会议在自动化所召开 [The Acceptance Meeting of the 973 Program Project 'Social Perception Data Processing for Public Safety' Was Held in the Institute of Automation]," CASIA, September 27, 2016. https://web.archive.org/web/20211119160137/https://www.cas.cn/yx/201609/t20160927_4576183.shtml.

122 "面向公共安全的社会感知数据处理 [Cyber-Physical Space Sensory Data Processing for Public Security]," 973 Program, Accessed November 2, 2021. https://web.archive.org/web/20200310015418/http://www.nlpr.ia.ac.cn/973/project.html.

123 "Profile," CASIA, https://web.archive.org/web/20210609011807/http://english.ia.cas.cn/au/bi/.

124 "中科院自动化所谭铁牛所长一行来新疆进行科技合作调研 [Director Tan Tieniu of the Institute of Automation of the Chinese Academy of Sciences and His Party Came to Xinjiang for Scientific and Technological Cooperation Research]," Chinese Academy of Sciences, April 2, 2007. https://web.archive.org//web/20211119160415/https://www.cas.cn/xw/yxdt/200704/t20070403_984090.shtml.

125 "中国科学院自动化研究所2018年11月招聘1名军工项目课题工作主管启事 [Notice from the Institute of Automation of the Chinese Academy of Sciences to Recruit a Director of Military Projects in in November 2018]," Graduate Recruitment Network, November 23, 2018. https://web.archive.org/web/20211119160521/http://www.100zp.com/Institute/2018/131494.html.

126 王欣刚 [Wang Xingang], CASIA, https://web.archive.org/web/20220124164959/http://www.ia.cas.cn/sourcedb_ia_cas/cn/iaexpert/200908/t20090804_2310523.html.

127 "自动化所军民融合创新中心党支部召开'诵读科学经典' [The Party Branch of the Military-civilian Integration Innovation Center of the Institute of Automation Held a 'Recitation of Science Classics']," Chinese Academy of Sciences, June 1, 2020. https://web.archive.org/web/20211119160638/http://www.bjb.cas.cn/djdt2016/202006/t20200601_5600783.html.

128 "自动化所与戴尔、国投创新签署战略合作备忘录 [Automation Institute Signed a Strategic Cooperation Memorandum with Dell and SDIC Innovation]," CASIA, November 11, 2017. https://web.archive.org/web/20211119160828/http://www.ia.cas.cn/xwzx/jryw/201711/t20171111_4890628.html.

129 Ibid.

130 "戴尔科技：在中国为中国 携手伙伴共攀数字化高峰 [Dell Technologies: In China for China, Join Hands with Partners to Climb the Peak of Digitalization]," People's Daily, November 18, 2020. https://web.archive.org/web/20211119161008/http://scitech.people.com.cn/n1/2020/1118/c434383-31935498.html.

131 Emily de La Bruyere, "China's Quest to Shape the World through Standards Setting," Hinrich Foundation, July 2021, https://www.hinrichfoundation.com/research/article/tech/china-quest-to-shape-the-world-through-standards-setting/.

132 "自动化所起草编制的团体标准'人工智能职业技能要求与评价 第1部分：计算机视觉'正式发布 [The Group Standard 'Artificial Intelligence Vocational Skill Requirements and Evaluation Part 1: Computer Vision' Drafted and Compiled by the Automation Institute Is Officially Released]," CASIA Sohu account, November 30, 2020. http://web.archive.org/web/20211119161127/https://www.sohu.com/a/435425053_120053921.

133 Chen Jie, "高性能计算正成为材料基因研究的助推"发动机" [High-Performance Computing Is Becoming a Booster 'Engine' for Material Gene Research]," Science and Technology Daily, June 17, 2020. http://web.archive.org/web/20211119161251/http://digitalpaper.stdaily.com/http_www.kjrb.com/kjwzb/images/2020-06/16/02/KJWZB2020061602.pdf.

134 See, for example, other Chinese HPC entities designated for export restrictions by the US Department of Commerce: https://www.federalregister.gov/documents/2019/06/24/2019-13245/addition-of-entities-to-the-entity-list-and-revision-of-an-entry-on-the-entity-list.

135 "戴尔与贵阳市政府签署合作备忘录 [Dell and Guiyang Municipal Government Signed a Memorandum of Cooperation]," China Net, January 21, 2015. https://web.archive.org/web/20220124170800/http://finance.ce.cn/rz/yx/201501/21/t20150121_4396436.shtml.

136 戴尔与贵阳政府签署深化战略合作备忘录 [Dell and Guiyang Government Signed a Memorandum of Understanding on Deepening Strategic Cooperation], Sohu, May 26, 2016. https://www.sohu.com/a/77327331_374240.

137 "戴尔未来5年重点投资智慧城市 [Dell Will Focus on Investing in Smart Cities in the Next 5 Years]," IoT World, October 13, 2016. https://web.archive.org/web/20211119162230/http://www.iotworld.com.cn/html/News/201610/253a2fe108eccec9.shtml As related press coverage put it: "In fact, Dell has already started looking for government partners in smart cities….Wuhou District, Chengdu took the lead in getting on the boat." ("智慧城市成戴尔投资热点 未来5年在华再砸1250亿美元 [Smart Cities Become Dell's Investment Hotspot, Spending Another $125 billion in China in the Next 5 Years]," Huaqiang Electronic Network, December 13, 2017. https://web.archive.org/web/20220124170445/https://tech.hqew.com/news_1996456).

138 "每日互动：与华为和戴尔等知名公司保持合作 [Daily Interactive: Maintain Cooperation with Well-Known Companies Such as Huawei and Dell]," Sohu News, March 12, 2019. https://web.archive.org/web/20211119162406/https://www.sohu.com/a/300615476_115124.

139 “中国电子与戴尔构建全面业务合作伙伴关系 [China Electronics and Dell to Build a Comprehensive Business Partnership],” China Electronics Corporation via China SASAC, January 21, 2015. https://web.archive.org/web/20220124171239/http://www.sasac.gov.cn/n2588025/n2588124/c3789991/content.html; “戴尔’在中国为中国’祭出6大招 [Dell ‘In China for China’ Offers 6 Big Moves],” People’s Daily, March 9, 2016. https://web.archive.org/web/20211119154917/http://finance.people.com.cn/n1/2016/0309/c1004-28185666.html; “同方牵手戴尔瞄准企业级市场 [Tongfang Partners with Dell to Target the Enterprise Market],” Economic Information, July 14, 2015. https://web.archive.org/web/20211119162720/http://www.jjckb.cn/2015-07/14/c_134409062.htm?from=timeline.

140 “戴尔中国与联通签署战略合作备忘录 共同推动5G及物联网技术发展 [Dell China and China Unicom Sign a Strategic Cooperation Memorandum to Jointly Promote the Development of 5G and Internet of Things Technology],” Sohu, April 24, 2019. https://web.archive.org/web/20211119162619/https://baijiahao.baidu.com/s?id=1631696923211665084&wfr=spider&for=pc.

141 “戴尔商用解决方案亮相国际科技博览会 [Dell Business Solutions Appear at the International Technology Expo],” Sohu, September 23, 2016. http://web.archive.org/web/20211119163158/https://www.sohu.com/a/114935806_114838.

142 “戴尔科技集团大中华区董事长兼总裁黄陈宏：防范网络攻击，戴尔三箭齐发 [Huang Chenhong, Chairman and President of Dell Technology Group Greater China: Preventing Cyber Attacks, Dell Launches Three Arrows],” China Electronics News, June 4, 2021. https://web.archive.org/web/20211119163449/https://www.sohu.com/a/470466944_121134737.

143 Valentine Weber et al, “China’s Surveillance State” Top 10 VPN. Aug 2021. https://www.top10vpn.com/research/huawei-china-surveillance-state/.

144 Ibid.

145 Vicky Xiuzhong et al, “Uyghurs for Sale,” ASPI. 2019. https://www.aspi.org.au/report/uyghurs-sale.

146 Partners, Hefei Bitland, https://web.archive.org/web/20220124171821/http://www.bitland.com/Partners.

147 “Urumqi Retail Account Manager at Dell Careers,” Dell Technologies. https://archive.is/xcJYA.

148 Newley Purnell, “Facebook Staff Fret Over China’s Ads Portraying Happy Muslims in Xinjiang,” The Wall Street Journal, April 2, 2021. https://www.wsj.com/articles/facebook-staff-fret-over-chinas-ads-portraying-happy-muslims-in-xinjiang-11617366096.

149 Ibid.

150 Eva Xiao, “China Used Twitter, Facebook More Than Ever Last Year for Xinjiang Propaganda,” The Wall Street Journal, March 30, 2021. https://www.wsj.com/articles/china-used-twitter-facebook-more-than-ever-last-year-for-xinjiang-propaganda-11617101007.

