

THE EPOCH TIMES

TRUTH AND TRADITION

EXCLUSIVE
REPORT



Huawei plays a key role in China's programs of mass surveillance, human rights abuse, and technological dominance.

*Jasper Fakkert,
Editor-in-Chief*

IS CHINA'S **HUAWEI** WATCHING YOU?

A global media in 23 languages and 35 countries. A world leader in reporting on China.

Table of Contents

- Huawei Is Cornerstone of CCP Initiative to Overtake the United States.....**3**
- The Relationship Between Huawei and the Chinese Regime's Factional Politics.....**5**
- Meng Wanzhou, Chief Financial Officer and Vice Chair of Huawei.....**6**
- A Brief History of Huawei.....**7**
- Chinese User Agreements Force You to Abide by Chinese Censorship.....**9**
- Controlling Data: The CCP's National Security Law.....**10**
- Huawei's Role in Underhanded Deals and Influence Operations.....**11**
- Pentagon Technology Found Its Way to the Chinese Military.....**12**
- Exporting Tyranny: Telecom Role in the CCP's One Belt, One Road.....**14**
- 'F7': Huawei's Alleged Codename.....**14**
- Tools Huawei Developed to Persecute Falun Gong Now Repress All of China.....**19**
- US Technology Used for Mass Surveillance in China, Say US Lawmakers.....**20**
- Suicide of Chinese Scientist Sparks Controversy.....**22**

FRONT PAGE ILLUSTRATION: SHUTTERSTOCK & THE EPOCH TIMES

About Us

The Epoch Times is a media organization dedicated to seeking the truth through insightful and independent journalism.

Standing outside of political interests and the pursuit of profit, our starting point and our goal is to create a media for the public benefit, to be truly responsible to society.

We endeavor to educate readers about today's most important topics, seeking to

broaden and uplift minds. We believe that rational, balanced debate is key for fostering a healthy democracy and a compassionate society.

As an independent media outlet, we use our freedom to investigate issues overlooked—or avoided—by other media outlets. We seek to highlight solutions and what's good in society rather than what divides us.

We report respectfully, compassionately, and rigorously.

We stand against the destruction wrought

by communism, including the harm done to cultures around the world.

We are inspired in this by our own experience. The Epoch Times was founded in 2000 to bring honest and uncensored news to people oppressed by the lies and violence in communist China.

We still believe journalism is a noble vocation, but only when it genuinely seeks to serve its communities and help them to flourish. In all that we do, we will hold ourselves to the highest standards of integrity. This is our promise to you.

From the Editor

Chinese telecom company

Huawei has a controversial brand, yet details that explain this controversy are rarely made clear in news stories. With the recent arrest of Meng Wanzhou, chief financial officer and vice chairperson of Huawei, The Epoch Times is publishing this special edition to shed light on the company's opaque operations.

Some may wonder who Meng is and why her arrest is significant. In this edition, we explain her link to Huawei President Ren Zhengfei as well as why it matters that she has multiple passports. We also offer insight into how the company operates within the Chinese system, and how that affects the nature of her role.

Among the least-known aspects of Huawei's operations are its leadership and finances. Here, we provide information about the Chinese Communist Party's role in the company's leadership, along with details about its financing, origins, and direction from the Chinese regime.

Another major controversy surrounding Huawei that is often mentioned, yet

often poorly substantiated, is the ongoing concern that the company may pose a security threat to foreign nations by sharing data with Chinese authorities. Included in this special edition is information that should end this confusion, as we explain how Chinese laws require companies, including Huawei, to grant control over data to the state and allow authorities access to their systems. We also detail terms-of-service agreements for products from Chinese companies that have users abroad often unknowingly agreeing to abide by Chinese law.

Huawei also plays a key role in the Chinese Communist Party's programs of mass surveillance, human rights abuse, and technological dominance. This is fundamental to understanding the nature of the company's guidance and operations—all of which we explain in this special edition.



Jasper Fakkert
Editor-in-Chief

THE EPOCH TIMES

Lillian Fan, Publisher
Jasper Fakkert, Editor-in Chief

CONTACT US

Australian Epoch Times Ltd.
49A Treacy St,
Hurstville NSW 2220
02 8988 5600

Advertising
ad@epochtimes.com.au

Subscriptions
subscribe@epochtimes.com

General Inquiries
enquiry@epochtimes.com

Letters to the Editor
lettertoeditor@epochtimes.com



SUBSCRIBE TODAY

Get the
independent news
you won't find
anywhere else.

Subscribe and get the
insights only The Epoch Times
can provide, delivered everyday
to your inbox.

subscribe.epochtimes.com

GLOBAL DOMINANCE

Huawei Is the Cornerstone of a CCP Initiative to Overtake the US

JOSHUA PHILIPP

The Chinese Communist Party (CCP) is pushing a goal, under the banner of sovereignty, of eliminating reliance on foreign systems within China and then ensuring Chinese-made systems dominate the global landscape.

In the push to dominate this domain, the CCP has identified core technologies, including satellite GPS, internet infrastructure, and superconductors, with Huawei playing a key role in this agenda.

The Jamestown Foundation's China Brief noted June 5 that Chinese leader Xi Jinping recently has been promoting this concept as an approach to "technology, the internet, and governance, one that seeks to embed [China's] concept of 'cyber sovereignty' ... in the institutions of global internet governance."

In the past, the CCP's concept of cybersovereignty often referred to its push to dominate the global internet space, an effort dating to at least 2010, which included a play to gain control of the internet globally through the United Nations in 2015.

As the program has advanced, however, it has broadened to include the foundational technologies that make the internet and global technology systems work, while maintaining the CCP's spirit of social tyranny and global market domination.

Through the CCP's "One Belt One Road" initiative, it's constructing core infrastructure that includes an export of the "China Model" for totalitarian governance.

The Council on Foreign Relations reported in July that "China's exporting of surveillance goods is a critical component of its 'Digital Silk Road.'"

It noted that Huawei recently implemented its "Safe Cities" model in Nairobi, Kenya, where it installed 1,800 surveillance cameras as part of the program, and indicated that "although the cameras can help fight

Huawei plays a key role in China's goal to surpass the United States as the world leader in technology, under its Project 863 and "Made in China" 2025 programs.

(Top) A Huawei display at the Beijing International Consumer Electronics Expo in Beijing on July 9, 2018.



crime, they can also be used to monitor activists and protests."

In addition to Nairobi, the report stated, "Huawei has deployed its systems across 100 cities in approximately 30 countries worldwide. Exports of such technology are being coupled with Chinese government-backed grants that create dependency of the importing country on Chinese-produced gear and incentivize further purchases of such equipment."

A core aspect of this push is a new CCP-led internet framework that is separate from, yet interconnected with, the global internet. Included in this technology is the CCP's massive systems for internet censorship and online monitoring—and again, coupled with it is Huawei's internet infrastructure and systems for totalitarian social control.

Huawei plays a major role in the CCP's programs for human rights abuse and domestic surveillance. A 172-page internal document from Huawei in 2015, which was leaked to the internet, was a training manual for Chinese internet police to monitor, analyze, and process video content. It also showed Huawei's involvement with the CCP's Golden Shield Project for censorship and Skynet System for surveillance.

The company's technology is also part of the CCP's Social Credit System, which creates a database on each person, tracks all available data about the individual, and calculates a "citizen score" that determines their level of freedom in society.

The CCP is also making substantial efforts to replace the U.S. superconductor industry—technologies for which Huawei and Chinese telecom company ZTE still depend on Western companies, in developing and supplying them.

The United States indicted China's state-owned Fujian Jinhua Integrated Circuit on Nov. 1 for allegedly stealing trade secrets from U.S.-based superconductor developer Micron. The indictment also included United Microelectronics Corp., a Taiwanese

company, and three Taiwanese nationals—including Stephen Chen, a former president of Micron Memory Taiwan, a Micron subsidiary in Taiwan, who went on to work at the CCP's United Microelectronics Corp.

Weeks later, in late November, CCP officials claimed they had found evidence that Micron was price-fixing, along with Samsung and Hynix, and—without providing public evidence—claimed the companies were involved in anti-competitive behavior.

That came on the heels of temporary U.S. sanctions that banned ZTE from the U.S. superconductor market, after ZTE was found to have violated U.S. sanctions on Iran. Though the ban was quickly lifted, it acted as a warning shot about the effect that U.S. sanctions could have on the Chinese tech industry.

With Huawei now facing a similar fraud case related to Iran, the stakes have grown, and the CCP's programs to replace and surpass the United States as the global technology leader are front and center again, with initiatives to compete in 5G internet technology, new energy, quantum computing, and others.

In China, there's a concept of "surpassing you at the curve," and that's become a guiding concept for the CCP's aim to overtake the United States as the world leader in technology, under its Project 863 and China 2025 programs. The idea is that it's very difficult to surpass someone already ahead in a certain area, but when the whole world is making a turn, that person can be surpassed.

Under the CCP, that means a focus on new and emerging technologies is paramount. The Party has been using foreign investment, research partnerships, state financing, and theft of trade secrets to give its companies an edge over their often privately owned foreign competitors when market shifts take place.

Huawei is among the key companies being used to achieve this goal.

