

THE EPOCH TIMES

TRUTH AND TRADITION



Inside Huawei

CHINA'S VEHICLE FOR GLOBAL SUBVERSION

INSIDE HUAWEI

China’s vehicle for global subversion

Find our first special edition on Huawei at epochtimes.org.au/huawei-1.pdf

From the Editor

The U.S. Department of Justice unsealed two indictments on Jan. 28 against China’s Huawei Technologies Co., as well as two of its subsidiaries and its chief financial officer, Meng Wanzhou. The charges include allegations that Huawei violated sanctions against Iran and stole trade secrets from U.S.-based company T-Mobile.

While Huawei has grown to become the world’s largest telecommunications company and the second-largest smartphone manufacturer, it’s not a normal company by Western standards. Huawei plays a crucial role in several key initiatives of the Chinese Communist Party (CCP). For those familiar with the telecom giant and its operations—including some of the public statements made by company executives about its activities—these charges should come as no surprise.

In this second special edition on Huawei from The Epoch Times, we explain that the company is part of the backbone of the CCP’s One Belt, One Road initiative. We also outline

which of the company’s technologies are used by the CCP in its efforts to subvert other countries, and the risk this presents to national security.

Huawei operates on a unique business model designed for market domination. We explain the inner workings of its company culture.

Aside from Huawei’s alleged violations of sanctions on Iran, the company may have provided assistance to the Taliban. And with the telecom giant now being charged with stealing trade secrets, we provide a translation from a speech by its corporate senior vice president, in which he encouraged staff to use underhanded tactics to help drive the company’s development.

With these stories and others, we hope to shine a light on Huawei’s otherwise opaque operations and provide our readers with deeper insights on the news now dominating the headlines.



Jasper Fakkert
Editor-in-Chief

Table of Contents

3	Chinese Regime Enables Huawei’s Overseas Expansion Through One Belt, One Road Initiative A deeper look at the ties between Huawei and the Chinese regime’s global ambitions	6	Huawei’s History: Taking From IBM and Cisco The company rose to prominence by copying and stealing from U.S. tech giants	8	Huawei in Europe: Will Mao Zedong’s Strategy Win the Market? How Huawei uses the Maoist strategy of “seizing the countryside” to “capture cities”
4	Huawei’s ‘Dare to Die’ Business Model The “gan si dui” kamikaze strategy Huawei uses to dominate markets	6	Huawei Senior VP: Acknowledge and Study US Manufacturing Power An inside look at guidance given to Huawei employees by a senior vice president	10	Ban Huawei to Escape China’s Digital Dictatorial Embrace As Huawei constructs social control systems abroad, it is creating an Orwellian future for the world
4	Huawei’s 5G Patent Race How Huawei plans to get ahead of the technological curve and surpass the United States	7	Huawei’s Alleged Links to the Taliban Huawei’s potential ties to terrorist attacks against the United States	11	Huawei Reveals China’s Foreign Policy Agenda What recent incidents tell us about the CCP’s ambitions with Huawei
		8	Huawei’s Expansion in Africa Comes Under Scrutiny China’s strategy of using Huawei to conquer markets in Africa		

THE EPOCH TIMES

Lillian Fan, Publisher
Jasper Fakkert, Editor-in Chief

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.

CONTACT US

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

Advertising
ad@epochtimes.com.au

Subscriptions
subscribe@epochtimes.com.au

General Inquiries
enquiry@epochtimes.com.au

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 to your door every week.

02 8988 5600

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.

THE EPOCH TIMES

TRUTH and TRADITION

A CURE FOR FAKE NEWS SYNDROME

SUBSCRIBE TODAY 02 8988 5600

Chinese Regime Enables Huawei's Overseas Expansion Through One Belt, One Road Initiative

FRANK FANG

Embattled Chinese telecommunications giant Huawei has been able to expand its business internationally even as many governments around the world voice their concerns about the security of its equipment.

Huawei has successfully transformed into one of the biggest tech giants in the world from a small Chinese company because it serves the interests of the Chinese Communist Party (CCP): providing the advanced technology the Party needs to exert its political clout globally, while assisting the Chinese regime in carrying out surveillance and spying activities.

Huawei was able to build its presence in global tech sectors because the company has been piggybacking off China's "One Belt, One Road" (OBOR, or Belt and Road) foreign-policy initiative in recent years.

In 2013, Beijing rolled out "One Belt, One Road," an aggressive plan to build up trade routes connecting China, Southeast Asia, Africa, Europe, and Latin America. Through the financing of infrastructure projects in more 60 countries, the Chinese regime is seeking to bolster its geopolitical influence around the world.

Huawei is a key participant in those projects.

Internet Cables

On Oct. 22, 2018, Huawei Marine, a joint venture between Huawei and the U.K.-based submarine communications firm Global Marine Systems, announced its Peace Cable project: a 12,000 km (7,456 miles) long underwater high-speed internet cable system linking Pakistan, South Africa, Kenya, Somalia, Djibouti, Egypt, and France. The project is currently in its cable and material manufacturing stage.

The project, which will be jointly carried out by Huawei Marine and the Peace Cable International Network, a subsidiary of Chinese fiber optic manufacturer Hengtong Group, is expected to be in service by the first quarter in 2020, according to Huawei's official website, and will serve as a "new information expressway" from China to Europe and Africa.

Days earlier, Mao Shengjiang, chief operating officer of Huawei Marine, said while speaking at the third Asia Pacific Submarine Network Forum that Huawei Marine has been "contracted to build about 40,000 km (24,854 miles) of submarine cable worldwide, which [is long enough that the cables] could circle the earth at the equator."

But Huawei Marine's global ambitions were stonewalled in June 2018, when Australia stepped in to stop the company from laying underwater internet cables for the Solomon Islands. Australia offered to fund and build the cables instead, which the Pacific island nation accepted. According to Reuters, Australia's decision was based on security concerns, given that Huawei would have had access to a broadband hub in Sydney if it were allowed to lay the cables.

5G Rollout

Huawei is also the key to the Chinese regime's plan to roll out 5G technology around the world.

5G is the next generation of wireless mobile communications technology. Countries are vying for leadership because that technology is seen as critical to future economic growth.

According to a Dec. 2018 report by U.S.-based think tank Center for Strategic and International Studies (CSIS), Huawei has become a market leader in manufacturing equipment that is vital for 5G networks, the radio access network (RAN).

RAN connects mobile users with the 5G core network. According to the report, Huawei is the market leader for RAN equipment, with a 31 percent market share, followed by Ericsson (29 percent) and Nokia (23 percent), in the first quarter in 2018.

Huawei's overseas ventures in both underwater fiber optics and 5G have been in part driven by China's national policy of OBOR.