151 Ibid.

152 Taylor Hatmaker, “Facebook caught Chinese hackers using fake personas to target Uyghurs abroad,” Tech Crunch, March 24, 2021. https://techcrunch.com/2021/03/24/facebook-earth-empusa-evil-eye-china-uyghur/.

153 Newley Purnell, “Facebook Staff Fret Over China’s Ads Portraying Happy Muslims in Xinjiang,” The Wall Street Journal, April 2, 2021. https://www.wsj.com/articles/facebook-staff-fret-over-chinas-ads-portraying-happy-muslims-in-xinjiang-11617366096.

154 Ibid.

155 “China Blocks Access to Twitter, Facebook after Riots,” Tech Crunch, July 2009. https://techcrunch.com/2009/07/07/china-blocks-access-to-twitter-facebook-after-riots/.

156 “Instagram Appears Blocked in China,” BBC News, September 29, 2014. https://www.bbc.com/news/technology-29409533.

157 Alyssa Abkowitz et al, “Facebook Is Trying Everything to Re-Enter China—and It’s Not Working,” Wall Streeet Journal, January 30, 2017. https://www.wsj.com/articles/mark-zuckerbergs-beijing-blues-1485791106.

158 Mike Isaac “Facebook Said to Create Censorship Tool to Get Back into China,” The New York Times, November 22, 2016. https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html.

159 “Facebook落户杭州设创新中心 [Facebook Settled in Hangzhou to Set up an Innovation Center],” Boxun.com, July 31, 2018. https://web.archive.org/web/20220125005634/https://news.boxun.com/news/gb/china/2018/07/201807262010.shtml; Lucas Niewenhuis “Facebook’s Office in Hangzhou Was Very Short-Lived,” Sup China, July 25, 2018. https://supchina.com/2018/07/25/facebooks-office-in-hangzhou-china-was-very-short-lived/.

160 Lin Yang, “How Facebook’s Zuckerberg Went from Courting to Criticizing Beijing,” VoA News, September 5, 2020. https://www.voanews.com/a/silicon-valley-technology_how-face-books-zuckerberg-went-courting-criticizing-beijing/6195455.html.

161 Paul Mozur and Lin Qiqing, “How Facebook’s Tiny China Sales Floor Helps Generate Big Ad Money,” The New York Times, February 6, 2019. https://www.nytimes.com/2019/02/07/technology/facebook-china-internet.html.

162 Paresh Dave and Katie Paul, “Facebook Makes a New Ad Sales Push in China after Zuckerberg Criticizes the Country,” CNBC, January 7, 2020. https://www.cnbc.com/2020/01/07/facebook-makes-a-new-ad-sales-push-in-china.html.

163 “元宇宙能否让千亿市值的歌尔股份再次起飞？ [Can Metaverse Allow Goertek’s shares, Which Have a Market Value of 100 Billion Yuan, to Take off Again?],” Xueqiu, March 10, 2021. https://web.archive.org/web/20211119164423/https://xueqiu.com/1608947171/200394447.

164 “元宇宙能否让千亿市值的歌尔股份再次起飞？ [Can Metaverse Allow Goertek’s Shares, Which Have a Market Value of 100 billion Yuan, to Take off Again?],” Xueqiu, March 10, 2021. https://web.archive.org/web/20211119164423/https://xueqiu.com/1608947171/200394447; “歌尔股份表示，华为是公司长期合作的战略客户 [Goertek Stated that Huawei Is the Company’s Long-Term Strategic Customer],” *Xueqiu*, June 16, 2021. https://web.archive.org/web/20211119164518/https://xueqiu.com/6985073409/183114612; “重磅！总书记主持召开企业家座谈会！海康威视、高德红外、歌尔股份董事长在列 [Heavy! The General Secretary Presided Over a Symposium for Entrepreneurs! The Chairmen of Hikvision, AutoNavi, and Goertek Are Listed],” EastMoney, July 21, 2020. https://web.archive.org/web/20200725013317/http://finance.eastmoney.com/a/202007211564092860.html; “歌尔股份2021年半年报分析 [Analysis of GoerTek’s 2021 Semi-Annual Report],” Zhihu, August 27, 2021. https://web.archive.org/web/20220124015437/https://xueqiu.com/1983721775/195662880.

165 “头部企业在青岛系列报道丨歌尔：投资青岛，打造全球研发中心 [Reports from Leading Companies in Qingdao: Goertek: Invest in Qingdao to Build a Global R&D Center],” Qingdao News Net, May 20, 2020. https://web.archive.org/web/20211119152801/https://baijiahao.baidu.com/s?id=1667221194266904864&wfr=spider&for=pc.

166 Vicky Xiuzhong et al, “Uyghurs for Sale,” Australian Strategic Policy Institute. 2019. https://www.aspi.org.au/report/uyghurs-sale.

167 “咸宁为新疆籍有组织劳务输出开辟’绿色通道’ [Xianning Opens up a ‘Green Channel’ for the Export of Organized Labor Services from Xinjiang],” QCC News, May 18, 2018. https://web.archive.org/web/20220125150323/http://news.qcc.com/postnews/0de67a557f4ad972e7c05c34685a95ec.html.

168 “连续三年参展进博会 GE聚焦’智造’持续深耕中国市场 [Participating in CIIE for Three Consecutive Years, GE Focuses on ‘Smart Manufacturing’ and Continues to Deepen the Chinese Market],” People’s Daily, November 9, 2020. https://web.archive.org/web/20211119181104/https://baijiahao.baidu.com/s?id=1682843765477438671&wfr=spider&for=pc.

169 “中国航空工业集团公司和美国通用电气公司获’携手合作奖’ [Aviation Industry Corporation of China and General Electric Company of the United States Won the ‘Hand in Hand Award’],” Zhizhu Park. https://web.archive.org/web/20220124174623/http://www.zizhupark.com/news/view/2974.

170 “中航通用电气民用航电系统有限责任公司今日揭牌成立 [AVIC General Electric Civil Avionics System Co., Ltd. Was Inaugurated Today],” GE, October 20, 2012. http://web.archive.org/web/20220124174806/https://www.ge.com/news/press-releases/%E4%B8%AD%E8%88%AA%E9%80%9A%E7%94%A8%E7%94%B5%E6%B0%94%E6%B0%91%E7%94%A8%E8%88%AA%E7%94%B5%E7%B3%BB%E7%BB%9F%E6%9C%89%E9%99%90%E8%B4%A3%E4%BB%BB%E5%85%AC%E5%8F%B8%E4%BB%8A%E6%97%A5%E6%8F%AD%E7%89%8C%E6%88%90%E7%AB%8B.

171 园中之园-特色园区 [Garden in the Park-Special Park], AVIC CAE. http://web.archive.org/web/20220124174909/http://www.aviccae.com/info.asp?base_id=4.

172 David Barboza, Christopher Drew, and Steve Lohr, “G.E. to Share Jet Technology with China in New Joint Venture,” The New York Times, January 17, 2011. https://www.nytimes.com/2011/01/18/business/global/18plane.html.

173 "China's Boeing Wannabe Could Land in U.S. Government Crosshairs," Bloomberg News, October 13, 2020. https://www.bloomberg.com/news/features/2020-10-12/china-aerospace-firm-avic-raises-us-alarm-over-ties-to-ge-airbus.

174 "通用电气医疗健康集团将X光机全球总部搬至中国 [GE Healthcare Moves the Global Headquarters of X-ray Machines to China]," China Economic Net, July 26, 2011. https://web.archive.org/web/20211119181735/http://intl.ce.cn/specials/zxxx/201107/26/t20110726_22565198.shtml.

175 "我们的创新 [Our Innovation]," GE China. https://web.archive.org/web/20220124190421/https://www.ge.com/cn/company/research.

176 GE in China Fact Sheet," GE.com. https://www.ge.com/cn/sites/www.ge.com.cn/files/GE%20in%20China%20fact%20sheet%20EN.pdf.

177 "中国华电集团公司与成立合资公司，共拓中国能源应用市场 [China Huadian Corporation and the Establishment of a Joint Venture Company to Jointly Expand China's Energy Application Market]," General Electric, August 31, 2011. https://web.archive.org/web/20220124180519/https://www.ge.com/news/press-releases/%E4%B8%AD%E5%9B%BD%E5%8D%8E%E7%94%B5%E9%9B%86%E5%9B%A2%E5%85%AC%E5%8F%B8%E4%B8%8Ege%E6%88%90%E7%AB%8B%E5%90%88%E8%B5%84%E5%85%AC%E5%8F%B8%EF%BC%8C%E5%85%B1%E6%8B%93%E4%B8%AD%E5%9B%BD%E5%88%86%E5%B8%83%E5%BC%8F%E8%83%BD%E6%BA%90%E5%B8%82%E5%9C%BA.

178 Ibid.

179 "Shanghai Jiaotong University and GE China R&D Center Cooperate to Establish an Advanced Manufacturing Joint Laboratory in UM," University of Michigan, https://news.umich.edu/zh-hans/ge-um/.