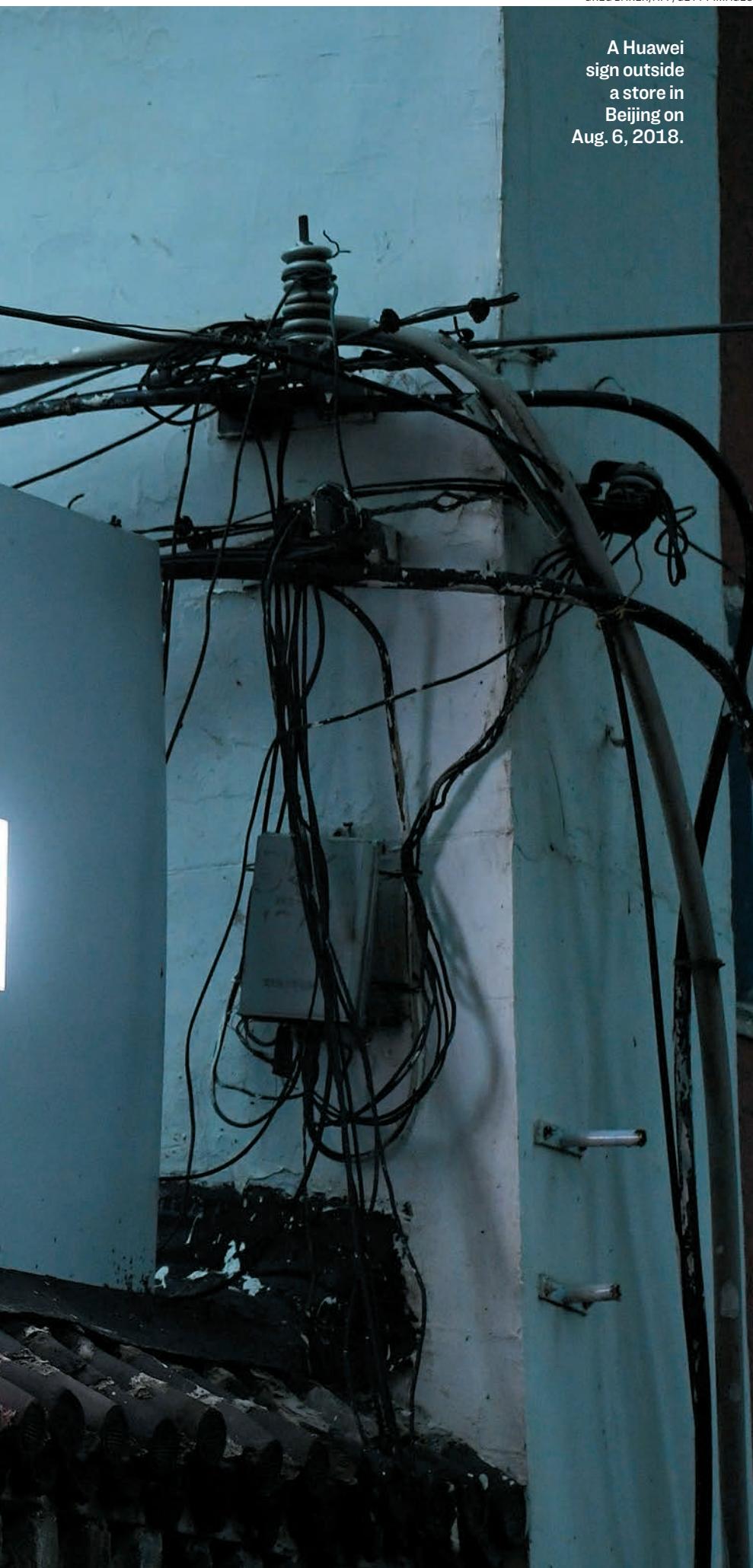
GREG BAKER/AFP/GETTY IMAGES



With its close connections to the Chinese regime under Jiang Zemin, Huawei has played an extensive role in building and upgrading China's internet censorship and surveillance apparatus.

GREG BAKER/AFP/GETTY IMAGES

A Huawei sign outside a store in Beijing on Aug. 6, 2018.



HUAWEI LEADERSHIP

HUAWEI

and the Chinese Regime's Factional Politics

NICOLE HAO

The arrest of Huawei Chief Financial Officer Meng Wanzhou by Canadian authorities has thrust the world's largest telecommunications company into the international spotlight.

While officially considered a private enterprise, Huawei isn't listed on any stock exchange, and governments around the world consider the company an important tool for China's communist authorities. U.S. prosecutors have accused Huawei of using a Hong Kong company to skirt sanctions imposed on Iran, mirroring earlier charges against ZTE, another prominent Chinese tech company that sold U.S.-made equipment to Iran and North Korea.

Taken at face value, Huawei is an employee-owned private company. Founder Ren Zhengfei officially holds 1.4 percent of Huawei's shares, while the rest are distributed to 80,000 employees via the company's trade-union committee.

However, the committee has no other role, and Huawei workers automatically lose their shares when they leave the company. Real power is held by company managers and their Chinese Communist Party (CCP) connections.

A look at the company's top personnel reveals that Huawei has close informal relationships with Chinese security forces, the military, and the CCP political faction associated with former Party leader Jiang Zemin.

Ren has a background in the Chinese People's Liberation Army (PLA), with his first wife, Meng Jun, being the daughter of a prominent PLA political officer. Their first daughter is Meng Wanzhou, the recently arrested CFO and vice-chairwoman of Huawei.

Ren, whose own family was persecut-

ed in the Cultural Revolution during the 1960s and 1970s, married into his wife's family. As a result, Meng Wanzhou took her mother's surname.

Meng Jun's father, Meng Dongbo, rose from his position in the PLA to become CCP secretary of a city in Sichuan Province, and eventually became the province's deputy governor. He also served as a representative in both the Sichuan provincial People's Congress and the National People's Congress during the 1980s.

Ren, who enjoyed a good relationship with his father-in-law, was supported by his political connections.

Huawei Chairwoman Sun Yafang, who has been in the position since 1999, is another prominent figure in the company and considered one of the most powerful women in the world. According to CIA reports, she has a background in the Ministry of State Security (MSS), China's intelligence agency.

Huawei, Spies, and Factional Struggle

Sun's influence within Huawei overshadowed Ren's. In 2010, Sun pressured Ren into giving up plans to promote his son, Ren Ping, as heir of Huawei. This suggests that Huawei is largely controlled by Chinese regime intelligence.

Additionally, prior to the corruption purges launched by current Chinese leader Xi Jinping, the MSS was firmly in the hands of the Jiang faction.

The heads of the MSS between 1985 and 2016 were Jia Chunwang, who served until 1998, then Xu Yongyue, who was on the job after Jia until 2007, when he was replaced by Geng Huichang.

Jia has strong relations with former Communist Party leader Jiang and his allies. Jia's son-in-law is Liu Lefei, the chairman of CITIC Private Equity Funds Management Co. Ltd. and the son of Liu Yunshan, a retired high-ranking →

MATTHEW LLOYD/AFP/GETTY IMAGES



(Above) Huawei President Ren Zhengfei (R) shows Chinese leader Xi Jinping around the tech firm's offices in London on Oct. 21, 2015.

(Top right) A logo of Huawei next to a Chinese flag in Shanghai on Oct. 1, 2014.

CCP official linked to Jiang. Before his retirement at the beginning of this year, Liu Yunshan was one of seven members of the Politburo Standing Committee that leads the Communist Party.

Xu is the son of Party officials and also associated with the Jiang faction, having served as minister of state security at the time when Jiang's political influence was at its peak.

Geng worked closely with Zhou Yongkang, another former member of the Politburo Standing Committee. Zhou, now imprisoned on charges of corruption and plotting to undermine Xi's leadership, is a central figure in the Jiang network. He was purged in 2014; the next year, he received a death sentence that was commuted to life in prison.

Geng was placed under investigation in 2016. That November, he was replaced by Chen Yongqing, a former vice chairman of the Fujian Province CCP committee. Chen is considered an ally of Xi Jinping.

Huawei's Role in the CCP's Censorship Infrastructure

Jiang Zemin was general secretary of the CCP from 1989 to 2003. After Jiang's retirement, his associates, many of whom had been promoted to high positions in the CCP and the Chinese government, carried out his influence throughout the two terms of Chinese leader Hu Jintao.

Individuals in this sprawling web of patronage are still being rooted out in a continuous anti-corruption campaign, years after Xi Jinping came to power in 2013.

Wang Youqun, who served as a CCP disciplinary official between 1993 and 2002, told The Epoch Times that according to a former Huawei employee familiar to him, Huawei was a company used for intelligence, and that it served "the previous dynasty," that is, the leadership of Jiang.

Aside from nepotism and corruption, Jiang is notorious for starting new abuses

A look at the company's top personnel reveals that Huawei has close relationships with Chinese security forces, the military, and the CCP political faction associated with former Party leader Jiang Zemin.

LINTAO ZHANG/GETTY IMAGES



Jiang Zemin.



of human rights under the CCP, most notably the nationwide campaign against the spiritual practice Falun Gong in 1999.

In order to better monitor and censor online expression, the Jiang leadership launched the vast system of internet controls popularly known as the Great Firewall of China.

With its close connections to the Chinese regime under Jiang, Huawei has played an extensive role in building and upgrading the Great Firewall.

An important component in the early stages of the firewall was the Golden Shield Project, which established surveillance over internet users throughout the country.

The Great Firewall and the Golden Shield Project were created under the oversight of Jiang's eldest son, Jiang Mianheng, who has close ties to Huawei, according to previous reports.

In 2003, the state-run Central Central Television reported that the first phase of Golden Shield Project, begun in 2001, had cost 6.4 billion yuan (about \$770 million at the time) by the end of 2002. Further expenditures on the project have not been published.

Given the scale, costs, and importance associated with the Great Firewall, it's unlikely that Jiang would have trusted Huawei to do critical work on the project were he not satisfied with its political background.

Tang Jingyuan, a U.S.-based commentator on Chinese current affairs, told The Epoch Times on Dec. 10 that Huawei chairwoman Sun was likely appointed to her position at the behest of the Jiang faction, which made the company politically reliable.

"They [figures in the Jiang faction] have treated Huawei as their own business since then," Tang said. "It's easy to understand why Jiang Mianheng gave its orders to Huawei."

MENG WANZHOU

Chief financial officer and vice chair of Huawei

Recent Arrest

Meng was arrested by the Canadian government on Dec. 1 in Vancouver, while she was traveling from Hong Kong to Mexico via Canada, on suspicion of violating U.S. sanctions against Iran. The United States accused Huawei of using its subsidiary, the Hong Kong-based Skycom Tech Co., to do business with Iranian telecommunications companies between 2009 and 2014. Meng was allegedly involved in these deals.

Details on Meng's Passports

Meng has held at least seven passports over the past 11 years, according to U.S. authorities. Hong Kong's Ming Pao newspaper reported Dec. 8 that Meng had an eighth passport that she used in Hong Kong in 2004 for a Huawei anniversary event. In court, Meng's lawyer David Martin said that Meng has two valid passports, one of which, issued by the Hong Kong authorities, was used by Meng to travel in Canada. Another passport, issued by China, was delivered to Canada following Meng's arrest. For Meng, the first letter of each of her four Chinese passport numbers was G, and the first letter of the three Hong Kong numbers was K. She allegedly used another Chinese passport, with a number starting with P, to register for an event.

The Significance of Multiple Passports

In mainland China, there are four types of passports, with numbers beginning with letters G or E, P, S, and D. Pass-

A Brief History of Huawei

The History of Huawei's Ties to the Chinese Communist Party

During the 1980s, China had severe import and export restrictions—especially after the 1989 Tiananmen Square massacre precipitated sanctions. Countries also had strict regulations over

what technology could be exported into China.

Despite that, Ren Zhengfei, a former military officer, founded Huawei in 1987 with a meager 21,000 yuan (about \$5,000 at the time) and was able to import sensitive equipment. Sanctions forbade Huawei from importing complete sets of equipment.

The company turned to importing key components, then manufacturing complementary parts and assembling them in China.

Huawei was China's sole communications equipment supplier. It received contracts to set up communications networks for local governments in China's

central and western regions.

Huawei grew its domestic market rapidly in the 1990s.

Huawei began expanding into international markets, after China joined the World Trade Organization in 2001 and many countries opened their markets.

Evidence of State Funding

Sina, a Chinese news portal, reported in January 2005 that the state-owned China Development Bank (CDB) loaned Huawei \$10 billion in December 2004. Huawei was the only private firm that could receive loans from CDB at the time.