OBOR

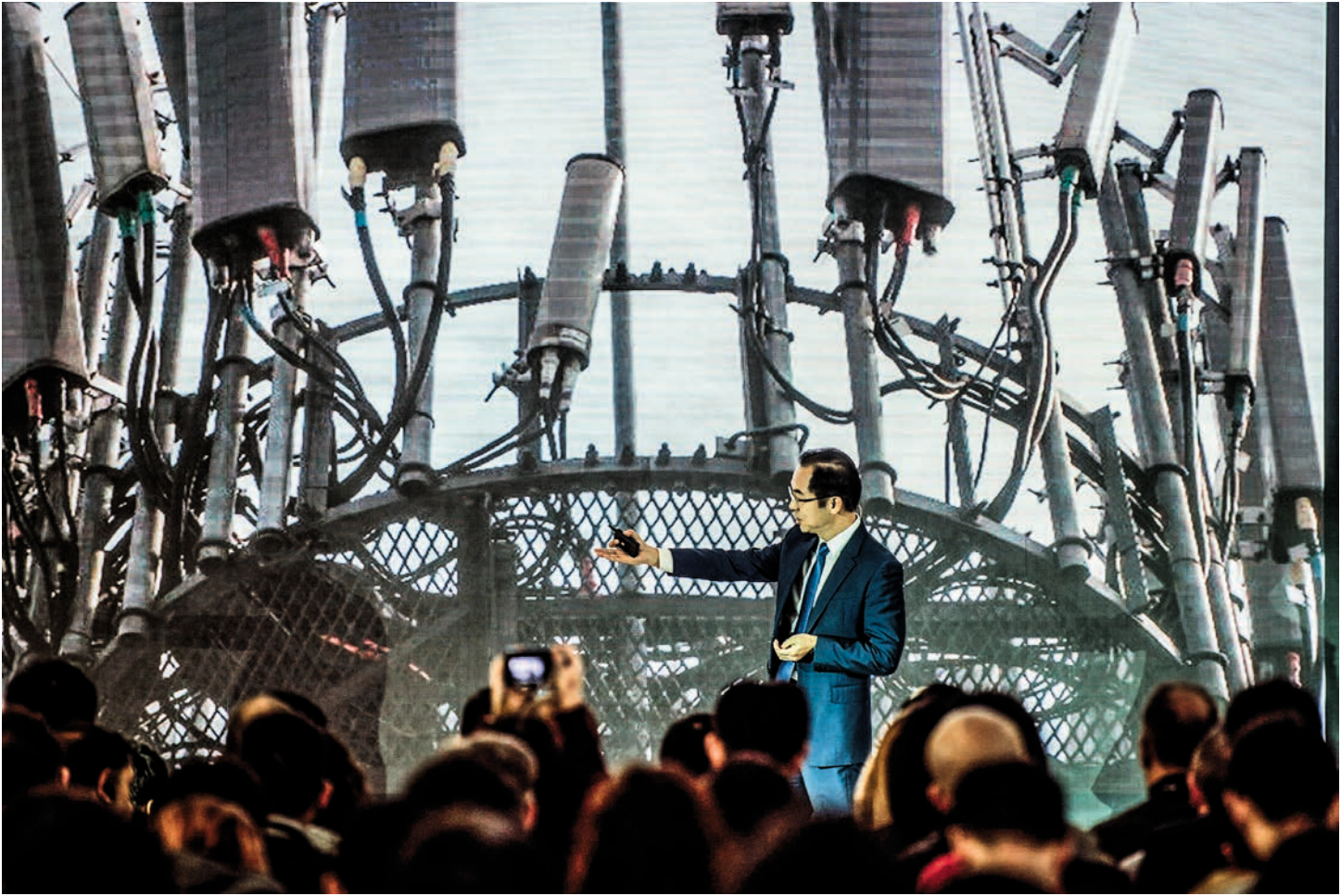
In March 2015, the Chinese regime made clear how important these technologies are to its interests: the National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce, jointly issued a directive detailing goals and actions for OBOR. Two key objectives were the "construction of transnational fiber topics for communications" and "synchronizing technological standards [between China and other countries]."

By dominating 5G standards at international standard-setting agencies, Huawei could pocket licensing fees from mobile-service providers and governments that use its 5G technology. Huawei would also gain earnings from future contracts for maintenance or repair jobs of its sold equipment.

This agenda is in line with Beijing's overall desire to become less dependent on foreign technology. In January 2018, China's state-run media Xinhua reported on its intention to accelerate the development of technical standards for technologies such as 5G and the internet of things (IoT), under the name of "China Standards 2035."

In May 2018, Zhou Jialiang—who was a company director working in Kyrgyzstan at the time and now serves as director for Huawei's Volkswagen account, according to his LinkedIn page—said in an interview with Chinese media 21st Century Business Herald that OBOR provided many opportunities for the company to expand its market in Central Asia and elsewhere.

Zhou said that different OBOR infrastructure projects, such as railways, roads, airports, and oil pipelines, would all require modern telecom equipment to allow systems to communicate with each other—prime business opportunities for Huawei.



FRED DUFOUR/AFP/GETTY IMAGES

Ryan Ding, Huawei president of the carrier business group, at the Huawei Beijing Executive Briefing Center in Beijing on Jan. 24, 2019.

Huawei was able to build its presence in global tech sectors because the company has been piggybacking off China's 'One Belt, One Road' foreign-policy initiative.



GREG BAKER/AFP/GETTY IMAGES

A police officer outside the Canadian Embassy in Beijing on Jan. 27, 2019.

By participating in OBOR, Huawei, which had relied on concessional loans and business loans for overseas expansion, would be able to receive funding from the Asian Infrastructure Investment Bank (AIIB) and the state-owned Silk Road investment fund.

The fund was designed to foster investment in countries under OBOR. Beijing pledged \$40 billion when it was established in December 2014.

Huawei executives have continually made it clear their intentions to capitalize on the Chinese regime's flagship project. While speaking at the annual World Internet Conference in China in December 2015, Richard Yu, CEO of Huawei's customer service division, Consumer Business Group, announced that Huawei would embark on its own "One Belt, One Road" initiative: a plan to reach out to untapped markets around the world.

'Smart City' Projects

OBOR also involves exporting another of China's technological advances: the "smart city."

China's State Information Center published a research paper in December 2015, detailing how the construction of smart cities could help lead the OBOR initiative. The paper applauded Huawei, as well as its domestic competitor ZTE, for undertaking an important role in building "smart cities" in other countries.

In May 2017, at the Belt and Road Forum in Beijing, where Chinese leader Xi Jinping invited heads of state to participate in the project, Xi reiterated the importance of building smart cities under OBOR.

On the company's official website, Huawei has touted its ability to provide "smart solutions," including "safe cities" and "smart cities"—in other words, using Huawei's surveillance technology and cameras.

"A Smart City is a complex mesh of systems across sectors such as transportation, energy, water, and healthcare," according to Huawei's website. The company claims that its "smart city" solution can build up a network, much like a person's nervous system, with "real-time situation reporting and analysis that combines cloud computing, IoT, Big Data, and Artificial Intelligence (AI)."

But inside China, such technology has been used to monitor citizens and snuff out dissidents.

The dangers of Huawei exporting such technology abroad were explained by the think tank Jamestown Foundation, in an article published in June 2018.

"While the smart cities of the future could be better, more efficient cities, they could also provide authoritarian regimes with previously undreamt of tools of surveillance and control," the foundation warned. Additionally, when used in democratic countries, Huawei equipment may "act as a conduit for [Beijing's] intelligence gathering."

An example of Huawei's "smart cities" is at Astana, the capital of Kazakhstan, under the OBOR initiative, according to a 2017 article published by Huawei on its official WeChat social-media account.

In the WeChat article, Huawei claimed that it had reduced the number of traffic violations and crime rates after placing more than 10,000 cameras in Astana.

Jamestown Foundation, in the same article, noted that within three years from 2014 to 2017, Huawei doubled the number of countries where it has deployed its "smart city" technology: to 40 from 20. An interesting pattern emerged: Huawei first deployed it in "a number of authoritarian and hybrid regimes" such as Pakistan, Venezuela, Laos, and Angola, before branching out to democratic countries, such as France and Germany.

In January 2018, the German city of Duisburg signed a memorandum of understanding on a smart city partnership with Huawei. Under the agreement, the two partners will work together on projects such as expanding the city's WiFi network, improving government cloud solutions, traffic management, smart street lamps, and 5G technology.

Smart Energy

Huawei's OBOR projects also include another "smart solution": selling its "smart energy" system to petroleum companies and oil-producing countries,

according to a Nov. 8, 2016 article on its website.

During a speech at the Huawei Global Energy Summit held in Abu Dhabi, Jerry Ji, an executive within Huawei's Enterprise Business Group unit, said that "Huawei is committed to helping oil and gas companies address challenges and build competitiveness in the global market in today's digital age."

Huawei's answer is to offer data solutions technology to energy companies. In November 2016, Huawei and Abu Dhabi Marine Operating Company, a subsidiary of the UAE state-owned Abu Dhabi National Oil Company, announced they established a new cloud data center to help the latter process huge volumes of data created by offshore oil exploration and production.

Huawei, in an article published on its website in June 2018, announced that its oil and gas data solutions have been implemented in 45 countries, providing the service to 70 percent of the world's top 20 oil and gas companies. Some of these "smart energy" deals have been officially declared OBOR projects by the Chinese regime.

Also a part of its "smart energy" solutions, Huawei inked a solar power plant project in Argentina, the company's first successful OBOR project in the South American country.

The solar project, a 300 megawatt (MW) power station, is being built at Cauchari village in northwest Argentina, with financing from Chinese loans. The plant, which adopted Huawei's internet-enhanced "Smart PV" system, is being built by Shanghai Electric, a subsidiary of China's state-owned construction company, PowerChina.