180 In 2004, they established General Electric-Harbin Power-Nanjing Turbine Energy Service Co., Ltd. ("我国首家燃气轮机本土服务合资企业在秦开工 [China's First Local Gas Turbine Service Joint Venture Started]," Hebei Daily, October 23, 2004. https://web.archive.org/web/20041025131409/http://news.sina.com.cn/c/2004-10-23/10184012201s.shtml) In 2015 they joined hands to develop a gas power plant in Pakistan. ("GE and Harbin to Provide Large, High-Efficiency Gas Power Plant to Help Meet Energy Demand in Pakistan," GE, October 14, 2015. https://www.businesswire.com/news/home/20151014005988/en/GE-and-Harbin-to-Provide-Large-High-Efficiency-Gas-Power-Plant-to-Help-Meet-Energy-Demand-in-Pakistan) In 2020 the two companies announced that they would partner on a gas turbine project contracted by state-owned power utility Guangdong Energy Group Co., Ltd. ("GE and Harbin Electric Contracted to Boost China's Greater Bay Area Transition," Modern Power Systems, November 11, 2020. https://www.modernpowersystems.com/news/newsge-and-harbin-electric-contracted-to-boost-chinas-greater-bay-area-transition-8356555).

181 "GE新创新中心落户哈尔滨 [GE's New Innovation Center Settled in Harbin]," Economic Information Daily, March 31, 2014. https://web.archive.org/web/20220124182401/http://covid-19.chinadaily.com.cn/hqcj/gjcj/2014-03-31/content_11500762.html.

182 "通用电气（GE）哈尔滨创新中心成立 与哈电携手全力支持中国燃气发电产业发展 [General Electric (GE) Harbin Innovation Center Established]," GE, March 26, 2014. https://web.archive.org/web/20220124181902/https://www.ge.com/news/taxonomy/term/2221?page=6.

183 "军民融合哈电集团军民融合新举措—— 舰船动力装置维修服务保障三亚分中心正式成立 [Military-Civil Fusion: Harbin Electric Group's New Measures for Military-Civil Fusion-Ship Power Plant Maintenance Service Support Sanya Branch Was Formally Established]," Sina Finance, September 23, 2017. https://web.archive.org/web/20220124183823/http://finance.sina.com.cn/roll/2017-09-23/doc-ifymeswc9451846.shtml.

184 "哈电集团军民融合新举措—— 舰船动力装置维修服务保障三亚分中心正式成立 [HE Group's New Measure of Military-Civil Fusion - Ship Power Plant Maintenance Service Guarantee Sanya Sub-Center Was Officially Established]," East Money, August 24, 2017. https://web.archive.org/web/20220124183823/http://finance.sina.com.cn/roll/2017-09-23/doc-ifymeswc9451846.shtml.

185 军民融合哈电集团军民融合新举措—— 舰船动力装置维修服务保障三亚分中心正式成立 [Military-Civil Fusion: Harbin Electric Group's New Measures for Military-Civil Fusion-Ship Power Plant Maintenance Service Support Sanya Branch Was Formally Established], Sina Finance, September 23, 2017. https://web.archive.org/web/20220124183823/http://finance.sina.com.cn/roll/2017-09-23/doc-ifymeswc9451846.shtml.

186 Ibid.

187 新疆生产建设兵团第七师五五工业园区2×350MW热电联产项目2号机组顺利通过168小时试运行 [Unit 2 of the 2×350MW Combined Heat and Power Project in the Fifth Five Industrial Park of the 7th Division of Xinjiang Production and Construction Corps successfully passed the 168-hour trial operation], Harbin Electric Group, August 23, 2021. https://web.archive.org/web/20211119183438/https://m.bjx.com.cn/mnews/20210823/1171906.shtml.

188 "Treasury Sanctions Chinese Entity and Officials Pursuant to Global Magnitsky Human Rights Executive Order," *US Treasury.* July 31, 2020. https://home.treasury.gov/news/press-releases/sm1073.

189 GE与天津缔结战略合作共建智慧城市 [GE and Tianjin Signed a Strategic Cooperation to Build a Smart City], GE, May 24, 2016. https://web.archive.org/web/20220124183707/https://www.ge.com/news/press-releases/ge%E4%B8%8E%E5%A4%A9%E6%B4%A5%E7%BC%94%E7%BB%93%E6%88%98%E7%95%A5%E5%90%88%E4%BD%9C%E5%85%B1%E5%BB%BA%E6%99%BA%E6%85%A7%E5%9F%8E%E5%B8%82.

190 See, for example, Matthew Keegan, "In China, Smart Cities or Surveillance Cities?" *US News*, January 31, 2020. https://www.usnews.com/news/cities/articles/2020-01-31/are-chinas-smart-cities-really-surveillance-cities; James Kynge, "Exporting Chinese Surveillance: The Security Risks of 'Smart Cities,'" *Financial Times*, June 9, 2021. https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab.

191 "通用电气：助力中国EPC'一带一路' [General Electric: Helping China's EPC 'One Belt One Road']," People's Daily, October 24, 2015. https://web.archive.org/web/20211119183845/http://finance.people.com.cn/n/2015/1024/c1004-27734978.html; "中国电信与GE签署协议 共同打造工业互联网生态圈 [China Telecom and GE Signed an Agreement to Jointly Build an Industrial Internet Ecosystem], People's Daily, March 17, 2017. https://web.archive.org/web/20220124185558/http://www.xinhuanet.com/tech/2017-03/17/c_1120644590.htm.

192 "中国电信与GE签署协议 共同打造工业互联网生态圈 [China Telecom and GE Signed an Agreement to Jointly Build an Industrial Internet Ecosystem], People's Daily, March 17, 2017. https://web.archive.org/web/20220124185558/http://www.xinhuanet.com/tech/2017-03/17/c_1120644590.htm.

193 General Electric (China) Co., Ltd Urumqi Office [通用电气（中国）有限公司乌鲁木齐办事处]. https://web.archive.org/web/20220121030757/http://www.likuso.com/city32/75379.html.

194 US Department of State, "Xinjiang Supply Chain Business Advisory," https://www.state.gov/xinjiang-supply-chain-business-advisory/.

195 "中国华电与新疆摄影'能源领域战略合作框架协议' [China Huadian and Xinjiang Photography 'Strategic Cooperation Framework Agreement in the Energy Field']," Huadian Group, September 15, 2021. https://web.archive.org/web/20220124185613/https://guangfu.bjx.com.cn/news/20210915/1176998.shtml.

196 Ibid.

197 "福建首家Google AdWords体验中心落户厦门 [Fujian's First Google AdWords Experience Center Settled in Xiamen]," Page One, January 7, 2016. https://web.archive.org//web/20211119184731/https://www.sohu.com/a/53008637_128225.

198 "第一页受邀参加谷歌大中华区合作伙伴峰会 [First Page Was Invited to Participate in the Google Greater China Partner Summit]," Page One, December 13, 2017. http://web.archive.org/web/20211119184856/https://www.dyyseo.com/newsdetail_n209.

199 "Google 出海体验中心一览 [Overview of Google's Overseas Experience Center]," LinkedIn, https://web.archive.org/web/20220124191823/https://cn.linkedin.com/pulse/google-adwords%E4%B-D%93%E9%AA%8C%E4%B8%AD%E5%BF%83%E4%B8%80%E8%A7%88-%E6%99%AF%E9%9B%A8-%E4%BF%A1.

200 Ibid.

201 "最近成立很多google adwords 体验中心，请问成为体验中心的这些互联网广告公司的前途怎么样？[Recently, Many Google Adwords Experience Centers Have Been Established. What Is the Future of these Internet Advertising Companies that Become Experience Centers?]", Zhihu, January 15, 2016. https://web.archive.org/web/20211119185816/https://www.zhihu.com/question/38554652. As one of Google's local Chinese partners explains on LinkedIn, "since 2014, under the leadership of Google, our partners in various places have worked hand in hand with local governments to deepen foreign trade marketing techniques, teach companies to successfully reach overseas buyers through Google AdWords, and sell Chinese brands to the world." ("Google 出海体验中心一览 [Overview of Google's Overseas Experience Center]," LinkedIn, https://web.archive.org/web/20220124191823/https://cn.linkedin.com/pulse/google-adwords%E4%BD%93%E9%AA%8C%E4%B8%AD%E5%BF%83%E4%B8%80%E8%A7%88-%E6%99%AF%E9%9B%A8-%E4%BF%A1).

202 "广西领郡信息技术有限公司(Google AdWords 广西体验中心)招聘 [Guangxi Lingjun Information Technology Co., Ltd. (Google AdWords Guangxi Experience Center)]," Zhipin.com December 31, 2015. https://web.archive.org/web/20220124192402/https://www.zhipin.com/companys/f4f7294cb525b30a0HR82Ni6.html.

203 Matt Sheehan, "How Google Took on China—And Lost," MIT Technology Review, December 19, 2018. https://www.technologyreview.com/2018/12/19/138307/how-google-took-on-china-and-lost/.