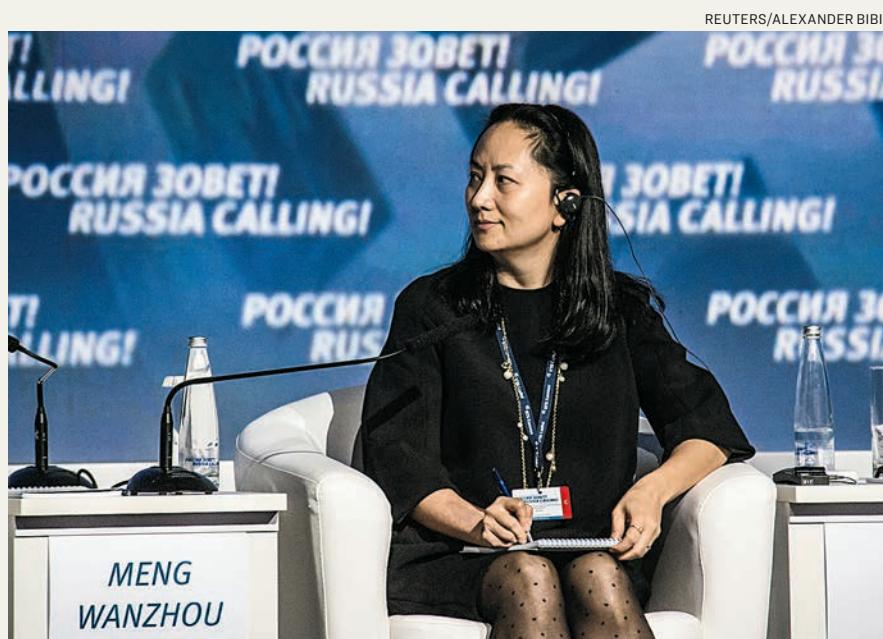
In September 2009, state-run media Xinhua reported that CDB signed a new round of the strategic cooperation agreement with Huawei, loaning it \$30 billion.

ports labelled with "S" are service passports. "D" indicates diplomatic status. "G" and "E" passports are for the general public, with "E" denoting the upgraded biometric passport that has been in use since May 2012. The P passport, which Meng reportedly possesses, is for public affairs. It is granted to government clerks and employees of state-owned enterprises. P passports are within the family of S service passports.

Before reforms made in 2007, all China-issued passports were valid for five years. In 2007, the validity period of S, D, and P passports was shortened to four years, while G and E passports had their expiry dates extended to 10 years from date of issue.

The fact that Meng has had four Chinese passports issued to her in the past 11 years, despite the validity period being four years, has raised questions. Also intriguing is the fact that she possesses Hong Kong passports, while by law Chinese are not allowed to hold dual citizenship and must revoke their Chinese passport if they gain a Hong Kong passport. Hong Kong and neighboring Macau are former British and Portuguese colonies administered as part of China but allowed some functions of self-rule, including separate citizenship.

Given how things are normally done in China, Meng would have had to give up either her Chinese or Hong Kong passport when applying for travel documents that would allow her to go between the mainland, Hong Kong, and Macau. This has raised questions about which document Meng used to



Meng Wanzhou, CFO of Chinese technology giant Huawei, at a VTB Capital Investment Forum in Moscow on Oct. 2, 2014.

travel between China and Hong Kong. Besides her Chinese and Hong Kong citizenships, Meng once received permanent residency in Canada, which expired in 2009.

Meng Family Connections

Meng, 46, is the oldest child of Huawei founder Ren Zhengfei and was widely believed to be next in line to assume leadership over the military-linked company. She dropped out of high school and took up a job at a bank in China's southern metropolis of Shenzhen. She joined Huawei in 1993 and was named CFO in 2011. But her ties to Ren were not publicly revealed until 2013—which drew speculation that she would succeed her father to take the helm of the company.

Notably, Meng and Ren do not share the same last name. That is due to the prominent social status of Meng's mother and Ren's ex-wife, Meng Jun.

Chinese culture traditionally follows a patrilineal family system, whereby women marry into their husbands' families. Some men, however, will marry into their wives' families due to the higher economic or social status of the latter.

Meng Jun's father was Meng Dongbo, deputy secretary of a political committee with the East China Field Army—a CCP army unit during China's civil war. Meng Dongbo later enjoyed a long political career in Sichuan Province. Ren, on the other hand, came from a poor area of Guizhou Province, and his

family was persecuted during the Cultural Revolution.

Because of the political prominence of the Meng family, Ren moved in to live with the Meng family following his marriage. As a result, their first child, Meng Wanzhou, born in 1972, took on her mother's last name.

Court Details

Meng, 46, faces a maximum sentence of 30 years for each charge in the United States. Meng was initially granted a publication ban by the British Columbia Supreme Court, which would have restricted the media's ability to report on what happens in court. The ban was lifted on the morning of Dec. 7, just before the court hearing.

Stateside, the U.S. District Attorney's Office in the Southern District of New York confirmed that Meng's case is being handled by their colleagues in the Eastern District office. John Marzulli, spokesperson for the Eastern District office, declined to comment on the case.

Broader Implications

Many have speculated about whether the arrest would have implications for the ongoing trade dispute between China and the United States. In fact, both the U.S. administration and Chinese authorities have made statements saying that they were committed to negotiations and sorting out a deal within the 90-day period agreed upon between U.S. President Donald Trump and Chinese leader Xi Jinping on the sidelines of the G-20 meeting in Buenos Aires.

Annie Wu contributed to this report.

ED JONES/AFP/GTETT IMAGES



Xiaomi's user agreement says that you must follow the Chinese regime's rules on the suppression of religion, and that you can no longer undermine its 'national religious policy.'

A man checks surveillance cameras on Tiananmen Square in Beijing on Oct. 31, 2013.

SURVEILLANCE STATE

Chinese User Agreements Force You to Abide by Chinese Censorship

JOSHUA PHILIPP

If you're looking to pick up a phone or laptop made by a Chinese company, be sure to read the fine print in the terms of service. You may be putting yourself at the mercy of Chinese law.

The policies may give a glimpse of what's to come, as the Chinese regime has passed new laws requiring it to enforce its brand of "national security" abroad.

If you're using a Xiaomi smartphone, for example, it's likely you've unwittingly agreed "to bear all the risks and take full legal liability" to not engage in activities the Chinese regime has banned.

According to the fine print, you've actually limited yourself quite a bit.

First and foremost, it bans you from opposing the principles of the Constitution of the People's Republic of China. You're also not allowed to leak state secrets or subvert the government.

If you believe in a free Tibet, an independent Taiwan, or a democratic Hong Kong, you're violating Xiaomi's user agreement, since it forbids you from "undermining national unity."

Also be careful if you're spiritual or believe in a religion.

The agreement says you have to follow the Chinese regime's rules on the suppression of religion, and you can no longer undermine its "national religious policy."

If you write about Tibetan Buddhism or House Christians, you may violate its rules on what the Chinese regime calls "cults." You also can't write about any beliefs it calls "superstitions."

When it comes to

Any company that wants to do business in China must uphold these rules.

(Below) People take photos in Tiananmen Square in Beijing on Oct. 24, 2017. Many major Chinese products have terms-of-service agreements that make users abide by Chinese laws on censorship and religious discrimination.



GREG BAKER/AFP/GETTY IMAGES

news and politics, the agreement forbids you from "spreading rumors." When discussing news, that usually means you're not allowed to say things that don't align with the state-approved lines of the Chinese regime's official mouthpiece news outlets.

You've also given Xiaomi the "right to access" your account.

Xiaomi isn't alone in these requirements, either. Chinese tech firms including Huawei and Decathlon have similar user agreements.

There are a few differences in each. With Decathlon, for example, you're not allowed to spread anything that could "damage the reputation of government organizations."

The text in the agreements has actually been there for some time. According to archives of the Xiaomi website, the parts banning discussion on "cults" and "superstition" and the requirements to abide by the Chinese regime's constitution were added in October 2014.

What's concerning, however, is what these existing standards mean for new binding laws on foreign technology companies that do business in China, and new

laws for exporting Chinese "national security" abroad.

German satirist Christoph Rehage was among the first foreign targets of these policies. In December 2015, he uploaded a YouTube video that called the founder of the Chinese Communist Party (CCP), Mao Zedong, "China's Hitler." A Communist Youth League website called for Rehage to be punished for violating Chinese law, even though he lives in Hamburg. They argued that Rehage, who speaks Chinese, made the video to circulate in China, which they said undermined the sovereignty of the country's internet.

Earlier in 2015, a Hong Kong-based editor who wrote gossip books about Chinese leaders disappeared along with four of his colleagues.

This could tie to a shift in Chinese policy that began on July 1, 2015, when the National People's Congress Standing Committee passed the National Security Law.

The law emphasizes that "China must defend its national security interests everywhere," and, according to *The Diplomat*, "[affects] almost every domain of public life in China—the law's mandate covers politics, the military, finance, religion, cyberspace, and even ideology and religion."

Alongside the National Security Law was another passed on Dec. 27, 2015, called the Counterterrorism Law.

The Counterterrorism Law was particularly contentious since it requires foreign tech firms to cooperate with the Chinese regime's investigations—and its brand of "counterterrorism" is far different from that in the West.

As *The Diplomat* noted, the CCP has its own definition of terrorism, which includes "any thought, speech, or activity that, by means of violence, sabotage, or threat, aims to generate social panic, influence national policy-making, create ethnic hatred, subvert state power, or split the state."

In other words, at one extreme it does include terrorism—but at the other extreme it also makes "thought" and "speech" illegal, if those thoughts or words challenge the CCP's rule.

Any company that wants to do business in China will need to uphold these rules. The Chinese regime's policy is still being developed, but if the user agreements of Chinese companies tell us anything, it's possible we may all soon be required to follow its standards on totalitarian rule or, as Xiaomi's warning states, "bear all the risks and take full legal liability."

Eyal Levinter contributed to this report.

NEWS ANALYSIS

Controlling Data: The CCP's National Security Law

JOSHUA PHILIPP

Under the Chinese regime, all network infrastructure and information systems are required by law to be “secure and controllable.” This requirement on data monitoring is enforced under the National Security Law, which was passed in 2015 by the National People’s Congress, China’s faux legislature.

Among the key concerns around Huawei and similar Chinese technology companies is whether they share data with Chinese authorities or the Chinese military; under the National Security Law, this argument is moot. All companies operating in China are required to abide by the law, and the Chinese regime has created a law that requires companies to grant it control of data.

The U.S.–China Economic and Security Review Commission noted the implications of the National Security Law in a 2015 report. It states that the new rule “would require any company operating in China to turn over to the government its computer code and encryption keys, as well as to provide a backdoor entry into its commercial computer networks.”

