WEEK 52, 2020

THE EPOCH TIMES

CHINA INSIDER

ALEX CIMBAL/SHUTTERSTOCK

IBM China's office in Beijing on July 18, 2015.

CCP CELLS

EMBEDDED IN MAJOR US FIRMS, LEAKED DATABASE REVEALS

See Page 6

STR/AFP VIA GETTY IMAGES

Workers produce face masks at a factory in Nanchang, China, on April 8, 2020.

CHINA PHOTOS/GETTY IMAGES

A woman feeds a baby who suffers from kidney stones after drinking tainted milk powder at the Chengdu Children's Hospital in Chengdu of Sichuan Province, China, on Sept. 22, 2008.

OPINION

The 'Made in China' Quality Crisis

WANG HE

Amid the COVID-19 pandemic, Beijing has used the crisis as a business opportunity to export Chinese-made personal protective equipment (PPE) and medical supplies. However, a large number of Chinese-made COVID-19 testing kits and masks are of inferior quality. And this has once again tarnished China's international image.

The Chinese Communist Party (CCP) has denied responsibility for spreading the coronavirus and has even accused other countries of being the source. At the same time, it has engaged in "mask diplomacy" and "anti-epidemic diplomacy."

Defective Testing Kits

On Aug. 25, the Swedish Public Health Agency stated that about 3,700 people in Sweden were given false positive results due to defective test kits from China. And these kits were also widely distributed to other countries.

On April 27, White House trade adviser Peter Navarro accused China of "sending low-quality and even counterfeit coronavirus antibody testing kits to the United States."

On the same day, the Indian Council of Medical Research asked the state governments to return the rapid antibody test kits "as the results were not satisfactory," according to Indian media reports. The kits were from two Chinese companies, Wondfo Biotech and Livzon Diagnostic.

> The regime's propaganda slogans such as 'building the Party for the public, governing for the people,' leading the Chinese people to create 'economic miracles,' 'building a moderately prosperous society in an all-round way,' and 'common prosperity' are all just nonsense.

Defective Masks

On March 28, the Dutch Ministry of Health issued a statement that they received 1.3 million masks, marked "KN95," from a Chinese manufacturer. However, after two tests, the ministry found problems with the masks as "they did not close over the face properly, or had defective filters," the Dutch public television channel NOS reported. Part of the shipment was distributed to various hospitals. The authorities immediately recalled nearly half the shipment of masks and said future shipments would be subjected to extra testing.

Mask quality has had an even greater impact in the United States. On April 3, due to a severe shortage of N95 masks, the Food and Drug Administration (FDA) issued a new emergency use authorization (EUA) for Non-NIOSH-Approved Disposable Filtering Facepiece Respirators (FFRs) manufactured in China. Data shows that from March 1 to May 5, China provided more than 6.6 billion masks to the United States. For safety reasons, the FDA conducted a second review of these Chinese-made masks. Test results released on May 7 found that about 60 percent of 67 different types of imported N95 masks did not meet quality standards. On the same day, the FDA stated that it had withdrawn the permits of more than 60 Chinese manufacturers to export N95 masks to the United States, leaving only 14 authorized companies.

In response to the international pushback, Chinese officials announced on March 31 that "test reagents, medical facial masks, medical protective suits, ventilators and infrared thermometers for export must be certified by state medical products administration departments and conform with the quality requirements of the importing country or region."

However, these official measures cannot completely solve the "made in China" quality crisis because the quality crisis is the result of China's corrupt business environment. If this environment is not rectified, then the quality crisis will emerge at any time. The COVID-19 pandemic was merely one catalyst.

The Hill published a commentary by U.S. Congressman Michael McCaul (R-Texas) who wrote: "Beijing has engaged in "mask diplomacy"—sending medical supplies around the world in an attempt to cast themselves as a worthy partner in the fight against coronavirus and in the hope the world will forget the CCP's failures are to blame for our global suffering. Of course, their subsequent propaganda conveniently failed to mention just how many of these supplies were defective or how they reportedly hoarded their stockpile while they lied about the spread of the virus within their own borders."

Melt-Blown Cloth Production

Melt-blown cloth is the non-woven fabric used as the core raw material of masks. This year, the price of melt-blown cloth per ton has risen from the original 18,000 yuan (about $2,754) to more than 700,000 yuan (about $107,000), and the supply could not meet demands. According to Chinese media reports, melt-blown cloth related enterprises in China increased by 1,250 between Feb. 1 and April 13 this year; compared with the same period in 2019, the growth rate was over 4,500 percent. The substandard product quality in these new melt-blown cloth production shops prompted local authorities to shut down all production "for rectification."

Substandard Manufacturing Environment

The pandemic led to a shortage of masks worldwide. It's rumored that toilet paper was used to keep up with the demand for masks when COVID-19 began to spread in Asia.