204 "Google Removes Ads for Sites Helping to Get Past China's Censor," WARC, February 4, 2019. https://www.warc.com/newsandopinion/news/google-removes-ads-for-sites-helping-to-get-past-china's-censors/41885.

205 This profile offers a relatively extensive survey of Google's engagement with China because that engagement is limited. As a result, it covers operations and partnerships which, for other companies more involved in and exposed to problematic elements within China's system, would have fallen below the threshold of inclusion in the company's narrative profile in this report.

206 Matt Sheehan, "How Google Took on China—and Lost," *MIT Technology Review,* December 19, 2018. https://www.technologyreview.com/2018/12/19/138307/how-google-took-on-china-and-lost/.

207 Ibid.

208 Miguel Helft and David Barboza, "Google Shuts China Site in Dispute Over Censorship," *The New York Times*, March 22, 2010. https://www.nytimes.com/2010/03/23/technology/23google.html.

209 "最近成立很多google adwords 体验中心，请问成为体验中心的这些互联网广告公司的前途怎么样？[Recently, Many Google Adwords Experience Centers Have Been Established. What Is the Future of these Internet Advertising Companies that Become Experience Centers?]", Zhihu, January 15, 2016. https://web.archive.org/web/20211119185816/https://www.zhihu.com/question/38554652.

210 Ibid.

211 Jen Copestake, "Google China: Has Search Firm Put Google Dragonfly on hold?" *BBC News*. December 18, 2018. https://www.bbc.com/news/technology-46604085; Olivia Solon, "Google's 'Project Dragonfly' Censored Search Engine Triggers Protests." *NBC News.* January 17, 2019, https://www.nbcnews.com/tech/tech-news/google-s-project-dragonfly-censored-search-engine-triggers-protests-n960121.

212 "Google Looks to Promote TensorFlow AI-Building Software, Investment, Presence in China," Indian Express, October 31, 2017. https://indianexpress.com/article/technology/google-looks-to-promote-ai-building-software-investment-presence-in-china-4915314/; The framework has been implemented by JD.com and Xiaomi. It is also available at Google experience centers. ("让中国开发者更容易地使用 TensorFlow 打造人工智能应用 [Make It Easier for Chinese Developers to Use TensorFlow to Build Artificial Intelligence Applications]," *Developers Google Blog*, August 31 2017. / web/20211119190202/https://blog.csdn.net/jILRvRTrc/article/details/78100572).

213 "Waymo Sets up Subsidiary in Shanghai as Google Plans China Push," *Reuters*, August 24, 2018. https://www.reuters.com/article/us-waymo-china/waymo-sets-up-subsidiary-in-shanghai-as-google-plans-china-push-idUSKCN1L90BP.

214 Michael Grothaus, "Google and Softbank Invest in Chinese Truck-Hailing firm Manbang," *Fast Company*, April 24, 2018. https://www.wsj.com/articles/softbank-and-google-funds-to-invest-in-chinese-truck-hailing-firm-manbang-1524494553.

215 "满帮集团主营盈利靠财政补贴 进军同城业务被指"没戏 [Manbang Group's Main Profit Relies on Financial Subsidies to Enter the Same City Business, Accused of 'No Play']," *Sina Finance*, June 19, 2021. https://web.archive.org/web/20211119190303/https://baijiahao.baidu.com/s?id=1702926496779400582&wfr=spider&for=pc.

216 Vicky Xiuzhong et al, "Uyhurs for Sale," *ASPI*. 2019. https://www.aspi.org.au/report/uyghurs-sale.

217 Goertek Electronics, LinkedIn, https://www.linkedin.com/company/goertek-electronics.

218 "元宇宙能否让千亿市值的歌尔股份再次起飞？[Can Metaverse Allow Goertek's shares, Which Have a Market Value of 100 billion Yuan, to Take off Again?]," *Xueqiu*, March 10, 2021. https://web.archive.org/web/20211119164423/https://xueqiu.com/1608947171/200394447; "歌尔股份表示，华为是公司长期合作的战略客户 [Goertek Stated that Huawei Is the Company's Long-Term Strategic Customer]," *Xueqiu*, June 16, 2021. https://web.archive.org/web/20211119164518/https://xueqiu.com/6985073409/183114612; "重磅！总书记主持召开企业家座谈会！海康威视、高德红外、歌尔股份董事长在列 [Heavy! The General Secretary Presided Over a Symposium for Entrepreneurs! The Chairmen of Hikvision, AutoNavi, and Goertek Are Listed]," *EastMoney*, July 21, 2020. https://web.archive.org/web/20200725013317/http://finance.eastmoney.com/a/202007211564092860.html; "歌尔股份2021年半年报分析 [Analysis of GoerTek's 2021 Semi-Annual Report]," *Zhihu*, August 27, 2021. https://web.archive.org/web/20220124015437/https://xueqiu.com/1983721775/195662880.

219 "头部企业在青岛系列报道丨歌尔：投资青岛，打造全球研发中心 [Reports from Leading Companies in Qingdao | Goertek: Invest in Qingdao to Build a Global R&D Center]," *Qingdao News Net*, May 20, 2020. https://web.archive.org/web/20211119152801/https://baijiahao.baidu.com/s?id=1667221194266904864&wfr=spider&for=pc.

220 Its corporate documents describe support for military civil fusion. (飞天诚信：2020年度非公开发行股票募集资金使用的可行性分析报告 [Feitian Integrity: Feasibility Analysis Report on the Use of Funds Raised by Non-public Issuance of Shares in 2020], May 26, 2020. https://web.archive.com/web/20220124195348/https://q.stock.sohu.com/cn,gg,300386,5776113925.shtml).

221 Valentine Weber et al, "China's Surveillance State,"T*op10VPN,* August 2021. https://www.top10vpn.com/research/huawei-china-surveillance-state/.

222 飞天诚信：2020年度非公开发行股票募集资金使用的可行性分析报告 [Feitian Integrity: Feasibility Analysis Report on the Use of Funds Raised by Non-public Issuance of Shares in 2020], May 26, 2020. https://web.archive.com/web/20220124195348/https://q.stock.sohu.com/cn,gg,300386,5776113925.shtml; "飞天诚信：公司持有宏思电子91.49%的股份 [Feitian Integrity: The Company Holds 91.49% of Hongsi Electronics], Sohu, August 9, 2021. https://web.archive.org/web/20220124194347/https://www.sohu.com/a/482306673_115362; "北京宏思电子技术有限责任公司 [Beiing Hongsi Electronic Technology Company]," 51semicon.com, https://web.archive.org/web/20220124194724/http://www.51semicon.com/com/hongsi-ic/introduce/.

223 "飞天诚信科技股份有限公司: 2021 年半年度报告 [Feitian Integrity Technology Co., Ltd.: 2021 Semi-Annual Report]," July 2021. https://web.archive.org/web/20220125173549/https://pdf.dfcfw.com/pdf/H2_AN202107261506233822_1.pdf?1627322583000.pdf.

224 Dieter Bohn, "Google is Replacing Bluetooth Titan Security Keys Because of a Vulnerability," *The Verge*, May 15, 2019. https://www.theverge.com/2019/5/15/18625028/google-titan-security-keys-bluetooth-vulnerability-replacement-free.

225 "飞天诚信：公司供给微软、谷歌公司的产品目前处于启动期 [Feitian Integrity: The Company's Products for Microsoft and Google Are Currently in the Start-Up Period], *Securities Times*, December 23, 2020. https://web.archive.org/web/20211119191145/https://baijiahao.baidu.com/s?id=1686852194510888177&wfr=spider&for=pc; That same article described cooperation between Feitian and Microsoft in biometric security authentication.

226 "Secure Your Accounts with Google Advanced Protection," Feitian Integrity. https://web.archive.org/web/20220124200113/https://www.ftsafe.com/article/621.html.

227 飞天诚信：2020年度非公开发行股票募集资金使用的可行性分析报告 [Feitian Integrity: Feasibility Analysis Report on the Use of Funds Raised by Non-public Issuance of Shares in 2020], May 26, 2020. https://web.archive.com/web/20220124195348/https://q.stock.sohu.com/cn,gg,300386,5776113925.shtml.

228 Bruce Andrews, "US Competitiveness is at Stake for Chip Manufacturing," Intel, October 1, 2021. https://www.intel.com/content/www/us/en/newsroom/opinion/us-competitiveness-stake-chip-manufacturing.html#gs.e50py7.

229 Meghan Bobrowsky, "Intel to Invest at Least $20 Billion in Ohio Chip-Making Facility," *Wall Street Journal,* January 21, 2022, https://www.wsj.com/articles/intel-to-invest-at-least-20-billion-in-ohio-chip-making-facility-11642750760?mod=hp_lead_pos1.