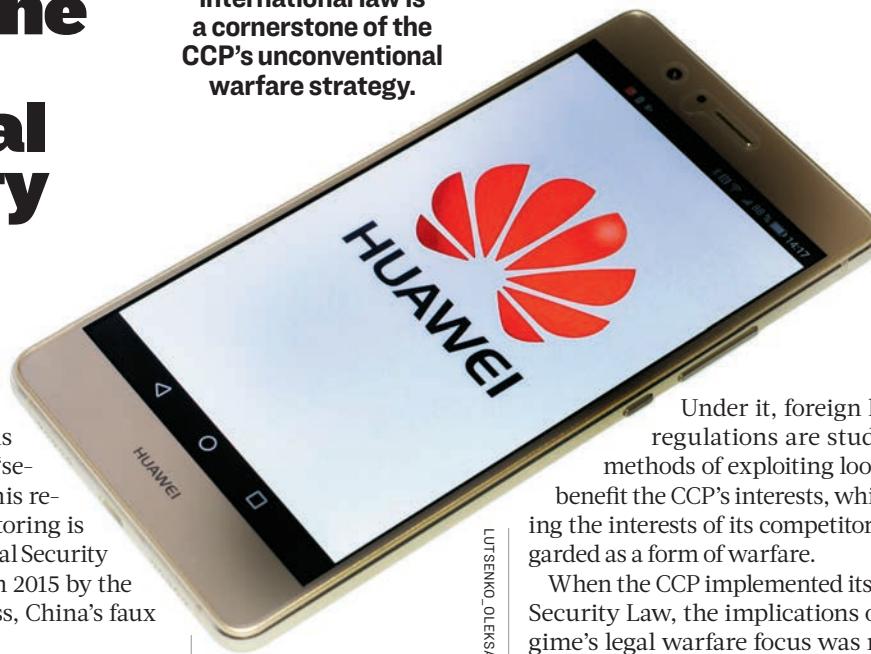
The United States has been paying close attention to Chinese technology companies. Also part of the National Security Law is a less discussed component that allows the CCP to selectively ban foreign imports while favoring its own companies. This works by manipulating a loophole in World Trade Organization regulations on protectionism, and was viewed at its onset as something that could allow the CCP to boot U.S. companies from China.

Under WTO rules on free trade, countries aren’t allowed to discriminate against imports. There’s an exception to this, however; countries can ban certain imports if they are deemed a national-security threat.

Manipulation of international law is a cornerstone of the CCP’s unconventional warfare strategy, as described under its Three Warfares concept of psychological warfare, media warfare, and legal warfare.



Manipulation of international law is a cornerstone of the CCP’s unconventional warfare strategy.



“The goal is to completely replace foreign information technology with Chinese information technology.”

Robert Atkinson,
president, Information
Technology and
Innovation Foundation

Under it, foreign laws and regulations are studied, and methods of exploiting loopholes to benefit the CCP’s interests, while harming the interests of its competitors, are regarded as a form of warfare.

When the CCP implemented its National Security Law, the implications of the regime’s legal warfare focus was raised by Robert Atkinson, president of the Information Technology and Innovation Foundation, a Washington-based think tank. He explained in an interview at the time that “the goal is to completely replace foreign information technology with Chinese information technology.”

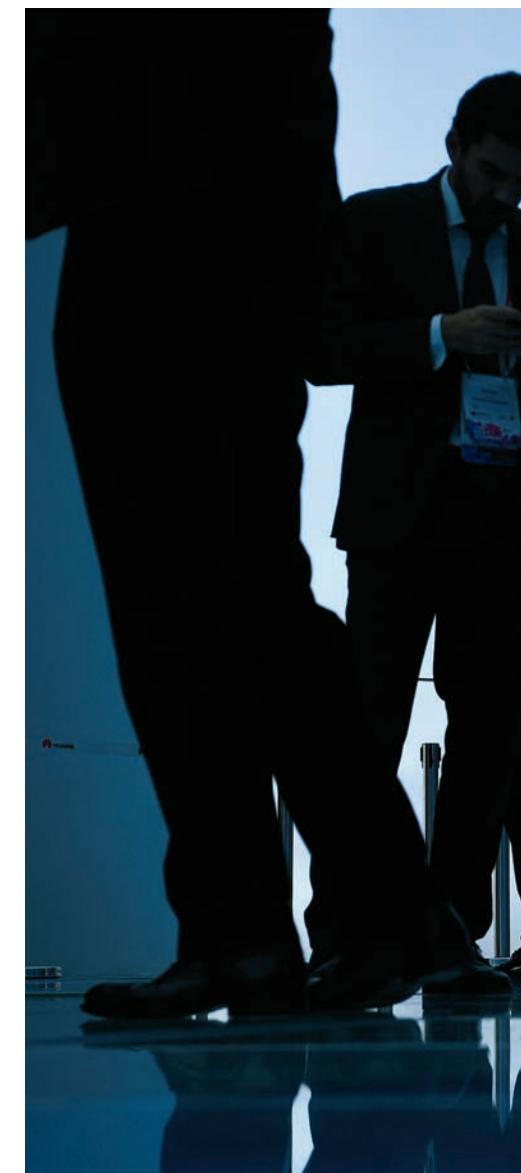
“The Chinese government has spent an enormous amount of time understanding the actual rules and laws of the WTO, so anything they do doesn’t run afoul of the WTO,” Atkinson said.

“The Chinese essentially want a closed loop where Chinese companies are making these things for China,” Atkinson said, “and the security provisions in the National Security Law are one of many, many tools the Chinese government is implementing to achieve this goal.”

As he noted, the National Security Law expanded on an earlier program of the CCP, the National Medium- to Long-Term Plan for the Development of Science and Technology, which was passed in 2006. The program requires that for companies to sell in China, they must first transfer their technology to Chinese companies.

In addition, under new “internet safety” rules announced by China’s police force in October, any official within China’s security apparatus can now enter a company’s premises, computer mainframe rooms, and any other workspace, for the purpose of carrying out an inspection.

Upon entering, security officials can demand that supervisors or internet administrators submit to questioning. The officials also can look up and make copies of any information relevant to the inspection. Security officials are now empowered to dispense administrative punishment or penal action for any behavior or action by companies that they deem to be illegal.



Visitors use their cellphones at the Huawei stand at the Mobile World Congress in Barcelona, Spain, on Feb. 28, 2017.

Researchers found that Huawei paid for 12 Australian federal politicians to travel to Huawei’s headquarters in Shenzhen between 2010 and 2018.



CORRUPTION

Huawei's Role in Underhanded Deals and Influence Operations

JOSHUA PHILIPP

Subversion operations of the Chinese Communist Party (CCP) include bribery, political influence, extortion, and programs for subtle influence. These operations are often carried out by Chinese agents, but Huawei has been accused on several occasions of engaging in similar actions.

Cases concerning Huawei's alleged influence operations made headlines in Australia, where the telecom company has allegedly been sponsoring politicians to travel to China, running influence operations, and receiving taxpayer funds to participate in military research programs.

Huawei is the largest corporate sponsor of overseas travel for Australian politicians, according to a Reuters report in June. It cited a report on travel disclosure registers from the Australian Strategic Policy Institute, a think tank.

The researchers found that Huawei paid for 12 Australian federal politicians to travel to Huawei's headquarters in Shenzhen between 2010 and 2018. Expenses included business-class flights, local travel, accommodations, and meals. Politicians included Australia's Foreign Minister Julie Bishop, Trade Minister Steve Ciobo, and former Trade Minister Andrew Robb.

The trips were just part of local concerns in Australia, however, and on June 28, its senate passed two laws that overhaul its previous laws on security and foreign interference. According to The Guardian, these included a new criminal offence for theft of trade secrets for a foreign govern-

ment, and a register for individuals acting on behalf of foreign principals.

Long-Standing Concerns

The reports of Australian politicians traveling on Huawei's dime followed on concerns that had long been brewing. News about CCP front operations in Australia had begun making headlines in 2017, when local media reports exposed the CCP's influence over the country's news outlets, universities, businesses, and politicians.

The Weekend Australian reported on June 10 that Australian tax dollars are helping fund the CCP's weapons programs, through cooperation between Australian universities and Chinese military-linked, state-owned enterprises.

"The Australian Research Council is funneling Australian taxpayer funds into research with applications to China's advanced weapons capacity through its linkage program," it states.

The Australian Research Council also gave \$466,000 to a joint-research program between the University of New South Wales, the Australian subsidiary of multinational company National Instruments, and Chinese telecom company Huawei.

The report notes that "Australia's intelligence agencies believe Huawei is linked to the Third Department of the PLA, the military's cyberespionage arm, which led [the Australian] government to place a ban on the use of Huawei equipment in Australia's National Broadband Network."

Corruption

In December 2017, a top executive of Huawei, Teng Hongfei, vice president of the Huawei Consumer Business Group in the Greater China region, was investigated for bribery. In his early career, Teng worked at Nokia as a regional CEO. In 2012, he moved to Samsung, before settling at Huawei in 2014.

A similar case had taken place in 2014. The Chinese business publication Caixin reported that 116 employees had accepted or solicited bribes, mainly by demanding kickbacks from 69 retailers. One regional director received bribes of up to 2 million yuan (around \$320,000 at the time). Huawei denied the allegations.

An insider cited in Telworld, a Chinese publication covering the domestic tech industry, said different departments at Huawei have allowed corruption to fester, including in the research and development, procurement, and sales departments.

In 2012, a group of Chinese tech executives, including one from Huawei, were convicted of bribery in an Algerian court. International arrest warrants were issued after the court found that they had bribed an executive at the state-owned Algérie Télécom to give their companies an edge.

MILITARY USE

Pentagon Technology Found Its Way to the Chinese Military

Sumitomo Electric Lightwave's fiber-optic technology now helps power the Chinese regime's weaponry

JOSHUA PHILIPP

The Chinese regime's fifth-generation fighters, state-of-the-art naval cruisers, and soon-to-be-launched aircraft carriers are more deadly than they otherwise would be because they are equipped with advanced fiber-optic cable originally built for the Pentagon, according to a U.S. military intelligence officer.

The saga of this cable is part of a bigger story of how American military technology ends up with the Chinese regime's military, an issue the Trump administration is seeking to address with sanctions and new legislation.

Fiber-optic technology transfers large amounts of information at very high speeds. It is a "dual use" technology, one used in both civilian and military sectors.

For public use, fiber optics carry telecom data, such as internet communications. For the military, fiber optics are used in ships, jets, and other systems to transmit high volumes of data. In a battle, the speed of these systems can mean the difference between victory and defeat.

A development contract was awarded by



A Chinese pilot stands by as foreign military attachés inspect one of the Chinese regime's J-10 fighter jets at the Yangcun air force base in Tianjin, China, on April 13, 2010.

the Pentagon to a Japanese-owned company based in North Carolina, known as Sumitomo Electric Lightwave, to develop a next-generation fiber-optic cable. After the company developed the technology for the U.S. military, however, it began selling the fiber optics to private companies. Through its offices in Beijing, Sumitomo sold this

technology to Chinese telecom companies ZTE and Huawei.

ZTE and Huawei have been no strangers to controversy. ZTE was sanctioned, and Huawei is under investigation for selling forbidden technologies to Iran. Both companies also have connections to the Chinese Communist Party's military, the People's

STR/AFP/GETTY IMAGES



A U.S. military intelligence officer speaking anonymously said that not long after Sumitomo sold this U.S.-funded fiber optics to ZTE and Huawei, the PLA got its hands on it.

Liberation Army (PLA).

A U.S. military intelligence officer speaking anonymously said that not long after Sumitomo sold this U.S.-funded fiber optics to ZTE and Huawei, the PLA got its hands on it.