Hong Kong media Ming Pao reported that the present management of mask factories in China is chaotic. Many dealers promoted their services through WeChat or word-of-mouth marketing and handled the certification process of medical supplies. Factory qualification certificates could easily be obtained, and some services charged 30,000 yuan (about $4,500) to get European and American certifications. Sixty percent of the factories don't have any aseptic workshops and the production areas are dirty and unhygienic. Most of the time, mask machines are immediately put into production without being properly sanitized after they arrive in the workshop. Some workers don't use masks or gloves.

Pengchang town in Xiantao city, Hubei Province is known as the capital of non-woven fabrics. The town's non-woven fabric production accounts for 60 percent of the country's total production and a quarter of the global market share. However, local authorities closed 273 illegal small workshops in the town and seized more than 46 million substandard masks, according to Chinese media reports.

Unethical Business Practices

Judging from China's current economic state and its product quality crisis, the Communist regime has fostered a corrupt environment.

> The Chinese people have been the biggest victims of the 'made in China' quality crisis. After all, exports are limited. Moreover, with the international market, especially the regulated markets in Europe, the United States, and Japan, the CCP has to be more careful as the quality control is much stricter than in the domestic market. Therefore, there is a peculiar phenomenon in the domestic market, namely, export goods sell better when they are imported back to China.

In fact, the CCP is aware that low quality has become a stumbling block for products made in China. It has also rolled out policies in an effort to launch a "quality revolution." In the years 1992, 1999, and 2007, the CCP held three national "quality work" conferences. The State Council of the CCP promulgated the "Outline on Revitalizing Quality 1996-2010" and "Quality Development Outline 2011-2020." After Xi Jinping took office, three "quality work" conferences were held in 2104, 2017 and 2019. On Sept. 5, 2017, the State Council issued the report, "Guidelines and Opinions on Carrying out Quality Improvement Actions."

However, these documents and policies did not make a difference as quality standards have not improved over the years. In 2007, Mattel, an American toy manufacturing company, announced a massive recall of Chinese-made products due to excessive levels of lead paint. In the following year, Chinese milk powder maker Sanlu Group announced a recall of some of its products because they were contaminated with the poisonous chemical compound melamine.

Japan and South Korea encountered similar quality crises during their growth in the 1970s and 1980s. At that time, Japanese and Korean low-cost cars entered the U.S. market but the quality was considered poor. However, Japan and South Korea turned things around. Japanese auto companies focused their resources in improving the quality of their products. Hyundai established a quality control team in 1999, learning from the mistakes of Japanese carmakers and continuously increasing R&D investment. As a result, Japanese and Korean cars have gained worldwide recognition in the past few years.

CCP Is Hopeless

It is impossible for the CCP to make real improvements, similar to what Japan and South Korea accomplished in creating quality cars. When the CCP is faced with a major crisis, it refuses to deal with the issue directly. It pretends to be the victim or shifts the blame, claiming that the other party is "demonizing China" or "being political." The CCP looks for a scapegoat and deals with the "perpetrators." At the same time, the regime controls public opinion and cracks down on whistleblowers and dissidents. Under a totalitarian system, it has created a vicious cycle in dealing with crises.

In this light, it's not so difficult to understand the fate of Zhao Lianhai, the father of a child who developed kidney stones in 2008 from drinking contaminated milk formula. Zhao is the founder of "Kidney Stone Babies," a group that helps parents seek legal redress for their children's illnesses due to melamine-tainted milk. In 2010, he was sentenced to two and a half years in prison for the crime of "disturbing social order" after he took part in organizing a gathering of parents and accepted media interviews.

The Chinese people have been the biggest victims of the "made in China" quality crisis. After all, exports are limited. Moreover, with the international market, especially the regulated markets in Europe, the United States, and Japan, the CCP has to be more careful as the quality control is much stricter than in the domestic market. Therefore, there is a peculiar phenomenon in the domestic market, namely, export goods sell better when they are imported back to China.

This practice fundamentally violates the principles of modern quality management. But the CCP has done this for many years. In 2007, the year when the first "made in China" quality crisis occurred, Chinese officials provided two sets of data on product qualification rates. One was that the domestic food safety qualification rate was 85.1 percent, and the other is that over the past few years, food exported from China to more than 200 countries and regions had a qualification rate of over 99 percent. The gap was about 15 percent.

These two statistics make it clear that the CCP doesn't care about its own people. The regime's propaganda slogans such as "building the Party for the public, governing for the people," leading the Chinese people to create "economic miracles," "building a moderately prosperous society in an all-round way," and "common prosperity" are all just nonsense.

If you still don't know what the CCP is, take a look at how it handled COVID-19 when it first broke out in Wuhan city last year. Its botched handling of the outbreak caused a global pandemic. And substandard PPE products from China did not make much of a difference in saving lives.

Wang He holds master's degrees in law and history, and has studied the international communist movement. He was a university lecturer and an executive of a large private firm in China. Wang now lives in North America and has published commentaries on China's current affairs and politics since 2017.

Views expressed in this article are the opinions of the author and do not necessarily reflect the views of The Epoch Times.