230 "英特尔中国区总裁杨旭：我们要和中国一道共赢未来 [Yang Xu, President of Intel China: We Want to Win the Future Together with China]," Sohu News, September 24, 2019. https://web.archive.org/web/20220124200936/https://www.sohu.com/a/343026382_123753; "认识英特尔—根植中国 服务中国[Know Intel - Rooted in China to Serve China]", Intel.cn, https://web.archive.org/web/20220124201422/https://www.intel.cn/content/dam/www/public/cn/zh/pdfs/know-intel.pdf.

231 Worldwide Campus Locations," Intel, https://www.intel.sg/content/www/xa/en/support/contact-intel.html?tab=campus-locations#support-world-locations.

232 "英特尔中国区总裁杨旭：我们要和中国一道共赢未来 [Yang Xu, President of Intel China: We Want to Win the Future Together with China]," Sohu News, September 24, 2019. https://web.archive.org/web/20220124200936/https://www.sohu.com/a/343026382_123753; 认识英特尔—根植中国 服务中国[Know Intel - Rooted in China to Serve China]", Intel.cn.

233 "走进英特尔中国研究院：60人撑起四大研究领域 [Walk into Intel China Research Institute: 60 People Support Four Major Research Fields]," NetEase, December 13, 2018. http://web.archive.org/web/20220124201551/https://www.163.com/tech/article/E2T5F5UN00098IEO.html.

234 中国英特尔物联技术研究院正式挂牌投入运营 [China Intel IOT Technology Research Institute was Officially Listed and Put into Operation], Chinese Academy of Sciences Institute of Automation, November 28, 2012. https://web.archive.org/web/20220124203732/http://www.ia.cas.cn/xwzx/ttxw/201211/t20121128_3692007.html; Wu Wenliang, "英特尔中国研究院：技术与标准，双流驱动智能交通发展 [Intel China Research Institute: Technology and Standards, Shuangliu Drives the Development of Intelligent Transportation]," Leiphone, November 30, 2020. http://web.archive.org/web/20211119192054/https://baijiahao.baidu.com/s?id=1684800464987352905&wfr=spider&for=pc.

235 "如何布局量子科技？专访英特尔中国研究院院长：发展前沿计算需要'另一种眼光' [How to Deploy Quantum Technology? Interview with the Dean of Intel China Research Institute: The Development of Cutting-Edge Computing Requires Another Perspective]," China News Network, June 11, 2021. https://web.archive.org/web/20220124204234/https://www.sohu.com/a/471775198_123753.

236 "英特尔亚太地区应用设计中心落户深圳 [Intel Asia Pacific Application Design Center Settled in Shenzhen]," Fast Technology, October 31, 2002. http://web.archive.org/web/20211119192524/https://news.mydrivers.com/1/7/7132.htm.

237 Ibid.

238 "英特尔成都概览 [Overview of Intel Chengdu]," China Campus Jobs, https://web.archive.org/web/20220124203528/https://chinacampus.jobs.intel.cn/intel/home/index?page=chengdu.

239 Ibid.

240 "英特尔成都工厂完成认证，将可生产酷睿i9-9900K [Intel Chengdu Factory Completes Certification and Will Be Able to Produce Core i9-9900K]," IT Home via iFeng, June 21, 2019. https://web.archive.org/web/20220124204739/https://ishare.ifeng.com/c/s/7ngpMkCZclK.

241 "英特尔研发的中国布局 [Intel's China Research and Development Layout]," China Campus Jobs, https://web.archive.org/web/20220124204811/https://chinacampus.jobs.intel.cn/intel/home/index?page=rnd.

242 "缔造中国传奇——"神秘"的英特尔亚太研发中心 [Create a Chinese Legend-the "Mysterious" Intel Asia Pacific R&D Center]," Laoyaoba, October 27, 2010. http://web.archive.org/web/20211119193104/https://laoyaoba.com/html/share/news?news_id=618462.

243 "Intel 出售大连工厂！90 亿美元交易，让韩国主导世界 NAND 闪存，但我国已追上 [Intel sells Dalian Factory! US$9 Billion Transaction Has Allowed South Korea to Dominate the World's NAND Flash Memory, but China Has Caught Up]," Leifeng, October 20, 2020. https://web.archive.org/web/20211119193001/https://baijiahao.baidu.com/s?id=1681085860684910996&wfr=spider&for=pc.

244 Caroline Gabriel, "Trade wars don't stop Intel pursuing China with its expanding 5G range" *Rethink Research.* September 28, 2018. https://rethinkresearch.biz/articles/trade-wars-dont-stop-intel-pursuing-china-with-its-expanding-5g-range-2/.

245 Zhao Yuanchuang, "顶级半导体公司中国布局情况跟踪 [Tracking the Layout of Top Semiconductor Companies in China]," EETop, March 3, 2020. https://web.archive.org/web/20220124210509/https://www.sohu.com/a/377357837_458015.

246 "发力智能交通"新基建"，智慧交通研究院项目落户溧水开发区 [Efforts to Develop Smart Transportation "New Infrastructure", the Smart Transportation Research Institute Project Settled in Lishui Development Zone]," Lishui Development Zone, November 25, 2020. https://web.archive.org/web/20211119193427/https://baijiahao.baidu.com/s?id=1684239255999488717&wfr=spider&for=pc.

247 "北京市、英特尔和中国科学院联合成立'中国英特尔物联技术研究院' [Beijing, Intel and the Chinese Academy of Sciences Jointly Established the 'China Intel Institute of IoT Technology']," EEFocus, April 12, 2012. https://web.archive.org/web/20220123174014/https://www.eefocus.com/communication/298066.

248 "英特尔携手清华大学、中国科学院，入局自动驾驶研究 [Intel Joins Hands with Tsinghua University and Chinese Academy of Sciences to Enter Autonomous Driving Research]," People's Daily, May 31, 2018. / web/20211119193855/https://baijiahao.baidu.com/s?id=1601978456774566624&wfr=spider&for=pc.

249 For a thorough overview of CASIA and implications for international research collaborations, see: Jeff Stoff and Glenn Tiffert, "Eyes Wide Open: Ethical Risks in Research Collaboration with China," Hoover Institution, December 2021, https://www.hoover.org/research/eyes-wide-open-ethical-risks-research-collaboration-china.

250 "973计划项目 '面向公共安全的社会感知数据处理'课题验收会议在自动化所召开 [The acceptance meeting of the 973 Program Project 'Social Perception Data Processing for Public Safety' was held in the Institute of Automation]," CASIA, September 27, 2016. https://web.archive.org/web/20211119160137/https://www.cas.cn/yx/201609/t20160927_4576183.shtml.

251 "面向公共安全的社会感知数据处理 [Cyber-Physical Space Sensory Data Processing for Public Security]," 973 Program, Accessed November 2, 2021. https://web.archive.org/web/20200310015418/http://www.nlpr.ia.ac.cn/973/project.html.

252 "Profile," CASIA, https://web.archive.org/web/20210609011807/http://english.ia.cas.cn/au/bi/.

253 "中科院自动化所谭铁牛所长一行来新疆进行科技合作调研 [Director Tan Tieniu of the Institute of Automation of the Chinese Academy of Sciences and His Party Came to Xinjiang for Scientific and Technological Cooperation Research]," Chinese Academy of Sciences, April 2, 2007. https://web.archive.org//web/20211119160415/https://www.cas.cn/xw/yxdt/200704/t20070403_984090.shtml.

254 "中国科学院自动化研究所2018年11月招聘1名军工项目课题工作主管启事 [Notice from the Institute of Automation of the Chinese Academy of Sciences for the Recruitment of to Recruit a Director of Military Projects in November 2018]," Graduate Recruitment Network, November 23, 2018. https://web.archive.org/web/20211119160521/http://www.100zp.com/Institute/2018/131494.html.

255 王欣刚 [Wang Xingang], CASIA, https://web.archive.org/web/20220124164959/http://www.ia.cas.cn/sourcedb_ia_cas/cn/iaexpert/200908/t20090804_2310523.html.

256 "自动化所军民融合创新中心党支部召开'诵读科学经典' [The Party Branch of the Military-Civilian Fusion Innovation Center of the Institute of Automation held a 'Recitation of Science Classics']," Chinese Academy of Sciences, June 1, 2020. https://web.archive.org/web/20211119160638/http://www.bjb.cas.cn/djdt2016/202006/t20200601_5600783.html.

257 "英特尔与计算所建联合实验室 助高性能计算应用普及 [Intel and the Institute of Computing Technology Build a Joint Laboratory to Help Popularize High-Performance Computing Applications]," CNET, February 11, 2012. https://web.archive.org/web/20211119193535/http://zhuanti.cww.net.cn/tech/html//2012/11/2/20121121047451087.htm.

258 "英特尔（中国）代表一行参观先进院高性能计算中心 [Intel (China) Representatives Visited the Advanced Institute of High Performance Computing Center]," Center for High Performance Computing, January 19, 2021. https://web.archive.org/web/20211122134729/http://hpcc.siat.ac.cn/news/xwdt210119.html.