The officer said he had seen intelligence that confirmed PLA military equipment is using the same fiber optics commissioned by the Pentagon.

"It wasn't stolen. It was for civilian, or non-military, purposes," he said. "In China, it is being used for naval and for aircraft, like the J-10 jet, the high-end destroyers, cruisers, as well as for these evolving carriers."

Sumitomo Electric Lightwave has been the leading edge of developing highly advanced fiber optics for shipboard use, as well as for fighter jets and drones.

"Some of the technology has inadvertently come into control of ZTE and Huawei."

A Quiet Arms Race

When it comes to advances in military equipment, underlying technologies such as fiber optics also need to keep pace to make the weapons systems effective. The

officer noted that between nations, "it's a constant race" to keep up with the development of systems such as fifth-generation fighter jets and shipboard weapons that process massive amounts of data. "If you, as an adversary, have access to that technology, you see generations of development."

"The core issue of fiber optics is the ability to transmit data rapidly. Each new generation speeds it up. The faster you can transmit, the better it is," he said, and added that there is "light-years' [worth]" of difference between fiber optics technology today and that of 30 years ago.

According to Richard Fisher, a senior fellow with the International Assessment and Strategy Center, advanced fiber-optic cables such as those developed by Sumitomo, "would be very attractive to the PLA."

To grasp the significance of fiber optics to military technology, Fisher noted that it's important to understand a bit of history.

In the 1970s, fighter jets moved to "fly by wire" technology, in which pilots controlled the planes by electric rather than hydraulic signals. Fisher said that for the fighter jets, this allowed for a "radical increase in maneuverability."

The next development was with the introduction of fiber optics, referred to as "fly by light" technology. He said, "Compared to 'fly by wire,' fiber-optic cable allows for much more rapid and far greater transmissions of data."

"Modern fighter radar and electronic warfare systems are dealing with data loads that are orders of magnitude greater than radar and electronic systems of the 1980s," Fisher said. "The ability to move data faster could mean the difference in who calculates a fire solution first and shoots down the other guy."

The officer said the same applies to missile systems. "The quality of rapid communications and high-speed data transmission is critical for effective missiles, and anti-ship missiles, and whatever missiles you can think of."

Technology Transfers

According to an intelligence memo obtained by The Epoch Times, the Sumitomo technologies may have also been transferred to Iran. It states, "In Iran, the products ended up sometime between May 2009 and December 2009 with Isfahan Optics Industries, part of state-owned defense operation."

It says these technologies are believed to be "a substantial quantity of FTTx Service Drop cable and about 30 (or many more) of the Type 39 Alignment Splicer." The memo notes there is "limited information" on the exact quantities that were transferred.

It says the products made their way to Iran first through Malaysia, then through Dubai. It includes unconfirmed analysis on four additional companies believed to have been involved with the transfers to Iran.

The officer made clear that Sumitomo's previous dealings with ZTE and Huawei do not appear to have been illegal. Yet, he said, the problem of dual-use technologies finding their way into hostile hands is becoming one the United States can no longer ignore.

"The suppliers, there is nothing nefarious about them—they are not trying to do something bad," he said. Among the problems is that after technologies are sold in a country like China, "technology suppliers don't know how it will be used," since there is no requirement for companies to know their end users.

He noted several additional cases. One involved a company selling technology to Iran for high-value specialty metal alloys. Although the initial use of the technology was benign, he said, "The exact same stuff can be used to build similar components for nuclear weapons—these were dual-use."

Another case was a Shanghai steel company that was obtaining metal technologies from Western companies. The technologies were then used for PLA weapons programs.

"The issue here is, there is no restraint to using technology in questionable environments," he said.

"One of the biggest culprits in this whole scheme is President [Bill] Clinton, because he freely allowed China access to advanced military technology, like the W88 nuclear warhead. There were no restrictions."

"The [CCP] gained 25 years of development by getting U.S. technology for free."

Regarding the case of a Pentagon-financed program ending up in the PLA's hands, the officer said that the Beijing office of Sumitomo "should have at least made the attempt to see who the true end user is ... Japanese companies, U.S. companies, whatever, know that a transfer technology could be used for all kinds of things."

He said it's a common problem in China that a foreign company working there does so with the knowledge that the Chinese Communist Party will obtain their technology. "The moment you insert technology into China, it's lost," he said.

Fisher shared a similar perspective, saying, "The Chinese military-industrial complex is constantly scouring the earth for top-of-the-line technologies that can be applied to military systems China is developing."

"Huawei and ZTE are cat's paws for Chinese Communist Party domination, and we should treat them as such in every conceivable way."

"The reality of China's pervasive civil-military integration policies means that anything we sell to China will be evaluated for military exploitation. ... Anything we sell China ... should be evaluated on whether that technology could end up killing our troops."

ZTE and Huawei did not respond to requests for comment sent by email.

EXPORTING TYRANNY

Telecom Role in the CCP's One Belt, One Road

EMEL AKAN & FRANK FANG

The CCP has built a vast, high-technology system to surveil the Chinese people, and it is exporting this system as part of its One Belt, One Road initiative. Two of the primary players in this push are the companies ZTE and Huawei.

Recently, Sens. Marco Rubio (R-Fla.) and Chris Van Hollen (D-Md.) warned the Trump administration that ZTE was helping China export surveillance tactics to the Nicolás Maduro regime. The Chinese telecommunications giant, which has been penalized for violating trade sanctions on Iran and North Korea, may acquire additional U.S. sanctions as the company's business with the Venezuelan government faces new scrutiny.

Rubio and Van Hollen sent a letter to the U.S. secretaries of state, the treasury, and commerce, urging an investigation into company's activities.

"Huawei and ZTE are two sides of the same coin," Van Hollen said in a state-

“

Huawei and ZTE are two sides of the same coin.

Sen. Chris Van Hollen (D-Md.)

ment, adding that Chinese telecom companies represent a "fundamental risk" to U.S. national security.

In the letter, the senators referred to a recent Reuters report stating that the Chinese telecom firm assisted the Venezuelan government in establishing control over its citizens. According to the Reuters report, ZTE helped the Maduro regime to build a database that enables the monitoring and tracking of Venezuelan citizens and, since 2016, to centralize video surveillance.

"We are concerned that ZTE, by building this database for the Venezuelan government, may have violated U.S. export controls and sanctions laws, as well as the terms of the Commerce Department's June 2018 superseding settlement agreement with ZTE," the senators said in the letter.

ZTE has a history of breaching U.S. government sanctions. In April, the Commerce Department found ZTE had violated a settlement reached in 2017, and blocked the company from buying crucial components and software from American technology companies. ➤



'F7' Huawei's Alleged Codename

ANNIE WU & CATHY HE

At a court hearing on Dec. 7, details emerged about the alleged crimes of Huawei Chief Financial Officer Meng Wanzhou, who was arrested in Canada days earlier at the request of U.S. authorities.



A crowd waits in line to enter the courtroom to watch the bail hearing for Huawei CFO Meng Wanzhou in Vancouver, Canada, on Dec. 10, 2018. RICH LAM/GETTY IMAGES

According to Canadian prosecutors, Meng had committed fraud in relation to violating Iran sanctions. She had misrepresented the relationship between Huawei and Skycom, a Hong Kong-based company that reportedly sold U.S.-manufactured computer equipment to Iran. Huawei, in fact, controls Skycom, the prosecutors allege.

Huawei's Iran dealings were hinted at in 2016, when the U.S. Commerce Department published internal documents from Huawei competitor ZTE. The company, also a major telecoms firm in China, was punished by U.S. authorities for violating sanctions to provide electronic equipment to Iran.

Competitor Codenamed 'F7'

The internal ZTE document, dated August 2011, cited a rival company code-

YURI CORTEZ/AFP/GTET IMAGES

Venezuelan riot policemen shoot tear gas at students in Caracas on Nov. 21, 2018. Chinese technology companies are helping China's communist party to export surveillance tactics to the Maduro regime.



named “F7” as an example of how to skirt U.S. export controls.

Such guidance was needed because at the time, ZTE had projects in five embargoed countries: Iran, Sudan, North Korea, Syria, and Cuba, according to the document. It said that F7 hired attorneys specializing in U.S. export-control laws for its main company as well as its subsidiaries. It recommended similar methods for ZTE.

F7 also hired a “big IT company” to serve as a front to sign contracts for projects in embargoed countries.

The document goes on to warn that F7’s actions had caught the attention of U.S. lawmakers.

“In 2010, U.S. Representatives reported to Congress about F7’s on-going projects

The document’s description of F7 squarely matches that of Huawei.

in embargoed countries and this affected its project acquisitions in the U.S.,” it read. In particular, “F7’s proposal to acquire U.S. 3leaf Company was opposed by the U.S. government, citing the impact to U.S. national security.”

In 2011, it was widely reported that Huawei had sought to acquire U.S. server-technology company, 3Leaf. Huawei dropped the bid after the U.S. government concerns.

And so, the document’s description of F7 squarely matches that of Huawei.

Codenames Common

In fact, bloggers in China had already published the meaning of the F7 code back in 2014.

At high-level internal meetings, many

major Chinese companies use codes instead of directly mentioning one another.

“F7” was code for Huawei because when said in Mandarin Chinese, “F7” sounds like “fu qi,” meaning “husband and wife.” The first letters of the phrase correspond to Huawei’s abbreviation, HW.

In Huawei’s internal documents, its chief competitor ZTE is referred to by executives as 26.

The numbers “er liu,” when spoken in Mandarin Chinese, sound like the Chinese phrase for “second-rate”—a way of signaling contempt for a competitor. Furthermore, the 26th letter of the alphabet is Z, referring to ZTE.

Huawei considers itself a first-class company compared to ZTE.

ZTE is highly dependent on U.S. suppliers like Qualcomm, Google, and Corning to manufacture its cellphones and telecom equipment.

The ban nearly brought the company to the brink of bankruptcy, prompting a rare intervention by Chinese leader Xi Jinping.

In June, ZTE reached a settlement with U.S. authorities, agreeing to pay a total of \$1.4 billion in fines and to overhaul its board of directors and senior management ranks. In exchange, the United States lifted the ban.

"The Venezuelan government hired ZTE to build a database and develop a mobile payment system for a smart ID card," the lawmakers wrote.

The project was inspired by China's national identity card program that tracks the social, political, and economic behavior of its citizens. The program enables the government to monitor everything from a person's personal finances to medical history and voting activity.

The system in Venezuela was built using components from Dell Technologies in the United States, which alarmed the senators.

"ZTE installed data storage units built by Dell Technologies," the letter stated. "Though Dell's transaction appears to have been with ZTE in China, we are concerned that ZTE may have violated U.S. export controls by misidentifying the end-user or purpose of the end use."

ZTE is China's second-largest telecom equipment maker. The company is publicly traded, but its largest shareholder is still a Chinese state-controlled enterprise.

Violations

A spokesperson for the Commerce Department confirmed that it had received the senators' letter.

"The Department of Commerce will remain vigilant against any threat to U.S. national security and continues to diligently implement the settlement agreement with ZTE. We have no further comment at this time," stated the spokesperson in an email.