Huawei's possession of such sensitive data can have dangerous ramifications, given its close ties to Beijing. In February 2018, the U.S. Council of Economic Advisers, which conducts economic research to advise the White House, highlighted the potential for cyber attacks on critical U.S. infrastructure sectors to "generate especially large negative spillover effects to the wider economy." Examples of critical infrastructure include utilities, agriculture, and finance.

The council's report cited a 2014 report by PricewaterhouseCoopers that explains the motivation behind such attacks: nation-states would target critical infrastructure providers in order to steal trade secrets and proprietary IP, including financial and workforce-related information, for the purpose of "advancing their political and economic advantages."

Several U.S. lawmakers recently voiced security concerns that Huawei's sales of solar equipment in the United States could threaten the entire American electricity grid.

Rep. Tom Marino (R-Pa.) wrote a letter to the U.S. Energy Secretary Rick Perry, according to the Financial Times, about his concern that "[Huawei's] entrance into large-scale and residential solar markets may pose a threat to our nation's infrastructure."

National Emergency System

One of the country's signature OBOR projects is the national emergency system developed in Ecuador, according to China's official OBOR web portal.

The emergency system, named ECU 911, is built by China's state-owned China National Electronics Import and Export Corporation (CEIEC). Huawei supplied tens of thousands of dollars in equipment to the system, including 4,500 surveillance cameras—some equipped with facial recognition technology, routers, wireless access points, network switches, and wireless access controllers.

Shashank Joshi, a senior fellow at the Royal United Services Institute, a UK-based think tank, expressed concerns about buying surveillance equipment from China, as it encourages authoritarian principles and omnipresent surveillance, according to an August 2018 editorial, titled "Ecuador's All-Seeing Eye Is Made in China" and published by Foreign Policy magazine.

Meanwhile, David Denoon, a professor of politics and economics at New York University and the director of the school's Center on U.S.-China Relations, pointed out another exploitative aspect of working with Chinese companies.

"Telecommunications and surveillance systems are considered attractive projects [for China] because they permit monitoring of local content and usually lead to long-term contracts for replacement parts [in surveillance equipment]," Denoon told Foreign Policy.

Huawei's 'Dare to Die' Business Model

NICOLE HAO

In his analysis of Huawei's business model, Chinese economist Wang Shuangyi came to the conclusion that the massive tech company serves as a "gan si dui," or "dare to die" kamikaze unit in Beijing's strategy to dominate markets around the world.

"The basic business model of Huawei can be summed up as a sweatshop [that works as] the Chinese Communist Party's 'dare to die unit' [in a global] Ponzi scheme," Wang wrote in the Dec. 20, 2018, article.

Wang used the term "dare to die" as a reference to the company's extreme work environment, as well as its special role in the Chinese regime's economic ambitions. Being, at least on paper, a privately owned business, Huawei can carry out certain activities that would be too risky or diplomatically inappropriate for a Chinese state firm.

"Under the banner of patriotism and localization, Huawei and [other Chinese companies] copied, plagiarized, and stole" technology from foreign entities, Wang said. They reverse-engineered foreign technology and "pushed the foreigner suppliers out of China."

"Then, using their profits from the Chinese market and different types of subsidies from China, they exercise active domination in overseas markets," Wang said. The key to this, he says, is that

Being, at least on paper, a privately owned business, Huawei can carry out certain activities that would be too risky or diplomatically inappropriate for a Chinese state firm.

(Below) Huawei CEO Richard Yu presents a new phone in Barcelona, Spain, on Feb. 26, 2017.

Huawei's products come with backdoors that provide a channel for Chinese regime hackers.

Huawei is the Communist Party's "spear," Wang said. "It carries the responsibility for comprehensively purchasing and stealing [foreign] technology."

Wang predicts that as the pernicious nature of the Huawei model becomes more apparent to foreign markets and governments, it will face increasing backlash for its actions. That's been prominently reflected in the recent arrest of CFO Meng Wanzhou by Canadian authorities for her company's alleged violation of U.S. sanctions against the Iranian regime.

The Chinese regime has reacted strongly to Meng's arrest, detaining several Canadian citizens in China and staging high-profile diplomatic protests. It's encouraged a boycott of the Canadian apparel company Canada Goose by the Chinese people. According to Wang, that shows how much the CCP regime values Huawei for its utility in gathering intelligence and expanding its global influence.

Phases of Expansion

Chen Lifang, a board member and senior vice president of Huawei, said in a speech to new Huawei hires last April that China still lags decades behind the United States in many technological fields.



LLUIS GENE/AFP/GETTY IMAGES

"In precision and smart instruments, and test equipment, the gap is bigger ... for all testing devices, we rely on imports," Chen said. "As for equipment banned by The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, our comrades who work on the hidden front have to take the risk and smuggle them."

According to Wang, Huawei has planned three phases to catch up with developed countries.

In the first phase, during the 2000s, Huawei copied the software of Cisco, an American multinational technology conglomerate, and sold its system for less than half the original price. Cisco sued Huawei, but strong CCP regime backing meant that the U.S. company could hardly succeed in court.

Meanwhile, Chinese propaganda promoted Huawei as a patriotic enterprise, and claimed that using Huawei's products was patriotic.

The second phase saw Huawei expand its business overseas while disregarding international

Huawei's 5G Patent Race

ANNIE WU

In January 2018, Chinese state-run media Xinhua first made mention of a new economic strategy with a short article that largely went unnoticed, in a report about a national conference on IT industry standards.

To dominate cutting-edge technologies—such as artificial intelligence (AI), cloud computing, IoT (internet of things), and big data—China intends to accelerate efforts to develop technical standards, eventually exporting them to the international market, the report said.

While global technical standards for these technologies have not yet been established, "this is the golden opportunity for our country's industries and standards to realize the goal of 'overtaking by changing lanes,'" the report quoted an official from China's national technical committee, the Standardization Administration, as saying.

That metaphor is commonly used in Chinese media to describe finding shortcuts to surpass other countries and become the leader, and Huawei's aggressive development of 5G technology fits exactly into the Chinese regime's ambitions.

By dominating 5G standards at international standard-setting agencies, Huawei could pocket licensing fees from mobile service providers and governments that use its 5G technology.

Today, Huawei and its domestic competitor, ZTE, own roughly 10 percent of the 1,450 5G patents filed, compared to Qualcomm's 15 percent, Nokia's 11 percent, and Ericsson's 8 percent, according to a 2018 report by the U.S.-China Economic and Security



Ryan Ding, Huawei president of the carrier business group, holds a Tiangang 5G base station chipset during a product presentation in Beijing on Jan. 24, 2019.

Review Commission.

Meanwhile, the entire country has filed 48,882 patents with the World Intellectual Property Organization (WIPO) in 2017, making it the second highest-ranking country behind the United States.

The year prior, ZTE and Huawei had topped the WIPO list of annual patent applications, at 4,123 and 3,692 patent filings focus on cutting-edge technologies like 5G, IoT, and cloud computing. Qualcomm came in third place.

The rush to file patents is not just about making money. The Chinese regime is keen on cutting its reliance on foreign technology and has championed the principle of "self-reliance" for its tech sector. Huawei, in turn, has stepped up to the plate.

Currently, Huawei is the only major Chinese telecommunications manufacturer that is trying to make the majority of 5G components by itself.

U.S. companies still lead market share for the most advanced technologies, and Chinese firms still depend on Western firms to supply most of the advanced components.

But Chinese firms are quickly catching up. Most critically, they are resorting to underhanded tactics in order to stake their dominance in 5G.

Beating Competition

In an analysis of 5G security concerns published by the U.S. think tank Center for Strategic and International Studies, researcher James Lewis noted that both Huawei and ZTE benefit from government subsidies, giving them the ability to manufacture products and sell them at discounted prices far below international competitors.

Put simply, "the market distorting effects of government-subsidized Chinese companies reduce market share and revenue for other Western firms," Lewis wrote.