259 "英特尔助力贵阳建设'中国数谷' [Intel Helps Guiyang Build 'China's Digital Valley']," Economic Information Daily, June 29, 2015. https://web.archive.org/web/20220124213147/https://world.huanqiu.com/article/9CaKrnJMvmI.

260 "中国人工智能开放创新平台下个月在贵阳正式投入运营 [China's Artificial Intelligence Open Innovation Platform Will be Officially Put into Operation in Guiyang Next Month], Guiyang Government Website, December 12, 2017.

261 "利用大数据分析改进交通管理 [Use Big data Analysis to Improve Traffic Management]," Intel China, Accessed November 12, 2021. https://web.archive.org/web/20211122135029/https://www.intel.com/content/dam/www/public/cn/zh/pdfs/trustway-casestudy.PDF.

262 "深化知识产权合作 推动创新发展: 工业和信息化部电子知识产权中心与英特尔公司结成战略伙伴关系 [Deepen Intellectual Property Cooperation and Promote Innovation and Development: The Electronic Intellectual Property Center of the Ministry of Industry and Information Technology and Intel Form a Strategic Partnership]," Microcomputer World, 2011(3). https://web.archive.org/web/20211122135232/https://xueshu.baidu.com/usercenter/paper/show?paperid=4f2daea3a1a67b045d2a11bfc4e064f4&site=xueshu_se.

263 "工信部副部长罗文15日会见美国英特尔CEO科再奇 [Vice Minister of Industry and Information Technology Luo Wen Met with Intel CEO on the 15th]," MIIT Website, December 20, 2017. https://web.archive.org/web/20211122135255/http://news.jstv.com/a/20171220/1513740105388.shtml.

264 "工信部副部长会见英特尔CEO：中国集成电路市场巨大 [Vice Minister of Industry and Information Technology Meets with Intel CEO: China's IC Market is Huge]," Observer Network, April 30, 2019. https://web.archive.org/web/20211122135352/https://baijiahao.baidu.com/s?id=1632228174866470909&wfr=spider&for=pc.

265 "创新应用、共赢5G，英特尔携手产业伙伴加速5G应用落地 [Innovative Applications and Win-Win 5G, Intel and Industry Partners Accelerate the Implementation of 5G Applications]," PT Expo, November 6, 2019. https://web.archive.org/web/20220124215141/https://tech.sina.com.cn/roll/2019-11-06/doc-iicezzrr7640815.shtml.

266 Ibid.

267 "开放数据中心委员会成立 [Open Data Center Committee Established]," IDC Quan, September 11, 2014. https://web.archive.org/web/20220124215228/http://news.idcquan.com/news/60852.shtml'开放数据中心委员会介绍 [Introducing the Open Data Center Council], OODC.org.cn, https://web.archive.org/web/20220124220846/http://www.odcc.org.cn/introduction.html.

268 "Zhao Yuanchuang, "顶级半导体公司中国布局情况跟踪 [Tracking the Layout of Top Semiconductor Companies in China]," EETop, March 3, 2020. https://web.archive.org/web/20211122135810/https://www.sohu.com/a/377357837_458015.

269 For background on Intel's stake see: https://www.marketscreener.com/quote/stock/INTEL-CORPORATION-4829/news/Intel-UNISOC-Completes-Equity-Restructuring-Promotes-IPO-Process-30914908/.

270 "紫光成立合资公司，Intel却不能有姓名 [Tsinghua Unigroup Established a Joint Venture Company, but Intel Cannot Have a Name], October 19, 2019. https://web.archive.org/web/20211122135857/http://mp.ofweek.com/ee/a045683021816.

271 澜起科技十大股东一 [List of Top Ten Shareholders in Lanqi Technology], East Money, https://web.archive.org/web/20220124222120/http://data.eastmoney.com/gdfx/stock/688008.html.

272 总投资20亿！英特尔与澜起、清华合作研发芯片.

[The Total Investment Is 2 billion! Intel Cooperates with Lanqi and Tsinghua to Develop Chips], March 31, 2017. https://web.archive.org/web/20211122140044/https://m.sohu.com/n/485838544/.

273 "澜起科技(688008)：津逮服务器持续超预期 [Montage Technology (688008): Jintide Server Continues to Exceed Expectations]," Orient Securities Co., Ltd, August 11, 2021. https://web.archive.org/web/20220124222134/http://stock.finance.sina.com.cn/stock/go.php/vReport_Show/kind/search/rptid/682008961384/index.phtml.

274 "澜起科技(688008)：津逮服务器持续超预期 [Montage Technology (688008): Jintide Server Continues to Exceed Expectations]," Orient Securities Co., Ltd, August 11, 2021. https://web.archive.org/web/20220124222134/http://stock.finance.sina.com.cn/stock/go.php/vReport_Show/kind/search/rptid/682008961384/index.phtml.

275 澜起科技宣布DDR5第一子代内存接口及模组配套芯片实现量产 [Lanqi Technology Announces Mass Production of DDR5 First Generation Memory Interface and Module Supporting Chips], EET China, October 29, 2021. https://web.archive.org/web/20220124222156/https://www.eet-china.com/mp/a86463.html.

276 澜起科技(688008)公司深度研究报告：引领内存接口芯片全球标准 津逮平台&AI 芯片开辟新蓝海 [Lanqi Technology (688008) Company In-Depth Research Report: Leading the Global Standard of Memory Interface Chip Jintide platform & AI chip Opens up a New Blue Ocean], West China Securities Co., Ltd, October 8, 2019. https://web.archive.org/web/20220124223216/http://stock.finance.sina.com.cn/stock/go.php/vReport_Show/kind/search/rptid/623849447882/index.phtml.

277 A corresponding October 2019 Federal Register notice is accessible online: https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list.

278 "英特尔与海康威视：十年合作深耕 人工智能全面布局安防监控 [Intel and Hikvision: Ten Years of Cooperation Deeply Plowing Artificial Intelligence Comprehensive Layout for Security Monitoring]," Intel Hikvision Artificial Intelligence, September 23, 2017. https://web.archive.org/web/20211122141148/https://www.prnasia.com/story/189056-1.shtml.

279 "英特尔助力海康威视打造"深眸"全局摄像机，推进视频监控智能化-英特尔[Intel Assists Hikvision in Creating a "Deep Eye" Global Camera, Advancing the Intelligentization of Video Surveillance-Intel], Intel.cn,. https://web.archive.org/web/20220124223310/https://www.intel.cn/content/www/cn/zh/analytics/artificial-intelligence/intel-power-hikvision-create-deep-eyes-global-video-camera.html.

280 A corresponding October 2019 Federal Register notice is accessible online: https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list.

281 "海康威视被列入实体清单，英特尔回应：将帮助客户减少冲击 [Hikvision Was Included in the List of Entities, Intel Responded: Will Help Customers Reduce the Impact]," Semiconductor Investment Alliance, October 8, 2019. https://web.archive.com/web/20211122141241/https://baijiahao.baidu.com/s?id=1646820514457043572&wfr=spider&for=pc.

282 "Dell, HP, Microsoft, Intel Oppose Proposed Tariffs on Laptops, Tablets," *Reuters*, June 19. 2019. https://www.reuters.com/article/us-usa-tech-tariffs/dell-hp-microsoft-intel-oppose-proposed-tariffs-on-laptops-tablets-idUSKCN1TK33V.

283 "英特尔与中国联通战略合作 共推全互联PC [Intel and China Unicom Strategically Cooperate to Promote Fully Connected PCs]," Xinhua, May 31, 2018. https://web.archive.org/save/https://baijiahao.baidu.com/s?id=1601867064080344782&wfr=spider&for=pc.

284 "英特尔与中国移动签署战略合作协议 [Intel and China Mobile Signed a Strategic Cooperation Agreement]," Intel China, December 6, 2018. https://web.archive.org/web/20220124224032/https://newsroom.intel.cn/news-releases/press-relase-2018-dec-06-01/.

285 Liza Lin and Josh Chin, "U.S. Tech Companies Prop Up China's Vast Surveillance Network," The Wall Street Journal, November 26, 2019. https://www.wsj.com/articles/u-s-tech-companies-prop-up-chinas-vast-surveillance-network-11574786846.

286 Don Clark, "当美国技术为中国监控新疆提供助力 [When U.S. Technology Helps China Monitor Xinjiang]," The New York Times, November 23, 2020. https://cn.nytimes.com/technology/20201123/china-intel-nvidia-xinjiang/.

287 "Xinjiang: Chairs Ask CEOs of Intel and NVIDIA About Possible Involvement in Human Rights Abuses," Congressional Executive Commission on China, December 8, 2020. https://www.cecc.gov/media-center/press-releases/chairs-ask-ceos-of-intel-and-nvidia-about-possible-involvement-in-human.