As part of the settlement deal in June, ZTE has allowed the U.S. Commerce Department to monitor the company's behavior.

Both Rubio and Van Hollen have been vocal about ZTE's potential violations and about retaining sanctions on the firm.

"We have not received a response to our letter at this point," stated a spokesperson for Van Hollen.

Van Hollen co-sponsored a bill introduced in September called the ZTE Enforcement Review and Oversight (ZERO) Act. The legislation requires the Commerce Department to put ZTE out of business if it violates the current agreement with the United States.



The ZTE stand during the Mobile World Congress in Barcelona, Spain, on Feb. 27, 2018.

Beijing is now exporting its surveillance technologies to other countries.

On Dec. 1, as part of a U.S. probe, Canada arrested Meng Wanzhou, the chief financial officer of Huawei, another Chinese telecom company.

The United States was pursuing Meng, the daughter of Huawei's founder, in a criminal probe related to the violation of sanctions against Iran.

"While the Commerce Department focused its attention on ZTE, this news highlights that Huawei is also violating U.S. law," Van Hollen said in the statement. "We need a comprehensive plan to hold the Chinese and their state-sponsored entities accountable for gross violations of the law and threats to our security."

A Push Into Panama

China's top telecom firms are also making inroads in Panama. R. Evan Ellis, a professor of Latin American studies at the U.S. Army War College Strategic Studies Institute, predicts that Huawei and ZTE will be the dominant providers of telecom infrastructure and services in Latin America and the Caribbean, with a "near-monopoly status" eclipsing local providers by 2050.

Such dominance, according to Ellis, would give China "virtually limitless capability to collect business intelligence or appropriate technologies to give an unfair position to PRC-based companies," he said for a report published by U.S. think tank Center for Strategic and International Studies on Nov. 21.

The two firms' dominance could also compromise "virtually any military, government, or business leader in the region, to obtain from them valuable political and military intelligence," he said.

Huawei was even recently awarded a contract for installing a street-level surveillance system with facial recognition cameras linked to a data network based in the city of Colón—allowing the Panama government to mimic China's mass

surveillance system, in which millions of cameras currently monitor citizens throughout the country and have been used to snuff out dissidents. Panama's system would also be wired to the government offices of defense, migration, fire department, and ambulance service.

Beijing has deployed advanced surveillance technology especially in the region of Xinjiang as part of its efforts to monitor and persecute Uyghur Muslims and other ethnic minorities. The Chinese regime is now exporting its surveillance technologies to other countries.

Many governments around the world, including in the United States and Australia, have raised concerns about equipment and phones made by Huawei and ZTE. The Pentagon issued an order in May to remove all phones from these two companies sold at stores on U.S. military bases, out of concern that those devices could be used to spy on U.S. forces.

China and Panama signed multiple cooperation deals after Chinese leader Xi Jinping's recent visit to the Central American country. However, experts are voicing concerns that the closer relationship between the two countries could be damaging to Panama's interests, as well as those of the United States.

Xi arrived in Panama on Dec. 2 for a 24-hour visit, during which he met with Panamanian President Juan Carlos Varela. The two leaders signed 19 cooperation agreements for trade, infrastructure, banking, education, and tourism, according to Reuters. One of the agreements calls for China to provide non-reimbursable aid to Panama for carrying out the different projects; the amount wasn't disclosed.

Additionally, Varela expressed support for Panama's continued participation in projects under Beijing's "One Belt, One Road" (OBOR, also known as Belt and Road) initiative, according to China's state-run media Global Times. Beijing first announced OBOR, a bid to build up geopolitical influence through trade networks, in 2013. The initiative includes billions of dollars' worth of investments in countries throughout Asia, Europe, Africa, and Latin America.

Corruption Concerns

Panamanian economist Eddie Tapiero raised concerns about the relationship with China, while speaking at a news program run by Panamanian broadcaster TVN.

"It calls us to be more demanding in areas of transparency, corruption, and the law. If that doesn't happen, the initiative [with Chinese investment] would not work out" because the money would be squandered, Tapiero said, and efforts "to boost Panama would not happen."

While Tapiero didn't elaborate on how corruption might take place, China's OBOR has been known to foster corruption in countries with weak institutions, while benefiting the Chinese regime and harming local interests. One example involves Malaysia, whose newly elected Prime Minister Mahathir Mohamad canceled some \$23 billion worth of OBOR infrastructure projects in August after his predecessor was charged with corruption and money laundering in relation to funding for the projects.

Similar transparency concerns were voiced by Miguel Antonio Bernal, a law professor and a candidate running in Panama's 2019 presidential election, who said, "[China has] a colonization plan and we don't have the professional capacity to resist it. We are like an ant wanting to be friends with an elephant," according to a Dec. 2 article by U.S.-based Spanish-language cable news channel Univision.

China Investments

Chinese companies have invested heavily in Panama in recent years. For example, in May 2017, China's Landbridge Group, under the OBOR initiative, was awarded the contract to expand Panama's largest port, the Colón Container Port, for about \$1 billion. The firm began construction in June 2017, according to China's state-run media.

In July 2018, China's state-run China Communication Construction and its subsidiary China Harbor Engineering won the bid to construct a new bridge over the Panama Canal, with a \$1.42 billion contract.

In an article published Sept. 21, Global Americans, a nonprofit platform that provides news and analysis on Latin America, pointed out several cases of Chinese companies being awarded public contracts under dubious circumstances.

China Harbor Engineering, for example, was awarded the bridge contract following the "unexplained withdrawal of one of the competitors from the bidding process." Additionally, the company's final design closely resembled one submitted by the competitor that lost the bid.

US Interests

Both the United States and China are heavily dependent on the Panama Canal for trade. According to statistics by government agency Panama Canal Authority, in the 2018 fiscal year, the United States was the top user of the canal, with about 68 percent of total trade going to or from the country. China was second, with about 16 percent.

The U.S. congressional committee China Economic and Security Review Commission (USCC), issued a report in October on China's engagement in Latin America

“
While the Commerce Department focused its attention on ZTE, this news highlights that Huawei is also violating U.S. law.

Sen. Chris Van Hollen

and the Caribbean, warning of the challenges posed by China's investment in the region. The report concludes that Chinese investment would reduce the United States' strategic influence in the region, diminish U.S. regional security relationships, and undermine U.S. promotion of international norms such as democracy and fair labor practices.

China is currently constructing port facilities at both ends of the Panama Canal: Port Balboa and the Amado Cruise Terminal near the entrance connecting to the Pacific Ocean; and Panama Colón Container Port at the Atlantic Ocean entrance.

The USCC report includes comments by Navy Adm. Kurt W. Tidd, commander of the U.S. Southern Command, who stated that "increased reach to key global access points like Panama creates commercial and security vulnerabilities for the United States."

The USCC report questions the economic feasibility of some of the Chinese projects, including the \$167 million Amado Cruise Terminal, which is "not along any major cruise ship routes."

LUIS ACOSTA/AFP/GETTY IMAGES



Chinese leader Xi Jinping (L) and Panama's President Juan Carlos Varela in Panama City on Dec. 2, 2018.



A delegate looks at his smartphone at the 19th Chinese Communist Party Congress in Beijing on Oct. 19, 2017.

GREG BAKER/AFP/GETTY IMAGES

Huawei toes the party line very closely on issues including the persecution of Falun Gong, a peaceful meditation and spiritual practice based on the tenets of truthfulness, compassion, and tolerance.

AP PHOTO/CHIEN-MIN CHUNG



Police detain a practitioner of the spiritual discipline Falun Gong in Tiananmen Square on Oct. 1, 2000.

HUMAN RIGHTS ABUSES

Tools Huawei Developed to Persecute Falun Gong Now Repress All of China

JENNIFER ZENG

WASHINGTON—While the West has only recently recognized the potential security threat posed by Chinese telecommunications company Huawei, some China insiders have long known that the company is part of the Chinese Communist Party (CCP) apparatus.

Huawei toes the party line very closely on issues including, for example, the persecution of Falun Gong, a peaceful meditation and spiritual practice based on the tenets of truthfulness, compassion, and tolerance. In cooperating with that persecution, Huawei has developed tools that should be of concern to everyone around the world, not just the practitioners of Falun Gong in China.

Persecution

In July 1999, then-CCP leader Jiang Zemin began a campaign to eradicate Falun Gong out of fear of the large numbers of Chinese who found its traditional moral teachings more attractive than the party's atheist ideology.

New York resident Mindy, who asked to only be identified by her given name due to fears for her family members back in China, came to the United States from China in 2009.

Huawei has done far more in the persecution of Falun Gong than simply policing its own employees.

She says that as early as 1999, when the persecution had just begun, Huawei had adopted a policy of not employing Falun Gong practitioners.

That year, Mindy was a graduate student at Zhejiang University. A Falun Gong practitioner she knew in the same university had studied computer science, and before he graduated, he had already been recruited by Huawei, which was aggressively hiring at the time.

However, when he was about to sign the contract with Huawei, he found that there was an item stipulating that all Huawei employees must guarantee that they wouldn't practice Falun Gong.

"This Falun Gong practitioner didn't want to sign this kind of contract," Mindy said. "As a result, he couldn't be employed by Huawei. And Huawei not only had this item in the contract, but also actively asked every would-be-employee if they practiced Falun Gong."

Mindy was married for nearly two years to an IT engineer who worked for Huawei. Her husband also was a member of the Party. Mindy says she once saw a rule in his copy of the Huawei employee handbook that forbade employees from practicing Falun Gong.

The Minghui website, which serves as a clearinghouse for information about the persecution of Falun Gong, reported the case of Wu Xia on Aug. 2, 2007. Wu, then 27, was a Falun Gong practitioner and a Huawei employee who was dispatched to the No. 1 Factory of Taijinbao Company (a Huawei supplier in Suzhou City) to work on quality control, together with her colleague Peng Weifeng. When Peng found out that Wu was a Falun Gong practitioner, he reported her to her manager.

On June 1, 2007, two Taiwanese managers of Taijinbao Company took Wu to the police station. The next day, Wu was transferred to the Wujiang City Detention Center in Suzhou City.

Another Minghui report on Feb. 26, 2008, stated that Wu was given a three-year jail term in December 2007 and was held at Nantong Women's Prison in Jiangsu Province. The report said that she had suffered severe mental and physical damage there and was not in a good condition.

No updated information about Wu can be found.

Another Huawei employee who has been persecuted for his connection with Falun Gong is Liu Guangrong. According to a Minghui report, Liu worked at the canteen of the European Headquarters of Huawei Technologies in Dusseldorf, Germany. He was dismissed by the company in September 2008 after he told a Chinese co-worker on the subway on his way to work about the persecution of Falun Gong and a grassroots movement to quit the CCP (known in Chinese as Tuidang).

"The colleague immediately reported their conversation to Liu Guangrong's departmental chief," the report states. "The chief told Mr. Liu, 'You must not talk to the Chinese staff about Falun Gong and the Quit-the-CCP movement. Our company has regulations that do not allow the staff to talk about these sensitive topics. It will do you no good if you talk about these subjects.'"