As Huawei continues to pursue overseas clients, governments will have to choose between risking security loopholes in buying cheaper Huawei 5G equipment, or paying more for secure equipment made by other firms. "Determining how to persuade countries that they should pay a premium is one problem; determining how to securely connect and communicate over telecom networks in other countries using vulnerable equipment is another," Lewis wrote.

China has also deliberately planned for Chinese technical standards to become the representative at international standards groups—pressuring tech firms to vote for Chinese standards.

One example cited in Lewis's report: Chinese tech company Lenovo had voted for a proposed standard by U.S. firm Qualcomm instead of Huawei at one of the most important standards groups, the Third Generation Partnership Project. The Chinese authorities immediately criticized Lenovo for making the move.

In another instance, the Chinese regime pressured Chinese companies to back a type of technology for which Huawei holds most of the core patents—known as polar codes—instead of more mature competing technologies pioneered by Qualcomm and other Western firms. A standoff ensued, which ultimately ended with the majority of companies voting in favor of polar codes. This means all 5G mobile cellular technology will employ the polar codes.



laws and regulations. Huawei's main competitor in this stage was ZTE, a state-owned telecommunication company and second-biggest telecom equipment manufacturer in China.

"We struggle very hard to compete with Huawei in Africa," Lu J., a ZTE senior project manager, told The Epoch Times. According to Lu—whose full name was withheld to protect his identity—both Huawei and ZTE use bribes in the global market, but Huawei is willing to give more. "They are very generous."

Huawei and ZTE have another advantage not available to U.S. companies.

The CCP regime funds infrastructure projects in other countries. One of the conditions for taking part in this development is that the host country must install Chinese-built equipment. This has resulted in Huawei and ZTE grabbing a big market share in Africa, South America, and other developing regions.

The third phase involves the further development of the CCP's plans, from forcing foreign com-

panies in China to hand over their technology, to recruiting overseas experts and scientists to work for Chinese companies.

"As a private company, Huawei looks independent. By investing in the institutes in Europe and North America, and aiding the universities, it receives technology from them," Wang wrote.

In addition to setting up cooperative programs with foreign universities and institutes, Huawei also creates research centers overseas that can benefit from cutting-edge technology that's produced locally.

"Some CCP military experts can even pose as Huawei employees, and receive training at European and American universities," Wang said. "Huawei's equipment plays a key role in the Party's cyber attacks."

Human Costs

In recent years, there have been many reports about Huawei employees dying from suicide, overwork, or being fired because of age or illness.

"Huawei emphasizes a wolf culture," Wang said. "It lays off employees over the age of 35 en masse."

Xie Ting, a young widow, published a long post on Dec. 25, 2018, to mourn her husband Qi Zhiyong, a 36-year-old Huawei engineer in Kenya, who died of overwork.

Xie said Qi wasn't allowed vacation for 22 months straight.

"One week before the death, he sent me a WeChat message and said might not finish the network cutover [upgrade]. Two days before he died, he worked day and night," Xie said.

After Qi died, Huawei refused to compensate Xie and her two young children, both of whom are under the age of 10.

"The Huawei human-resource manager in Kenya, representative in Kenya, and human-resources director at Huawei headquarters told me that I'm welcome to file a lawsuit for compensation," Xie wrote. "How can a single mom have the money, time, or energy to sue such a huge multinational conglomerate?"

A Huawei poster outside an Apple store in Shanghai on Oct. 26, 2018.

China's bid to dominate the next generation of mobile technology



A staff member displays 5G active antenna units during a product presentation in Beijing on Jan. 24, 2019.

"China has politicized the standards-making process," the report said.

Huawei has also increasingly taken senior leadership positions at these standard-setting bodies, as part of Beijing's attempts to raise its 5G sector's influence.

This is a concerted effort by China to stake its claim. Chinese companies take leadership positions at lower-impact committees, then use them "to promote Beijing's interests through a combination of holding the top leadership slots and contributing funding," the U.S. congressional report said.

Developing Own Chips

To fulfill the Chinese regime's mandate to cut reliance on foreign technology and develop domestic advanced semiconductor chips, Huawei's chip-making subsidiary, HiSilicon, has designed its own smartphone chips that are specially suited for 5G capabilities.

In September 2018, Huawei unveiled the world's first 5G-ready commercial chips for smartphones, equipped with artificial intelligence.

Chip development has consistently been included as part of the Chinese regime's tech development plans, providing significant state support and funding, such as state investment funds and local government funds.

HiSilicon is among a group of domestic firms that are part of a "relatively complete" industry supply

chain for IoT development, providing the bulk of chips, according to the U.S. congressional report.

HiSilicon's smartphone chips are exclusive to Huawei. The company does not sell to third parties. But this pivot toward domestic production is likely to cut into Qualcomm's chip sales—and increasingly, patent royalties—as Huawei pushes for more of its standards to be developed for 5G.

In the current generations of 3G and 4G, Qualcomm had dominated ownership of patents and technical standards, while allowing it to profit from the royalty fees.

To ensure that the United States maintains an edge in 5G innovation, Lewis of the CSIS think tank recommended that the U.S. government encourage private and public research and development, while working with U.S. allies to come to voluntary agreements on 5G security standards.

He also urged U.S. authorities to ensure U.S. companies don't face "unfair obstacles from antitrust or patent infringement investigations undertaken by any country to obtain competitive advantage."

He added that fair competition is crucial to 5G "because it incentivizes companies to build better products and offer better services."

Frank Fang contributed to this report.

In 2016, ZTE and Huawei had topped the WIPO list of annual patent applications, at 4,123 and 3,692 patent filings, respectively.



An employee deals with a customer at a Huawei store in Beijing on March 24, 2014.

Huawei's History: Taking From IBM and Cisco

WANG HUI

A look into Huawei's history reveals a pattern of plagiarism, theft of intellectual property, and hostile competition, through which the company became the world's biggest producer of telecommunications equipment.

Huawei rose to prominence by modeling itself after American tech giants.

In the 2000s, Cisco Systems dominated global market share in telecom equipment, leading the Chinese market, in particular, with its routers and switching equipment. It was at this time that Huawei quickly rose to become Cisco's biggest competitor in China.

In 2000, Huawei CEO Ren Zhengfei proposed the strategy of "crossing the Pacific Ocean with confidence and exuberance," that is, entering the U.S. market by establishing an American subsidiary, Huawei America.

In June of that year, Huawei made its debut at a telecom-equipment exhibition in Atlanta. Huawei presented communication products that were com-

By 2015, Cisco's share of China's router market by revenue had been nearly halved, compared to the beginning of 2014, while Huawei's had jumped by more than 50 percent.

parable to Cisco products in performance, but the prices were 20 to 50 percent lower.

Stealing Code

Around this time, Huawei placed ads in U.S. mainstream media that featured San Francisco's Golden Gate bridge in the background. Notably, Cisco's logo at the time was an outline of the bridge in red.

In a Jan. 2003 lawsuit filed in federal court in Texas, Cisco alleged that Huawei and its subsidiaries had stolen source code for Cisco's networking software—known as IOS—copied documents and copyrighted material, and infringed on Cisco patents.

The allegations centered around Huawei's Quidway switches and routers. Cisco claimed that the Quidway operating system, technical documentation, and user manuals were copied, including whole portions of text.

Huawei initially denied the claims. However, in late March 2003, Huawei admitted in court documents to copying code for its router software. Huawei said that an employee had obtained the code on a floppy disk from a Chinese man who hoped to work at Huawei, and the company's lawyers claimed that the employee didn't know that the software was copyrighted.

Cisco and Huawei reached a settlement in July 2004. Huawei promised to stop producing and sell-

ing Quidway routers and switches, and change its user manual, source code, and other elements at issue. But despite the settlement, Huawei continued to compete viciously for market dominance by offering low prices.

In 2011, Cisco began large-scale layoffs—its biggest at the time—and its stock price slumped.

In January 2013, then-European Union trade chief Karel De Gucht ordered an anti-dumping investigation into claims that Huawei and Chinese competitor ZTE undercut European firms by obtaining government subsidies and selling their cheap networking gear in Europe.

The Chinese media group Forward Business and Intelligence wrote an article about Huawei on Feb. 7, 2014, quoting CEO Ren as saying, "We have mobilized a full-scale war to smash Cisco around the globe."