288 新疆出入境边防检查总站边境智能管控系统采购项目中标公告 [Announcement on Winning the Bid for the Procurement Project of Border Intelligent Control System of Xinjiang Entry-Exit Border Inspection Station], China Ministry of Commerce, September 3, 2021. https://web.archive.org / web/20220125152652/http://www.ccgp.gov.cn/cggg/dfgg/zbgg/202109/t20210903_16826947.htm.

289 沙雅县公安局关于硬盘 2个，相机热靴收声器 1个等的在线询价公告 [Shaya County Public Security Bureau's online inquiry Announcement on 2 Hard Drives, 1 Camera Microphone, etc.], Shaya County Public Security Bureau, April 17, 2020. https://www.chinabidding.cn/zfcg/neWRb7.html.

290 昌吉回族自治州公安局关于数据库服务器 1台，比对服务器 1台等的在线询价公告 [Public Security Bureau of Changji Hui Autonomous Prefecture Announcement on Online Quotation of 1 Database Server, 1 Comparison Server, etc.], Changji Hui Autonomous Prefecture Public Security, April 9, 2020. http://zb.yfb.qianlima.com/winbid/detail/20210419_219357928.html.

291 "医疗影像云助力新疆分级诊疗实践 [Medical Imaging Cloud Helps Xinjiang Grading Diagnosis and Treatment Practice]," Intel, http://web.archive.org/web/20220124224543/https://www.intel.cn/content/www/cn/zh/cloud-computing/medical-imaging-cloud-power-grading-clinical-practice-in-xinjiang.html.

292 "Microsoft Research Lab- Asia," Microsoft, https://www.microsoft.com/en-us/research/lab/microsoft-research-asia/.

293 "About Us," Microsoft, https://www.microsoft.com/zh-cn/ard/aboutus/overview.aspx.

294 "李开复创新的微软亚洲研究院被誉为AI黄埔军校 [Kai-Fu Lee's Innovative Microsoft Research Asia is Known as the AI Whampoa Military Academy]," Zhihu, July 27, 2021. https://web.archive.org/web/20220124232654/https://zhuanlan.zhihu.com/p/48695512.

295 "第四届微软亚洲研究院"创新论坛"跨界共创成关键词 [The 4th Microsoft Research Asia 'Innovation Forum Cross-Border Co-Creation Keywords']," *Sina Finance*, June 16, 2021. https://web.archive.org/web/20220124232621/http://k.sina.com.cn/article_1642471052_61e61e8c020013j7k.html.

296 "Microsoft Research Asia Innovation Center," Microsoft Research Asia, https://web.archive.org/web/20220124232820/https://www.msra.cn/zh-cn/about/innovation-partnership.

297 "微软中国云计算创新中心落户上海 [Microsoft China Cloud Computing Innovation Center Settled in Shanghai]," Microsoft, September 16, 2010. https://web.archive.org/web/20211122143647/https:/news.microsoft.com/zh-cn/%E5%BE%AE%E8%BD%AF%E4%B8%AD%E5%9B%BD%E4%BA%91%E8%AE%A1%E7%AE%97%E5%88%9B%E6%96%B0%E4%B8%AD%E5%BF%83%E8%90%BD%E6%88%B7%E4%B8%8A%E6%B5%B7/.

298 Ibid; "微软中国创新中心落'沪' [Microsoft China Innovation Center Falls in Shanghai]," *International Finance News*, September 29, 2010. https://web.archive.org/web/20220124233324/http://m.10jqka.com.cn/63382271.html.

299 "中国首家微软创新中心将落户海南 [China's First Microsoft Innovation Center Will Be Located in Hainan]," DoNews, April 9, 2013. https://web.archive.org/web/20220124233432/https://www.donews.com/net/201304/1716793.shtm.

300 Jiangsu Microsoft Innovation Center Co., Ltd., Company Profile, https://web.archive.org/web/20220124233502/https://www.11467.com/qiye/46783402.htm; Shaanxi Microsoft Innovation Center Co., Ltd, Company Profile, https://web.archive.org/web/20220124233902/https://www.11467.com/qiye/41270806.htm.

301 "Pudong's First Batch of 20 Large Corporate Innovation Centers, 17 of Which Are in Zhangjiang," Min.news, October 27, 2021. https://min.news/en/economy/7fd41c4ba0337e2b1e3ab0192ab88ee3.html?__cf_chl_jschl_tk__=pmd_A9iUtrqtzDX13Mg.VOA13FllTIOqUu0MBWVPsBj81EM-1635290288-0-gqNtZGzNAnujcnBszQiR.

302 "投资总额达660亿元，微软创新中心等项目落户苏州 [With a Total Investment of 66 billion yuan, the Microsoft Innovation Center and Other Projects Settled in Suzhou]," Semiconductor Investment Alliance, August 30, 2019. https://web.archive.org/web/20211122144032/https://baijiahao.baidu.com/s?id=1643288799755251038&wfr=spider&for=pc; "重磅！微软再度签约园区！ [Heavy! Microsoft Once Again Signed a Contract with the Park!]," Leju Network, May 20, 2020. https://web.archive.org/web/20211122144042/https://baijiahao.baidu.com/s?id=1667253060419619426&wfr=spider&for=pc.

303 "镇江携手微软打造数字经济创新中心 [Zhenjiang Joins Hands with Microsoft to Build a Digital Economy Innovation Center]," China Jiangsu Net, November 9, 2020. https://web.archive.org/web/20211122144225/https://baijiahao.baidu.com/s?id=1682715971843577315&wfr=spider&for=pc; "微软镇江数字经济创新中心启动运营 [Microsoft Zhenjiang Digital Economy Innovation Center Starts Operation]," Zhenjiang Municipal People's Government, March 29, 2021. https://web.archive.org/web/20211122144246/https://baijiahao.baidu.com/s?id=1695533896281270387&wfr=spider&for=pc.

304 "工业和信息化部微软嵌入式技术联合实验室 [Microsoft Embedded Technology Joint Laboratory of the Ministry of Industry and Information Technology]," Tianjin University of Science and Technology, January 22, 2016. https://web.archive.org/web/20190316170016/http://kjc.tjut.edu.cn/info/1033/1129.htm.

305 "工信部部长肖亚庆会见美国微软公司总裁布拉德·史密斯 [Minister of Industry and Information Technology Xiao Yaqing Met with Brad Smith, President of Microsoft Corporation]," Shanghai Securities, September 2, 2021. /web/20211122144511/https://baijiahao.baidu.com/s?id=1709757703402693637&wfr=spider&for=pc.

306 "Microsoft in China," Microsoft, January 15, 2015. https://web.archive.org/web/20220124235047/https://news.microsoft.com/zh-cn/features/%E5%BE%AE%E8%BD%AF%E5%9C%A8%E4%B8%AD%E5%9B%BD/ See, for example, Microsoft's strategic cooperation agreements with Guangdong Province (2014) and Leshan City (2016). ("广东省政府与微软公司签署战略合作协议 [Guangdong Provincial Government and Microsoft Signed a Strategic Cooperation Agreement]," People's Daily, October 14, 2014. https://web.archive.org/web/20211122145236/http://world.people.com.cn/n/2014/1014/c157278-25833273.html; "峨眉旅游大数据产业基地成立 助力旅游行业走上云端 [Emei Tourism Big Data Industry Base Was Established to Help the Tourism Industry Go To the Cloud]," People's Daily, December 16, 2016. https://web.archive.org/web/20220123175623/http://travel.people.com.cn/n1/2016/1216/c41570-28956239.html).

307 See, for example, Microsoft's strategic cooperation agreements with Guangdong Province (2014) and Leshan City (2016). ("广东省政府与微软公司签署战略合作协议 [Guangdong Provincial Government and Microsoft Signed a Strategic Cooperation Agreement]," People's Daily, October 14, 2014.

308 "以智能云为基础，国开金融携手微软启动科技创新生态联盟，推进智慧城市发展 [On the Basis of Smart Cloud, CDB Capital Joins Hands with Microsoft to Launch a Technological Innovation Ecological Alliance to Promote the Development of Smart Cities]," Microsoft China, November 2, 2016. https://web.archive.org//web/20211122145307/https://news.mydrivers.com/1/505/505816.htm.

309 See, for example, Robert Muggah and Greg Walton, "'Smart' Cities are Surveilled Cities," *Foreign Policy*, April 17, 2021. https://foreignpolicy.com/2021/04/17/smart-cities-surveillance-privacy-digital-threats-internet-of-things-5g/; Katherine Atha et al., "China's Smart Cities Development," Research Report Prepared on Behalf of the US-China Economic and Security Review Commission, January 2020. https://www.uscc.gov/research/chinas-smart-cities-development.

310 "微软明年拟在中国新增四个数据中心，扩大数字服务能力 [Microsoft Plans to Add Four New Data Centers in China Next Year to Expand Digital Service Capabilities]," Interface News, June 18, 2021. http://web.archive.org/web/20211122145437/https://www.moer.cn/articleDetails.htm?articleId=401876.