Censoring and Spying

Huawei has done far more in the persecution of Falun Gong than simply ➤

NEWS ANALYSIS

policing its own employees. It has helped put in place the tools used by the Chinese regime to track Chinese citizens and censor what information they can access, thus enabling the persecution.

A 172-page internal document from Huawei, written in 2015, was leaked this year and circulated on the internet. The file was entitled “VCM (video content management) Operation Guide” and was used to train the Chinese regime’s internet police on how to monitor, analyze, and process video content in real time. The police were expected to send out alerts should they find anything “suspicious.”

According to Chinese commentator Chen Simin, this leaked document shows Huawei’s deep involvement with the CCP’s surveillance programs “Golden Shield Project,” which is used to block access to information, and “Skynet System,” used for surveillance of the whole society.

By blocking information, the Chinese regime works to prevent the Chinese people from learning about the massive violations of human rights carried out in the persecution of Falun Gong, as well as the teachings of the spiritual practice.

The surveillance tools Huawei has helped to develop are used for many purposes, but among them is the tracking of Falun Gong practitioners.

Chen said that the initial demands for the Golden Shield Project came from the Public Security Bureau and the 610 Office, the Communist Party executive commission tasked with carrying out the persecution of Falun Gong.

Social Credit Scores Going International

The Skynet System identifies an individual through facial recognition technology and locates the person’s information in a state database. That database now gives each person a “social credit” score that indicates the degree to which the individual aligns with the regime’s priorities.

The competence Huawei has developed in establishing this vast system may be used to collect data outside China.

Yu Chao, a U.S. system engineer, said that the international community should be very worried about the possibility of Huawei collecting mass data on people from other countries via their devices and networks. This information can then be used to compile a social credit score on non-Chinese as well.

“The gloomy picture is, although the CCP won’t use Americans’ ‘social credit scores’ to stop them from buying airplane tickets, they can gain very deep knowledge of virtually everything of someone who is in their database, and use this knowledge when needed,” Yu said.

“And that is really, really terrifying.”

SURVEILLANCE

US Technology Used for Mass Surveillance in China, Say US Lawmakers

Program to monitor minority populations serves as pilot for nationwide implementation and foreign export

LEO TIMM

As the Chinese regime expands and upgrades the technology of its campaigns against internal dissent, allegations have emerged that Western know-how indirectly aided the communist state’s repression of the Chinese people.

In May, U.S. Sen. Marco Rubio (R-Fla.) and Rep. Chris Smith (R-N.J.), who also chair the Congressional-Executive Commission on China, sent a letter to the U.S. Department of Commerce expressing concern about U.S. companies that sold surveillance and crime-control technology to Chinese firms.

According to the commission’s report about the letter, the Chinese authorities “continue to violate international protections of due process, privacy, association, religious practice and international prohibitions against torture and arbitrary detention.”

Citing the example of Xinjiang, Rubio and Smith described “dramatically increased surveillance activities of Uyghur Muslims and other ethnic minorities” living in the northwestern Chinese borderland province. Meanwhile, the lawmakers also cited a study by Adrian Zenz, a Germany-based researcher who estimates that between 500,000 and 1 million Uyghurs have been detained for “re-education” in a vast system of newly constructed camps.

In recent decades, as China built up extensive economic ties with the outside world, the Chi-

nese Communist Party (CCP) has gained access to trillions of dollars’ worth of technology and other intellectual property that greatly boosted the capabilities of the Chinese police.

Rubio and Smith’s letter identified Thermo-Fisher Scientific, an American company based in Massachusetts, as having sold “DNA sequencers with advanced microprocessors under the Applied Biosystems (ABI) Genetic Analyzer brand to the Chinese Ministry of Public Security and its Public Security bureaus across China.”

The letter urged the Department of Commerce to implement greater measures to prevent technology that could be used to assist the Chinese regime’s widespread human rights violations.

In the ongoing trade war between the United States and China, the Trump administration has broadly taken the CCP to task about its misuse of advanced technology. In April, the Department of Commerce announced a seven-year ban on selling U.S. components to ZTE, a prominent Chinese tech company that was pioneering an ambitious 5G network, for shipping U.S.-produced products to Iran and North Korea despite trade sanctions. The ban was lifted in July after ZTE paid \$1.4 billion in penalties.

Digital Dictatorship

The northwest region of Xinjiang—where a majority of the population practices Islam and belongs to various Central Asian ethnic groups rather than the Han Chinese national majority—has been a



GUANG NIU/GETTY IMAGES



Chinese policemen push Uyghur women who are protesting in a street in Urumqi, Xinjiang Province, China, on July 7, 2009.

One of the companies working with the public security authorities in Xinjiang is Chinese technology firm Huawei.

source of religious and ethnic unrest since the Chinese Communist Party took power in 1949.

The CCP, which promotes atheism and Marxism, has treated Chinese Islam with the same ideological prejudice that it uses to persecute other religious faiths. During the Cultural Revolution, Muslims were often attacked and humiliated, such as by being forced to consume pork. In later decades, terrorist attacks and other acts of defiance against the Chinese regime by Muslim radicals and ethnic separatists invited overwhelming crackdowns by the CCP security forces.

According to Adrian Zenz's report, the Chinese regime has imposed an unprecedented level of control over the population of Xinjiang, using brainwashing techniques originally devised to "transform" adherents of Falun Gong—the spiritual practice the CCP banned in 1999 and has tried to eradicate in the nearly two decades since.

Meanwhile, Xinjiang has served as a testing

ground for sophisticated forms of mass surveillance and control, made possible by the newest developments in digital technology.

Advanced facial recognition software allows the public security authorities to track the movements of just about every person using an extensive system of security cameras, while their cell phones are subject to frequent scanning. Police also collect samples of the blood and saliva of Xinjiang residents for storage in state DNA databases, as well as fingerprints and voice recordings.

Police methods pioneered in Xinjiang have been implemented elsewhere in China, where the draconian "social credit system" was recently used to bar people with low scores from buying air and rail tickets.

Large state-backed Chinese tech firms are playing a major role in the development of digital police tools.

As reported in a May 14 article by The Globe ➔

and Mail, one of the companies working with the public security authorities in Xinjiang is Chinese technology firm Huawei, which recently set up a development lab in Urumqi, the provincial capital of Xinjiang, in cooperation with the local police to ensure “social stability and long-term security.”

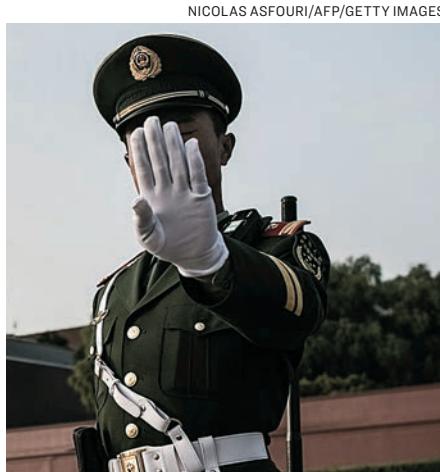
“The fact that companies like Huawei are able to develop such systems in regions like Xinjiang in tandem with the security services, and therefore with very few privacy restrictions—they are gaining a problematic advantage over comparable Western companies,” said Adrian Zenz, who is an expert on Xinjiang at the European School of Culture and Theology in Korntal, Germany, in an interview with The Globe and Mail.

“Moreover, the fact that these systems can serve multiple purposes at the same time—both improve city efficiency and governance and enable intrusive surveillance—makes surveillance both more accessible and perhaps also more palatable in other nations.”

Citing human rights workers, The Globe and Mail noted that Huawei, being a major multinational company controlled by the Chinese authorities, could help facilitate the expansion of the CCP’s “stability maintenance” methods beyond China’s borders.

“The surveillance technologies being developed and deployed in Xinjiang today will soon be sold and promoted globally,” said William Nee, a researcher at Amnesty International, in an interview with The Globe and Mail. “It is now absolutely vital that the international community take a stand and confront the human rights violations occurring in Xinjiang as a matter of strategic importance.”

“Huawei, for example, has promoted a ‘smart city’ concept that it has marketed around the world.” Nee characterized the concept as a tool “to facilitate city planning and management of vital services such as transportation and security.”



A paramilitary police officer near Tiananmen square in Beijing on Oct. 22, 2017.

CHINA TECHNOLOGY

Suicide of Chinese Scientist Sparks Controversy

NICOLE HAO

A Stanford University physicist and entrepreneur who was rumored to be in line for the Nobel Prize committed suicide on Dec. 1. His suicide has drawn attention to his record of achievement and his work to advance the objectives of the Chinese regime. It has also inspired speculation about what caused this gifted man to kill himself.

On the same day Zhang Shoucheng committed suicide, the chief financial officer of the controversial Chinese telecommunications company Huawei, Meng Wanzhou, was arrested. Chinese-language media have speculated there is a connection between the scientist’s death and Meng’s arrest, or between his death and U.S. investigations into intellectual property theft.

Zhang’s family has responded to these media reports with a statement: “There is no police investigation, and the authorities have no suspicions about Professor Zhang’s death. You will read that he committed suicide, and this is true. It occurred in San Francisco. But you will also read in the family statement that he had periodic bouts of depression.”

The family also stated: “There is no connection between his death and other events in U.S.–China relations, which has been speculated by some. This kind of misinformation is not only untrue but hurtful to Professor Zhang’s family, friends, and colleagues.”

Multiple Connections

The speculation about Zhang’s death is no doubt fueled by his connections with Huawei, which is at the center of U.S. con-



Physicist and venture capitalist Zhang Shoucheng.

Zhang had received numerous international awards since 2007 for his achievements.

cerns about intellectual property theft from the United States and the use of data to enable repression inside China, but also by his deep involvement in general with the Chinese regime.

In his career, Zhang had multiple connections with the regime, as a state-sponsored academic, a funder of technology projects in the West meant to benefit Beijing, as a recipient of state-sponsored funding meant to propel his venture-capital projects, as likely having connections with one of the more powerful individuals in China, and as a researcher whose discoveries were key to the regime’s goals.

Zhang’s company, Digital Horizon Capital (DHVC, previously known as Danhua Capital), is a major financier of technology found in Huawei phones, and receives Chinese state funding.

Zhang was also recently appointed as a distinguished professor at ShanghaiTech University and tasked with establishing a new research institute there. Since September 2013, the president of ShanghaiTech University has been Jiang Mianheng—the eldest son of former Chinese Communist Party leader Jiang Zemin—who also has close ties to Huawei. ShanghaiTech was founded by the Shanghai municipal government and the state-run Chinese Academy of Sciences.

Financing From China

A November report by the Office of the U.S. Trade Representative lists DHVC as being part of China’s “web of entities” established in Silicon Valley “to further the industrial-policy goals of the Chinese government.”

Such venture-capital firms invest in a

wide range of startups, then “to varying degrees have access to information, technology, and the ability to influence and potentially coerce management,” according to the “Section 301” report, an update on a prior investigation on China’s intellectual property theft practices released in March.