By 2015, Cisco's share of China's router market by revenue had been nearly halved, compared to the beginning of 2014, while Huawei's had jumped by more than 50 percent, according to data provided by Sanford Bernstein.

The competition between Cisco and Huawei is a prime example of the Chinese regime's strategy of "overtaking on a bend in the road," meaning, surpassing developed countries by taking shortcuts and using unconventional tactics.

Learning, Copying

In the evolution of Huawei, IBM also played a vital role.

Numerous Chinese media reports—and public statements from Huawei executives—have documented how IBM taught Huawei about Western management techniques.

In a 2012 interview with The Wall Street Journal, Huawei's then-senior vice president for the United States, Charles Ding, said his company had been working closely with IBM since 1997. Without IBM, Ding said, "We could not have had the Huawei of today." Ding is now president of Huawei's Brussels office.

A June 2009 article by Chinese business magazine Changjiang detailed the collaboration.

Beginning in August 1998, Huawei and IBM initiated an "IT Strategy and Protocol," in which IBM would provide eight of its management technologies to Huawei, including systems to optimize product development, supply chains, coding, and more.

Chinese media have touted Huawei and IBM's partnership as a "case study for success."

In an article published in Z.H. Island, a Chinese magazine for entrepreneurs, a Renmin University professor explained how it happened: Huawei paid 56 million yuan (\$8.24 million) to hire IBM as a consultant. The U.S. company sent teams of consultants to Huawei, who shared their management experience with Huawei's project managers. IBM also provided full coaching for Huawei through an in-house consultant team for each important project at Huawei.

With IBM's assistance, Huawei greatly reduced product development costs and also the time needed to bring a product to market, according to the article.



A fairgoer speaks on his cellphone in front of a giant IBM logo at the CeBit trade fair in Hanover, Germany, on March 5, 2008.

Huawei Senior VP: Acknowledge and Study US Manufacturing Power

NICOLE HAO

On April 20, 2018, Chen Lifang, corporate senior vice president and president of public affairs at Huawei, gave a speech at a seminar for new employees, in which she encouraged staffers to learn from U.S. companies—to poach technology from them.

Rather than adopting an "anti-American" attitude, "we must acknowledge the power of the United States, see the gaps, study firmly from the United States' example," she said.

Chen was speaking as a trade dispute was escalating between China and the United States, and as Chinese state media was criticizing the U.S. administration's plan to slap tariffs on Chinese goods.

Instead of employing nationalistic sentiment to oppose the United States, Chen urged her audience "not to be arrogant."

"If the business does not have growth potential, does not have added value, nor key know-how, we can't catch up with the United States," she said.

Chen then called on China to develop domestic versions of a wide-ranging list of top U.S. firms, from tech firms such as Cisco and IBM, to pharmaceutical companies Pfizer and Eli Lilly, to defense manufacturers Lockheed Martin and Northrop Grumman. These companies, of course, are in sectors that Beijing has selected for high-priority, aggressive development in order to become a high-tech powerhouse.

She acknowledged huge gaps in different technical fields: "The capability to process data that DuPont has

“If the business does not have growth potential, does not have added value, nor key know-how, we can't catch up with the United States.”

Chen Lifang, corporate senior vice president, Huawei

accumulated is more than 25 times than our country's. In the field of turbines, the materials we have developed and the tests we have conducted are only 5 percent of GE's."

Even greater is the gap in developing microelectronics and artificial-intelligence-enhanced equipment with as much precision and stability as the United States'.

Curiously, Chen then cited the Wassenaar Arrangement, a pact signed by 42 nations in 1996 to restrict countries' exports of dual-use technologies, or those with both military and civilian uses.

China isn't among the member states.

But Chen talked about the need to import "special testing equipment that is related to national defense"—which countries would be restricted from importing into China. "[For those technologies,] we can only rely on a 'hidden battlefield' and have comrades take the risk," she said—implying that the Chinese should secretly smuggle such goods into the country, in violation of the pact.

With China's heavy reliance on foreign imports, including for chips and other important tech components, Chen said there was much to learn from advances in the U.S. manufacturing sector.

"Without the American manufacturing industry, our CNC machines [machines automated by computers], electronics industry, energy industry ... and some military products would not work or the performance would be greatly reduced," she said—apparently confirming that Chinese sectors had acquired the technology from U.S. firms.



FARIDULLAH AHMADZAI/AFP/GETTY IMAGES



Fighters with Afghanistan's Taliban on the outskirts of Gardez, the capital of Paktia Province, on July 18, 2017.

Huawei's Alleged Links to the Taliban

NICOLE HAO

W

hile there is much scrutiny about Huawei's role in communist China's efforts to extend its influence worldwide, it's less known that the telecommunications company may have provided assistance to Afghanistan's Taliban regime, which supported Osama bin Laden and his terrorist attacks against the United States.

The Population Research Institute reported in September 2001 that the Chinese regime and suppliers played a key role in Osama bin Laden's war on America, supporting the Taliban both in arms and techniques, the report said. Huawei allegedly made a major contribution to building telecommunications networks for the Taliban.

Since the early 1990s, the Taliban regime enthusiastically aided and abetted Al-Qaeda against the United States, including the 1993 bombing of the World Trade Center, the 1995 bombing in Saudi Arabia that killed five U.S. servicemen, U.S. embassy bombings in East Africa in 1998, and the 2000 attack on the USS Cole, off the coast of Yemen that killed 17 U.S. sailors.

The Taliban also maintained a close relationship with the Beijing regime for decades. In December 2000, the U.N. Security Council voted to place an embargo on arms sales to the Taliban, which forced the group to close bin Laden's terrorist training camps in Afghanistan. Beijing abstained from voting.

Months later, Huawei made a deal with the Taliban to build an extensive military communications system throughout Afghanistan.

Huawei India allegedly was supplying communication surveillance equipment to the Taliban in Afghanistan, Pakistan, and Iraq.

Intelligence Agencies Scrutinize Huawei Deals

India's intelligence agencies placed Huawei on a watch list for alleged business dealings with the Taliban, according to Indian media in December 2001. Before the Sept. 11, 2001, terror attacks, Huawei India was suspected of supporting terrorism, the reports said. The India Software Technology Parks of India investigated Huawei's activities in India, and questioned Jack Lu, then Huawei India's chief operating officer.

In addition, India's Cabinet Committee on Security (CCS) planned to deport 178 Chinese engineers working for the Huawei India research and development center in Bangalore, because CCS had discovered Huawei India allegedly was supplying communication surveillance equipment to the Taliban in Afghanistan, Pakistan, and Iraq.

The Chinese regime refutes the allegation and said the report is misleading, while the Indian government didn't comment.

Taliban Linked to Afghan Cellular Curfew

The Taliban also is believed to be controlling Afghanistan's mobile communication system, according to a report by The New York Times in October 2011. The connection between the local region and the rest of the world relies on mobile phones because there is no other communication system available, according to the report.

Since the Taliban set up the mobile communication system, it exercised its authority by turning off the network at 8 p.m. every evening and turning it back on each morning. This cellular

curfew occurs in more than half the provinces across Afghanistan.

It's widely known the Taliban has been on the United Nations' sanctions list since 1999. No communications company has since been allowed to sell to them.

Huawei reportedly supplied the telecommunications system.

Links to Iran and Syria

On Jan. 8, Reuters reported that Huawei used two companies to do business with Iran and Syria to avoid sanction-related bans: Hong Kong-based Skycom Tech Co. Ltd and Mauritius-registered Canicula Holdings Ltd. Skycom Tech is an equipment vendor that operates as part of a shell corporation called Canicula Holdings.

Huawei may be more closely linked to the two companies than previously known, according to corporate filings and other documents. Reuters discovered that the manager of Skycom's Iran branch might be Shi Yaohong, who happens to share the name of a known Huawei executive. Shi was appointed by Huawei as its Middle East region president in June 2012.

In addition to this, most signatories of Skycom bank accounts in Iran are ethnically Chinese and, at least three of them, had signing rights for both Skycom and Huawei bank accounts.

The latest revelation in the U.S. case against Huawei CFO Meng Wanzhou is that Skycom Tech was essentially operating as a Huawei subsidiary in Iran, but Meng allegedly lied about the relationship between Huawei and Skycom, according to prosecutors.