311 Microsoft's partnership with 21Vianet dates back to 2012, when the two companies, as well as the Shanghai Municipal Government, signed a strategic partnership agreement in which Microsoft licensed the technology for Office 365 and Windows Azure services, as well as the right to operate and provide those in China, to 21Vianet (Jason Verge, "Microsoft Launches Azure in China Via 21Vianet Group," *DataCenter Knowledge,* May 22, 2013. https://www.datacenterknowledge.com/archives/2013/05/22/microsoft-launches-azure-in-china-via-21vianet-group.

312 "我们的优势 [Our Advantage]," 21Vianet Blue Cloud, https://web.archive.org/web/20211122145637/https://www.21vbluecloud.com/about-us/competitive-advantages/.

313 "关于我们 [About Us]," CMIT, https://web.archive.org/web/20220124232255/https://www.cmgos.com/web/about-us/intro/.

314 Gregg Keizer, "Microsoft Completes Windows 10 Customized for China's Government." *Computer World.* March 21, 2017. https://www.computerworld.com/article/3183664/microsoft-completes-windows-10-customized-for-chinas-government.html.

315 Ibid.

316 Gregg Keizer, "Microsoft Partners with a Chinese State-Owned Defense Conglomerate to Promote, Sell Windows 10 to Government." *Computer World*. December 18, 2015. https://www.computerworld.com/article/3016921/microsoft-partners-with-chinese-state-own.

317 "Addition of Certain Entities; and Modification of Entry on the Entity List," *Federal Register,* August 1, 2018, https://www.federalregister.gov/documents/2018/08/01/2018-16474/addition-of-certain-entities-and-modification-of-entry-on-the-entity-list.

318 OEM厂商 [OEM Partners], CMIT, https://web.archive.org/web/20211219123938/https://www.cmgos.com/web/partner/oem/.

319 渠道合作伙 [Channel Partners], CMIT, https://web.archive.org/web/20211125182026/https://www.cmgos.com/web/partner/channel/.

320 "安全厂商 [Security Vendors]," CMIT, https://web.archive.org/web/20220124231115/https://www.cmgos.com/web/partner/security/.

321 "奇安信与新疆信息产业有限责任公司达成战略合作 [Qi Anxin Reached a Strategic Cooperation with Xinjiang Information Industry Co., Ltd.]," Qi'anxin, July 30, 2021. https://web.archive.org/web/20211122150147/http://www.soxunwang.com/m/view.php?aid=90913.

322 Valentine Weber et al, "China's Surveillance State"T*op10VPN.* Aug 2021. https://www.top10vpn.com/research/huawei-china-surveillance-state/.

323 我市公安云平台建设技术交流会召开 [Our City's Public Security Cloud Platform Construction Technology Exchange Meeting Was Held], January 24, 2014. https://web.archive.com/web/20220123154422/http://jxj.cngy.gov.cn/new/show/741bca493579432b8a951ef4b77ee24d.html.

324 Julia Carrie, "Microsoft Blocks Bing from Showing Image results for Tiananmen 'Tank Man,'" *The Guardian,* June 5, 2021. https://www.theguardian.com/technology/2021/jun/04/microsoft-bing-tiananmen-tank-man-results#:~:text=Microsoft%20has%20blamed%20human%20error,anniversary%20of%20the%20military%20crackdown.

325 Valentine Weber et al, "China's Surveillance State"Top10VPN. Aug 2021. https://www.top10vpn.com/research/huawei-china-surveillance-state/.

326 "Partners," Haiyi Software, Accessed October 4, 2021. https://web.archive.org/web/20211122150407/https://haiyisoft.com/haiyi/kehu/hezuohuoban/.

327 Valentine Weber et al, "China's Surveillance State"Top10VPN. Aug 2021. https://www.top10vpn.com/research/huawei-china-surveillance-state/.

328 "政务公安行业 [Government Affairs and Public Security], Haiyisoft.com, https://web.archive.org/web/20211210071937/https://haiyisoft.com/haiyi/hangye/zhengwu/.

329 "Partners," Zhongke Fuxing, https://web.archive.org/web/20220124225634/http://sinobeststar.com/page/7.html.

330 Valentine Weber et al, "China's Surveillance State"Top10VPN. Aug 2021. https://www.top10vpn.com/research/huawei-china-surveillance-state/.

331 Vicky Xiuzhong et al, "Uyhurs for Sale," *ASPI*. 2019. https://www.aspi.org.au/report/uyghurs-sale.

332 Goertek, LinkedIn, https://www.linkedin.com/company/goertek-electronics.

333 "元宇宙能否让千亿市值的歌尔股份再次起飞？ [Can Metaverse Allow Goertek's shares, Which Have a Market Value of 100 billion Yuan, to Take off Again?]," *Xueqiu*, March 10, 2021. https://web.archive.org/web/20211119164423/https://xueqiu.com/1608947171/200394447; "歌尔股份表示，华为是公司长期合作的战略客户 [Goertek Stated that Huawei Is the Company's Long-Term Strategic Customer]," *Xueqiu*, June 16, 2021. https://web.archive.org/web/20211119164518/https://xueqiu.com/6985073409/183114612; "重磅！总书记主持召开企业家座谈会！海康威视、高德红外、歌尔股份董事长在列 [Heavy! The General Secretary Presided Over a Symposium for Entrepreneurs! The Chairmen of Hikvision, AutoNavi, and Goertek Are Listed]," *EastMoney*, July 21, 2020https://web.archive.org/web/20200725013317/http://finance.eastmoney.com/a/202007211564092860.html; "歌尔股份2021年半年报分析 [Analysis of GoerTek's 2021 Semi-Annual Report]," *Zhihu*, August 27, 2021. https://web.archive.org/web/20220124015437/https://xueqiu.com/1983721775/195662880.

334 "头部企业在青岛系列报道丨歌尔：投资青岛，打造全球研发中心 [Reports from Leading Companies in Qingdao | Goertek: Invest in Qingdao to Build a Global R&D Center]," *Qingdao News Net*, May 20, 2020. https://web.archive.org/web/20211119152801/https://baijiahao.baidu.com/s?id=1667221194266904864&wfr=spider&for=pc.

335 2016年年度报告 [2016 Annual Report], Huawei, https://web.archive.org/web/20220124224950/https://www.huawei.com/-/media/CORPORATE/PDF/annual-report/AnnualReport2016_cn.pdf?la=zh.

336 "DJI and Microsoft Partner to Bring Advanced Drone Technology to the Enterprise," *DJI Enterprise.* 2018. https://web.archive.org/web/20181026014707/https://enterprise.dji.com/news/detail/dji-and-microsoft-partner-to-bring-advanced-drone-tech-to-the-enterprise.

337 "FEITIAN Passwordless Login to Azure AD," AzureMarketplace, https://web.archive.org/web/20220124224751/https://azuremarketplace.microsoft.com/en-us/marketplace/apps/feitiantechnologiesusinc.passwordlessaccesstoazure?tab=overview.

338 Its corporate documents describe support for military civil fusion. (飞天诚信：2020年度非公开发行股票募集资金使用的可行性分析报告 [Feitian Integrity: Feasibility Analysis Report on the Use of Funds Raised by Non-public Issuance of Shares in 2020], May 26, 2020. https://web.archive.com/web/20220124195348/https://q.stock.sohu.com/cn,gg,300386,5776113925.shtml).

339 Valentine Weber et al, "China's Surveillance State," T*op10VPN,* August 2021. https://www.top10vpn.com/research/huawei-china-surveillance-state/.

340 飞天诚信：2020年度非公开发行股票募集资金使用的可行性分析报告 [Feitian Integrity: Feasibility Analysis Report on the Use of Funds Raised by Non-public Issuance of Shares in 2020], May 26, 2020. https://web.archive.com/web/20220124195348/https://q.stock.sohu.com/cn,gg,300386,5776113925.shtml; "飞天诚信：公司持有宏思电子91.49%的股份 [Feitian Integrity: The Company Holds 91.49% of Hongsi Electronics], Sohu, August 9, 2021. https://web.archive.org/web/20220124194347/https://www.sohu.com/a/482306673_115362; "北京宏思电子技术有限责任公司 [Beiing Hongsi Electronic Technology Company]," 51semicon.com, https://web.archive.org/web/20220124194724/http://www.51semicon.com/com/hongsi-ic/introduce/.

341 "飞天诚信科技股份有限公司: 2021 年半年度报告 [Feitian Integrity Technology Co., Ltd.: 2021 Semi-Annual Report]," July 2021. https://web.archive.org/web/20220125173549/https://pdf.dfcfw.com/pdf/H2_AN202107261506233822_1.pdf?1627322583000.pdf.

VICTIMS OF COMMUNISM
MEMORIAL FOUNDATION

900 15th Street NW
Washington, D.C. 20005
202.629.9500
victimsofcommunism.org

TRUTH. JUSTICE. MEMORY.