Zhang’s firm traces its funding to Chinese state-affiliated entities. An investment arm of the state-owned firm Zhongguancun Development Group (ZDG) has backed DHVC, among a number of other venture-capital firms in Silicon Valley.

When DHVC was first established in 2013, Beijing’s mayor attended the company’s signing ceremony in Silicon Valley, according to the report. A press release on the ZDG website explained that DHVC would focus on innovative tech developed at Stanford University and other nearby universities, for the purpose of steering projects to Beijing’s Zhongguancun tech hub to commercialize.

“Zhongguancun capital goes out and foreign advanced technology and human capital is brought in,” the press release read.

ZDG’s investment arm helped convince Chinese tech giants Alibaba and Baidu to contribute to DHVC’s first round of funding, raising the total to about \$91 million, according to the report. iFlyTek, a Chinese voice-recognition company that has received Chinese state funding and works closely with China’s Ministry of Industry and Information Technology, has invested \$5 million in DHVC.

BOE Technology Group Co., a tech firm that counts the Chinese regime as its biggest shareholder, invested about 60 million yuan (\$8.9 million).

The report also noted that Meta, an augmented-reality startup that’s among the 113 companies in DHVC’s portfolio, announced in September that it would lay off half its employees in Silicon Valley and move operations to China, “after the Chinese government pressured Chinese investors.”

DHVC also invests in Cohesity, a data management company that counts the U.S. Department of Energy and U.S. Air Force as clients, according to a Reuters report.

Zhang, Jiang, and Huawei

Zhang seems to have some connection both with Huawei, via DHVC, and with Jiang Mianheng, through his connections to ShanghaiTech.

Huawei’s smartphone P10 has a function named FingerSense, which allows users to use their knuckles to interact with the phone’s touchscreen. This technology was pioneered by Qeexo, a U.S. company.

“It’s Qeexo’s honor that Huawei extended our cooperation,” Sang Won Lee,

In his career, Zhang had multiple connections with the regime, as a state-sponsored academic, a funder of technology projects in the West meant to benefit Beijing, and as a recipient of state-sponsored funding meant to propel his venture-capital projects.

the CEO of Qeexo, said at the 2017 Mobile World Congress held in Barcelona, Spain.

Qeexo was founded in 2012. Its significant investors include Zhang’s DHVC and two other companies.

Like the Jiang family, Zhang came from Shanghai. In 1980, he went abroad and eventually became a naturalized U.S. citizen.

In 1999, Zhang was selected to join the Changjiang Scholars and Professors program by China’s Ministry of Education, an initiative to further develop higher education in China.

In 2008, Zhang was recruited into China’s Thousand Talents plan, a Beijing-led effort to attract top scientists and engineers from overseas to work in China, to conduct research at Tsinghua University.

Since then, Zhang was active in China’s academic community.

Zhang had made public statements expressing a desire to help China’s scientific development. In 2013, he became an academic at the Chinese Academy of Sciences.

In 2017, Zhang “discovered a new state of matter called topological insulator in which electrons can conduct along the edge without dissipation, enabling a new generation of electronic devices with much lower power consumption,” according to the U.S. National Academy of Sciences.

This research was seen as critical for further developing semiconductor chips with greater storage and processing capacity. That is an innovation the Chinese regime has aggressively supported to fuel its am-

bition to become a tech manufacturing powerhouse.

Apart from this, Zhang is famous for his work on the quantum Hall effect, the quantum spin Hall effect, spintronics, and high-temperature superconductivity. His passing marked a great loss to the field of physics.

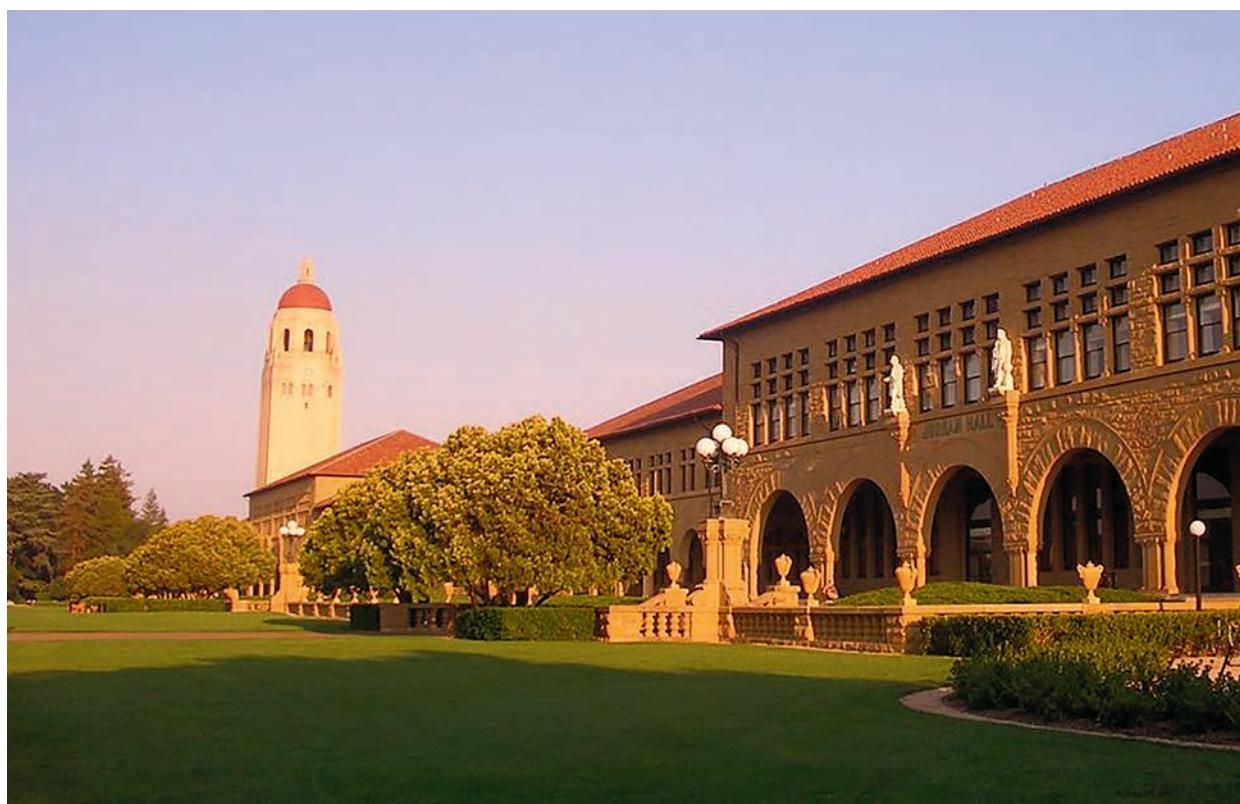
Zhang had received numerous international awards since 2007 for his achievements, including the Oliver Buckley Prize, the Dirac Medal, the Europhysics Prize, the Physics Frontiers Prize in Fundamental Physics, and the Benjamin Franklin Medal. At the time of his death, he and his research team were floated as candidates for a Nobel Prize in Physics.

Jiang Relations

On Jan. 23, the state-run China News Service reported that Zhang was setting up a Frontier Science and Technology Research Institute within ShanghaiTech University. The report quoted Xu Li, the director of the Shanghai government’s Overseas Chinese Affairs Office, as saying that Zhang’s institute had the support of the office.

While the exact relationship between Jiang and Zhang is unclear, Chinese university heads are usually acquainted with all professors at their schools. The establishment of a new research institute would certainly happen only with the approval of the president.

Adding to the uncertainty, following Zhang’s death, all reports about the relationships between him and Chinese entities and prominent individuals have been deleted by Chinese internet censors.



PERE JOAN/WIKIMEDIA COMMONS

The Stanford University campus. Zhang Shoucheng was a well-regarded physicist and professor at the school.

Share the Joy!

Tell your friends and family how they can subscribe to The Epoch Times

Dear Reader,

We hope you are enjoying this issue of The Epoch Times, including our special section on Huawei.

The Epoch Times reports the important news avoided by other media. We have been leading coverage of the Chinese communist threat for the past 18 years.

Recently, we conducted a survey. One of the questions was,

Among all other media, how much do you like The Epoch Times (on a scale from 1 to 10)? We are thrilled that 64 percent of our subscribers gave us a 10 out of 10! (See survey results to the right.)

We have received a lot of very inspiring feedback from subscribers that we would like to share with you:

"The Epoch Times has filled an intellectual hole in me that I've been unable to find in virtually every other news media ... particularly here in California."

I find it difficult to find truly unbiased coverage of anything ... but especially politics and current events. To hear my voice heard—and my opinions reflected—by a news publication is a long-overdue dream come true. I find your reporting literate, stimulating and often enlightening. I'll be a subscriber to The Epoch Times for as long as you publish!"

— Cindy McBride, California

Here are ways that our subscribers have shared The Epoch Times with others:

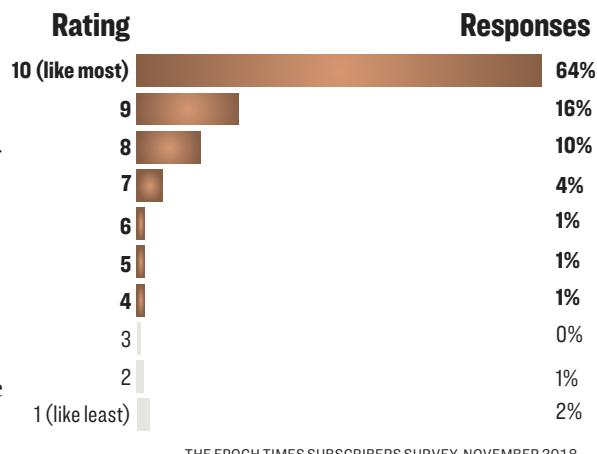
"I really enjoy the way you have it set up online; getting all the pages on the screen at once is great. I share the printed version with my friends."

"I gain a wealth of knowledge on various topics that are not covered by any other newspaper."



I am much better informed. I bring the paper to work to share in the break room."

"As a new subscriber, I take your paper to work and pass it along to others who have similar values that I have, in the hope that they might also subscribe."



"I have found the news coverage and opinion pieces in The Epoch Times to be informative and educational. Your articles on the Socialist/Communist Party in America, and the CCP and its infiltration of our civil institutions, are something that I haven't seen in any other publication. I picked up my first free copy of The Epoch Times as I was leaving a Whole Foods Market a couple of years ago and immediately decided to subscribe. I think you should place more free copies around the Philadelphia area once in a while. I'd be happy to distribute some to those of my friends and acquaintances who I think would appreciate your editorial stance."

"I have given old papers to my friends to read. I believe we must be informed so as not go down the 'same rabbit hole.'"

Tell Your Friends!

If you enjoy The Epoch Times, we hope you will share it with your family members, friends, coworkers, neighbors, and acquaintances.

They can subscribe to The Epoch Times by visiting

ReadEpoch.com

If you don't think they are ready to subscribe to the paper (print or e-paper), please invite them to subscribe to our FREE daily newsletter, filled with insights you won't find anywhere else, at

EpochNewsletter.com

THE EPOCH TIMES

TRUTH AND TRADITION