AFP/GETTY IMAGES



Shenyang J-15 fighter jets on China's aircraft carrier Liaoning during a drill at sea in April 2018.

Huawei's Expansion in Africa Comes Under Scrutiny

FRANK FANG

Chinese telecommunications giant Huawei's market dominance in Africa can be exemplified by remarks made in 2016 by Pang Jimin, then-president of the company's Global Government Affairs department.

"Of the several dozen available commercial 4G networks in Africa, more than 70 percent were built by Huawei," Pang said at an industry conference in Egypt, according to African online business site African Business Central.

Since making forays into the African market in 1999, Huawei has strategically monopolized telecom infrastructure.

For the previous-generation technology 3G, China's Ministry of Commerce claims that Huawei helped to build more than 50 networks in 36 countries, including Ghana, Kenya, Nigeria, Tanzania, Uganda, and Zambia.

And when it comes to rolling out the next-generation 5G technology, Huawei has cooperated with many local telecom providers in Africa for trial runs, including MTN Group, Africa's largest mobile operator; Vodacom, based in South Africa; and Safaricom, which is headquartered in Kenya.

Internet Infrastructure

Huawei also has been building up internet networks used by African governments—with security ramifications.

According to a December 2018 article by Kenya-based news site The East African, Huawei, along

Every night, data has been transferred from Huawei computer systems at the African Union headquarters to servers in Shanghai.

(Below) Gustavo Fuchs, Microsoft's director for Mobility Windows Phone for Middle East and Africa, introduces the Huawei 4Afrika, a Windows Phone 8 pre-loaded with select applications designed for Africa, in Lagos on Feb. 5, 2013.



PIUS UTOMI EKPE/AFP/GETTY IMAGES



with fellow Chinese tech company ZTE, have built "national fiber-optic communications networks and e-government networks in more than 30 countries."

That includes outfitting the headquarters of the African Union (AU). China fully funded and built the complex located in Ethiopia's capital, Addis Ababa.

In January 2018, French newspaper Le Monde revealed that since 2012, every night, data has been transferred from computer systems at the headquarters to servers in Shanghai. Additionally, hidden microphones were found inside the desks and walls of the building. Huawei was named in connection to the alleged spying. China denied Le Monde's claims.

According to an analysis by Canberra-based think tank Australian Strategic Policy Institute (ASPI), citing content from Huawei's own website and documents obtained from the African Union—including contracts for the union's IT infrastructure—the Chinese tech giant had provided

some of the headquarters building's equipment, including computing and storage devices. The think tank pointed out that while it is possible Huawei was not aware of the alleged data theft, the company's obliviousness would itself be cause for a "national security concern." Huawei has since denied ASPI's claims.

Joshua Meserve, senior policy analyst for Africa and the Middle East at the U.S. think tank Heritage Foundation, told a March 2018 congressional hearing on Africa relations that "the risk for African governments is significant."

Citing comments by former CIA head Michael Hayden, who said Huawei shared with Beijing "extensive knowledge of the foreign telecommunications systems it involved with," Meserve said that he believed Beijing "has already taken advantage of this African vulnerability."

State-Sponsored Strategy in Africa

Huawei's interest in doing business in Africa is

Huawei in Europe: Will Mao Zedong's Strategy Win the Market?

NICOLE HAO

Huawei is facing roadblock after roadblock in the European market.

Germany is considering stricter security requirements in an effort to exclude Huawei from building the country's next-generation 5G networks, while French telecommunications company Orange announced it would not hire Huawei system for 5G in France. The UK's BT Group also banned Huawei from 5G and said it would remove the company's equipment from its existing 3G and 4G operations. Meanwhile, Czech intelligence agencies warned of the security threats from Huawei, and Poland is considering a ban, too, after a Huawei employee was arrested and charged for espionage.

This wasn't something Huawei foresaw. The company's founder and CEO, Ren Zhengfei, had hoped to use former Chinese Communist Party leader Mao Zedong's strategy of "seizing the countryside and then using rural bases to encircle and capture cities."

As explained in a 2014 Chinese magazine article detailing Ren's life, the executive wanted Huawei to conquer the less developed markets first, then use that experience to penetrate the more competitive and developed markets.

The report noted that in 1997, Huawei made its

first foray into the overseas market with Russia. Russia's tech development was behind that of most of Europe and the United States, and the former communist country had maintained a good relationship with China.

After Russia, Huawei targeted African countries, Eastern European countries, the Middle East, Southeast Asia, and South American countries. The company's ultimate goal was to win business in Western Europe and the United States.

Forcing Its Way Into Markets

The company has used a slew of unorthodox tactics to win business in markets around the world.

On Oct. 14, 2014, Michael Makuei Lueth, minister of information for South Sudan, sent a formal letter to Barnaba Marial Benjamin, the country's minister of foreign affairs and international cooperation, alleging that Huawei hacked his official email account and sent a forged document to Li Ruogu, president of the Export-Import Bank of China, in order to help the company win a contract.

Given the forgery, "I suspect that Huawei has been hacking many government officials e-mail and falsifying and forging documents on behalf of the senior government officials," Lueth wrote in the letter.

In 2016, an anonymous Huawei sales manager

The executive wanted Huawei to conquer the less developed markets first, then use that experience to penetrate the more competitive and developed markets.

in Nigeria shared his experiences on social media.

He talked about an incident in 2012, when the equipment room of an unnamed European telecom network operator caught fire and Ericsson equipment valued at roughly \$20 million was burned to ashes. He and his colleagues saw a chance to enter the market.

"We decided to grab the chance and donate an equivalent system to them free of charge," the Huawei sales manager wrote. "Strategically, it will help us break through the market [if the operator agreed]." The manager did not disclose the European country where this occurred.

Lobbying, Hiring

Huawei also knew how to recruit the right people to the company.

In 2011, just after European Union Ambassador to China Serge Abou retired from his position, Huawei approached Abou to be its senior adviser. Abou joined Huawei in 2013 after the two years he was required to wait before taking on the consulting job—but the potential conflict of interest raised eyebrows.

In an October 2013 report, the South China Morning Post (SCMP) quoted Olivier Hoedeman of Corporate Europe Observatory, a Brussels-based nonprofit that researches the effects of corporate lobbying, as saying: "Even though Abou cannot directly lobby [for Huawei], he can help [the company] to gain access by his insider knowledge. There is a big risk of conflict of interest, because he knows which doors to knock on and how to open them."

Aside from Abou, Huawei also hired seven lobbyists "that are accredited to the European Parliament, and has hired five consultancy firms to lobby for them with the European Union," Hoedeman told SCMP.

According to the EU Transparency Register, a voluntary registry of lobbyists, Huawei spent about 3 million euros (\$3.42 million) each year lobbying the EU.



TONY KARUMBA/AFP/GETTY IMAGES

driven by its founder and CEO Ren Zhengfei—a former Chinese army engineer who headed the General Staff Department’s Information Engineering Academy—and to a great extent the ideology of the Chinese Communist Party (CCP). According to a biography published by China’s Huazhong University of Science and Technology Press in 2010, Ren often read the writings of former Chinese Communist Party leader Mao Zedong and used Mao’s thoughts to set up Huawei’s business strategy. For example, Ren adopted a well-known Maoist strategy—seizing power in the countryside and then using rural bases to encircle and capture cities, a method honed during China’s civil war—to expand Huawei’s business both domestically and internationally. Beginning in 1992—at a time when the Chinese telecom market was dominated by foreign firms such as Alcatel, Lucent, and Nortel—Huawei began to aggressively market its digital telephone switches in China’s rural areas, before expanding

to the rest of China, according to the book. Using the same Maoist strategy, Huawei first expanded into less-developed regions of the world, such as Africa, Southeast Asia, and western Asia, before expanding into major European and American markets. The Chinese tech giant is also one of many Chinese companies that followed Beijing’s call for overseas expansion—the “Go Out” strategy promulgated by former CCP leader Jiang Zemin (who ruled throughout the 1990s to early 2000s). According to China’s state-run media, Jiang first suggested the strategy in July 1996, after visiting six African countries: Egypt, Ethiopia, Kenya, Mali, Namibia, and Zimbabwe. The concept of Go Out was mentioned again in December 1997, when Jiang said during a CCP work meeting, “We should aggressively lead and organize competent companies to go out, to invest and set up factories at other countries, and utilize their markets and resources.”

A girl uses her smartphone in the Riruta suburb in Nairobi on Nov. 8, 2018.

In May 1998, at another CCP work meeting, Jiang identified Africa, along with the Middle East, Central Asia, and Latin America, as regions for aggressive investment, as part of his Go Out strategy. The concept eventually became an official element of China’s foreign policy in November 2002, when it was included in a political report during the 16th National Congress, a once-every-five-years conclave when the Party’s leadership transitions. During this time, Huawei took up the mantle, first setting up a subsidiary in Nigeria in 1999.

Training Initiative

The company also seeks to extend soft power through its corporate social responsibility program called Seeds for the Future, established in 2008 for the goal of developing local IT talents and promoting greater interest in the telecommunications sector. Usually, students studying in STEM-related (science, technology, engineering, and mathematics) fields are selected. Participants in the program receive Mandarin-language training at top universities in Beijing, according to Huawei’s website, as well as technical training at the company’s headquarters in the southern Chinese city of Shenzhen. Many universities around the world have noted that Seeds for the Future is an “all-expense paid” program. The program is available in many countries around the world, including the United States, and more than 20 countries in Africa, including Cameroon, Ghana, Kenya, Senegal, and South Africa.

According to Huawei’s website, more than 30,000 students from more than 350 universities, representing 108 countries and regions, had participated in its program as of 2017. But some experts believe these are more than just an education program. Huawei’s partnerships with top UK universities, including the Seeds for the Future program, have been called into question. Anthony Glees, a professor of politics at the University of Buckingham and a national security expert, called the relationships “deeply disturbing” and “absolutely classic Communist subversion tactics,” in a December 2018 article by The Daily Telegraph. Glees explained that Huawei’s programs have a “military, political, and industrial component to it that people have not understood,” due to the company’s close ties with Beijing, and Ren’s ties to the Chinese military. In a policy brief issued in July 2016, researchers at the School of Advanced International Studies at Johns Hopkins University questioned the effectiveness of Huawei’s training programs. “Are the training programs that Huawei labels as CSR programs truly focused on social and environmental well-being, or are they prudent cost saving, profitable business, or human resource development programs?” the policy brief asked.

Cloud Solutions

Huawei’s forays into cloud data storage have also prompted espionage concerns. In November last year, the company unveiled its new cloud computing station in South Africa. On its website, the company touted itself as the first cloud service provider to operate a local data center in Africa. Huawei also has inked deals with multiple information and technology firms around the world to provide cloud services to companies in Africa, including the South Africa-based Datacentrix, India-based Tech Mahindra, and Germany-based T-Systems. Security concerns surrounding Huawei’s cloud computing products were raised way back in September 2013, when the Virginia-based analyst firm Defense Group Inc. published a report at the request of the U.S.–China Economic and Security Review Commission. The report, titled “Red Cloud Rising: Cloud Computing in China,” warned of cloud computing services set up by Chinese “national champion” corporations, such as Huawei and ZTE, noting that their efforts to sell their services outside of China could indirectly result in a “significant amount of U.S. corporate data ending up on servers under Chinese control.”



ERIC PIERMONT/AFP/GETTY IMAGES

In October 2011, John Suffolk, former chief information officer for the UK government, joined Huawei as its global head of cybersecurity after getting approval—as per UK regulations—from then-Prime Minister David Cameron. Suffolk had worked in the UK government for seven years. He helped Huawei develop its cybersecurity assurance system. Today, Huawei has 18 research and development

centers in Europe, led by the Huawei European Research Institute based in Belgium. The company has academic partnerships with more than 100 universities in Europe, investing 75 million euros (\$85.29 million) in them, according to the company’s website. But they have recently been called into question amid growing scrutiny of the Chinese tech giant. In total, Huawei has signed more than 210 cooperation agreements with European companies.

(Above) Huawei CEO Richard Yu presents the new P20 smartphone at the Grand Palais in Paris on March 27, 2018.

Suspected Interference in Arts Scene

Huawei recently invested in the French arts and culture scene—with curious timing. On July 9, 2018, Paris Opera, France’s premier opera and ballet company, announced that Huawei would invest 900,000 euros (\$1.025 million) over three years to set up a global “digital academy” for the performing arts company, including online courses, archival videos, and more, according to a report by radio station Europe 1. Chinese state media also praised the partnership in a media report, noting that the effort is supported by China’s Ministry of Culture. Around the same time, the New York-based company Shen Yun Performing Arts was in negotiations with Paris Opera to rent a venue, the Palais Garnier, for several performances, as part of its 2019 world tour. Shen Yun’s presenters in France told The Epoch Times that the discussion about booking the venue suddenly came to a standstill after Paris Opera made the deal with Huawei. After talks with Paris Opera stalled, Shen Yun presenters ultimately brought the performance to another venue in Paris, the Palais des Congrès. The company just completed a successful run at the theater in mid-January and will perform there again in May. According to Shen Yun’s website, the company’s mission is to revive 5,000 years of Chinese civilization. Since its founding in 2006, the Beijing government has consistently tried to stymie the company’s presence in the West, apparently due to the company’s portrayal of topics considered “sensitive” by the regime, such as the Chinese Communist Party’s persecution of the spiritual meditation practice Falun Gong. The Epoch Times, as well as European media outlets, have documented that Chinese consulates and their operatives around the world have for years pressured theaters not to lease their spaces to Shen Yun, or have sought to coerce Western government officials to not attend the performances or voice public support for the company.

NICOLAS ASFOURI/AFP/GETTY IMAGES



A screen shows visitors being filmed by AI security cameras with facial recognition technology at the 14th China International Exhibition on Public Safety and Security at the China International Exhibition Center in Beijing on Oct. 24, 2018.

COMMENTARY

Ban Huawei to Escape China’s Digital Dictatorial Embrace

RICK FISHER

Free nations of the world have a choice: They can ban Chinese telecommunications giants such as Huawei and ZTE from building or dominating their next-generation “5G” digital communication networks, or they can let them in and watch their sovereignty and freedoms fade into the Chinese Communist Party’s (CCP) global digital dictatorship.

China’s digital dictatorship technology is on constant display and is for sale at electronics and military exhibitions around the world. The FBI notes that ZTE alone is building 150 “smart cities” in China, and the list could grow to 500.

Smart cities allow Chinese police and intelligence services to correlate data from millions of video surveillance cameras with vast databases containing intimate internet and phone activity, biometric, medical, and DNA data to assemble expansive profiles of the lives of Chinese citizens. Authorities then can construct individual “social credit” scores that rate loyalty to the CCP, which will then be used to determine an individual’s success in life, from education to employment, domicile, and permission to travel abroad.

Huawei already is at the forefront of building smart cities into stronger weapons to enable Chinese police and intelligence organs to better suppress the restive Muslim region of Xinjiang. Last year, Huawei revealed an “intelligent security industry” innovation laboratory in Urumqi, and a May 2018 Huawei press release stated, “Together with the Public Security Bureau, Huawei will unlock a new era of smart policing and help build a safer, smarter society.”

Chinese weapons-sales companies such as the China Electronics Technology Corporation (CETC) likely will market integrated smart cities at the world’s largest ground-forces military exhibition, Abu Dhabi’s IDEX exhibition, which starts Feb. 17.

While Huawei has had success in selling its integrated smart-city electronic infrastructure to the German city of Duisburg, the company also claims it has sold to 120 other cities its “Rhine Cloud,” a “Public Services Cloud Platform” that allows city maintenance and governance functions to be combined in a single database.

However, Huawei and ZTE communication networks in foreign countries also are deployed weapons that assist China’s foreign espionage, surveillance, and warfare objectives. Bill Gertz has reported that former Cen-

tral Intelligence Agency and National Security Agency Director Michael Hayden told Australian newspapers that Huawei has “shared with the Chinese state intimate and extensive knowledge of the foreign telecommunications systems it is involved with.”

In late 2017, African officials in the new Chinese-designed, built, and paid-for African Union headquarters building in Addis Ababa, Ethiopia, discovered that their Huawei and ZTE-built internet system was downloading contents daily to a server in Shanghai.

Following the Jan. 11 arrest in Poland of Huawei sales official and likely trained intelligence operative Wang Weijing, Poland’s Internal Affairs Minister Joachim Brudziński on Jan. 13 called for a European Union and NATO joint policy on whether to exclude Huawei from their markets.

The latest U.S. Defense Authorization Act, signed by President Donald Trump in August 2018, bans the U.S. government from using Huawei and ZTE equipment. Now, Australia, New Zealand, Japan, Great Britain, Germany, Italy, India, and Canada have either implemented, or are considering, similar bans.

The Dec. 1, 2018, arrest, at Washington’s request, of Meng Wanzhou—company heir-apparent and daughter of Huawei founder Ren Zhengfei—related to the company’s alleged violations of U.S. technology embargos on Iran, sparked a diplomatic furor. China almost immediately arrested two Canadians in retaliation and retried another Canadian already in a Chinese jail, before upgrading his punishment to a death sentence.

But it’s Canada’s review of whether to ban Huawei’s new 5G technology from its markets that has prompted special Chinese outrage. On Jan. 17, Chinese Ambassador to Canada Lu Shaye publicly threatened “repercussions” if Canada bans Huawei 5G technology.

The Chinese regime is now fighting for Huawei’s right to upgrade global computer connectivity networks to 5G from 4G because the new technology represents a leap from a soda straw to a firehose in digital power. Very soon,

China wants to lock you up in its digital dictatorship before your government wakes up and it’s too late.

5G networks will be enabling next-generation capabilities in artificial intelligence and the “internet of things,” such as the future ability of your computer-controlled house to operate your computer-driven car.

For militaries around the world, artificial intelligence, 5G technology, and advances in quantum computing could enable the first secure unmanned aircraft, ships, and robot soldiers capable of the myriad decisions necessary for autonomous combat. China’s understanding of these future trends prompted its People’s Liberation Army (PLA) in late 2015 to form the Strategic Support Force (SSF), the world’s first distinct military service charged with exploiting advances such as artificial intelligence, 5G, quantum computing, and space warfare, so as to achieve next-generation levels of cyber intelligence, surveillance, and warfare.

Crucial to the success of the PLA-SSF is access to, or even control of, new 5G networks built by companies such as Huawei and ZTE. The PLA-SSF could leap from running minor cyber influence operations (such as ballooning social-media traffic to favor opposition candidates in Taiwan’s recent elections), to creating real-time artificial newsfeeds to shape the behavior of governments during crises.

The PLA-SSF also could gather intimate databases on the citizenry of target countries so as to assign individual and national “social credit” scores, issuing positive and negative incentives, in the effort to build “compliant” populations around the world. Another crucial future SSF mission would be to take control of the unmanned military forces of China’s enemies.

That’s the real reason China is meting out death sentences to Canadians and screaming to defend its “right” to build 5G networks around the world. China wants to lock you up in its digital dictatorship before your government wakes up to it.

Rick Fisher is a senior fellow with the International Assessment and Strategy Center and author of “China’s Military Modernization: Building for Regional and Global Reach.”



The offices of Huawei in Warsaw, Poland, on Jan. 11, 2019.

PHOTO BY: REUTERS/KACPER PEMPEL



Chinese leader Xi Jinping (C) is shown around the offices of Huawei by its President Ren Zhengfei (2nd L) in London during Xi's state visit on Oct. 21, 2015.

COMMENTARY

Huawei Reveals China's Foreign-Policy Agenda

‘Crown jewel’ telecom firm identified as a tool of anti-American apparatus

JAMES GORRIE

The arrest of Huawei executive Meng Wanzhou by Canadian authorities at the behest of the U.S. government tells us that the old ways of doing business are over for China. Their days of feeding off American technology are numbered, and President Donald Trump isn't pulling any punches. It's about time.

Meng, Huawei's chief financial officer and the daughter of the company's founder, is charged with circumventing U.S. sanctions against Iran by trading through subsidiary companies. It confirms what some American security officials have suspected for years: that Chinese corporations are the ultimate front for implementing the foreign-policy agenda of the Chinese Communist Party (CCP).

More Than a Great Company

The CCP leadership's goal is to replace the United States as the predominant power in the world. But to confront and ultimately overtake America's global position, China must do so on multiple fronts—financially, technologically, and militarily. Dominating the communications and networking verticals is a very effective way to achieve results across all those channels. That's what makes the Huawei situation so compelling: It meets all of those criteria—and more.

Huawei isn't just a great technology company; it's a phenomenally successful one. In fact, it's considered by some to be the “crown jewel” of China's advanced tech industry. A global leader in electronic equipment and wireless communication components, Huawei rivals Apple in smartphone sales and is a global leader in the development and transition to 5G networking.

By going around U.S. sanctions, Huawei enabled Iran to receive critical technology transfers, as well as much-needed hundreds of millions of dollars from their transactions with the rogue Islamic regime.

China's Anti-US Foreign Policy Agenda

Quite unlike the U.S. corporate experience, the most important Chinese business and technology companies are state-owned. Their activities are conducted in coordination with the foreign policy agenda of the CCP. That context puts Huawei's actions in a much more nefarious light. Its violations of U.S. sanctions against Iran can be viewed as a direct challenge to America's foreign policy with Iran.

But Huawei's sanctions-violations charges are just the beginning. According to U.S. leaders, Huawei is actively involved in the theft of technology secrets from American companies and has been doing so for years. It's been watched closely by U.S. authorities since at least 2016 and has recently been charged with technology theft from U.S. companies such as T-Mobile and others.

Some regard the technology giant's true purpose as a data- and information-gathering apparatus for the Chinese government. As Rep. Jim Banks (R-Ind.) points out in an article appearing in The Washington Post: “Huawei is a state-directed entity actively undermining America's national security.”

Huawei certainly isn't acting alone. Stealing U.S. technology is a policy decision from the very top of China's regime; Huawei just leads the way. Chinese telecom supplier ZTE was also found to be involved in data theft, and in October 2018, Brussels authorities arrested a Chinese Ministry of State Security official for attempted theft of secret aviation data from U.S. defense contractors. China's theft of U.S. technology and products is immensely damaging to America's status as the dominant global economic and technological power. Theft from China alone reaches up to \$600 billion per year—almost twice the U.S. annual trade deficit with China

Stakes Couldn't Be Higher

Furthermore, a recent report identified China as the main perpetrator in the theft of U.S. data and intellectual property (IP). China's data-theft agenda is especially focused on biotechnology and quantum communications technology. It's those sectors that will play a critical role in determining which nation will shape and dominate the next several decades of technology.

Worse, China isn't merely a competitor on the international stage, but rather, a political and economic adversary out to fundamentally change the American-international order.

To that end, the Chinese foreign-policy agenda is one of actively waging war against all forms of American power. Huawei is at the forefront of those efforts. “The massive theft of American IP ... threatens our nation's security, as well as vitality,” said former Director of National Intelligence Adm. Dennis Blair.

Sea Change in America Policy

That's why the arrest of Meng and the U.S. government's banning of all Huawei telecom and network equipment is so powerful. It demonstrates a sea change in several areas of U.S. policy toward China. It shows just how serious the U.S. government is in pushing back against China's foreign-policy agenda of data and product theft. It also demonstrates that America won't turn a blind eye toward any nation—not even China—when it willfully assists a declared enemy of America.

What's more, going forward, the Huawei affair puts added weight behind the president's trade policies and his negotiating position. The arrest certainly caught China's leaders off-guard and has left them wondering what Trump will do next. They are bewildered and confused, which should be an advantage to the United States.

And perhaps just as importantly, the actions signal a major shift in U.S.-Chinese relations. For China and the rest of the world, the arrest of the Huawei CFO and banning the company from doing business with the United States have shattered their globalist assumptions that enabled China's rapid rise to the world's top economic and technological levels in the first place.

James Gorrie is a writer based in Texas. He is the author of “The China Crisis.”

THE EPOCH TIMES

TRUTH *and* TRADITION

READ WHAT
OTHERS
WON'T REPORT

The Epoch Times, a media committed to truthful
and responsible journalism, is a rare bastion of
hope and stability in these testing times.

SUBSCRIBE TODAY

02 8988 5600