DADO RUVIC/ILLUSTRATION/REUTERS

A 3D printed logo of video conferencing app Zoom. Unsealed court documents show that Chinese security authorities made numerous requests to the company for data on its users.

COURTESY OF FBI

Jin Xinjiang, a former executive at video-conferencing app Zoom, in a mugshot distributed by the FBI. He was recently charged for his role in censoring U.S.-based users on the platform.

CENSORSHIP

How Zoom Complied With Chinese Authorities to Censor US Users

CATHY HE

A Zoom executive worked with Chinese authorities to provide data on users located outside of China and ensure the U.S. video-call giant retained market access in the country, according to recently unsealed court documents filed by U.S. federal prosecutors.

The documents detailed internal communications between Zoom employees, which showed that Chinese security authorities made numerous requests to the company for data on users and meetings that discussed political and religious topics Beijing deemed unacceptable.

Zoom complied with most of these requests, at times involving users outside of China.

The revelations highlight how users outside of China's borders are increasingly being caught in the crosshairs as the Chinese Communist Party (CCP) steps up its demands on companies such as Zoom to surveil and censor users both at home and abroad. Zoom is a San Jose, California-based company, whose software is developed in China.

The claims arose in a prosecution announced on Dec. 18 against Jin Xinjiang, also known as Julien Jin, a China-based Zoom executive. Jin was charged over his role in disrupting a series of meetings this year commemorating the 31st anniversary of the Tiananmen Square Massacre—an event deemed taboo by the Chinese Communist Party (CCP).

> The regime requires all communications companies operating in China to monitor and censor speech deemed unacceptable to the CCP.

Prosecutors allege Jin, who worked as Zoom's main liaison with Chinese law enforcement and intelligence officials, was directed by the CCP to shut down at least four Zoom meetings about the Tiananmen Square Massacre, most of which were hosted by Chinese dissidents based in the United States.

At the time, the company attracted widespread criticism after it suspended the accounts of a group of U.S.- and Hong Kong-based Chinese activists who hosted meetings commemorating the anniversary. The company said at the time that it took action because participating in such events was considered "illegal in China."

In an updated statement issued on Dec. 18 after the federal case was made public, Zoom said it "fell short" by taking actions against users outside of mainland China, including suspending the accounts and shutting down meetings. It added that it would no longer allow requests from the Chinese regime to affect anyone outside the mainland.

Jin also took part in a scheme to infiltrate several meetings in May and June hosted by U.S.-based Chinese activists to remember the massacre, according to prosecutors. He and co-conspirators allegedly fabricated evidence to make it appear as if the meetings or participants engaged in conduct that breached Zoom's terms of service, such as by inciting violence, supporting terrorist organizations, or distributing child pornography.

They then used this concocted evidence to convince U.S.-based Zoom executives to cancel the meetings and suspend the accounts of the U.S. activists, prosecutors alleged.

Jin's case doesn't appear isolated. The court complaint details a series of other incidents from June 2019, when the company complied with data or censorship requests from Chinese authorities—notably in relation to accounts outside of China. A constant theme underlying these requests was that Zoom would be shut out of the Chinese market if they didn't cooperate.

Zoom, in another statement on Dec. 18, said the company has cooperated with federal investigators and has launched an internal investigation. The company said that Jin shared a "limited amount of individual user data with Chinese authorities," as well as data on less than 10 users based outside of China.

Jin was fired, the company said, while other employees have been placed on administrative leave pending the internal investigation.

Working With the Party

Jin, 39, held the position of "security technical leader" at Zoom's offices in eastern China's Zhejiang Province. He led the company's efforts to comply with the CCP's censorship directives, prosecutors said.

The regime requires all communications companies operating in China to monitor and censor speech deemed unacceptable to the CCP, including on topics critical of the regime and about religious groups persecuted by the Party. It also requires foreign companies to store data for Chinese users on servers located inside China. A company that fails to comply will risk being blocked from the Chinese market.

As Zoom's main liaison with Chinese authorities, Jin received directives from several bodies within China's censorship and security apparatus, including the Cyberspace Administration of China (CAC), the regime's internet regulator; the Ministry of State Security (MSS), China's top intelligence agency; and Ministry of Public Security (MPS), the regime's law enforcement body, according to the court complaint.

Jin was responsible for proactively monitoring meetings on Zoom for discussions deemed "illegal" by the regime. For instance, in August 2019, Jin singled out a Christian group hosting meetings on Zoom's U.S. servers, an FBI agent said in the complaint. Jin told a U.S.-based colleague that the group was a "Chinese cult" and its account should be blocked due to its discussion of Christian content.

In response, the colleague directed Jin to put the account on "quarantine" status, an action that limits its features, in the hopes that this would force the user to drop the platform.

In early September 2019, the Chinese regime blocked Zoom from operating in the country. To resume operations, Zoom was required to submit "rectification" plans to Chinese authorities, the complaint stated.

In the plan, Zoom agreed to proactively monitor communications for discussion of topics, including political views, deemed unacceptable to the CCP, migrate the storage of about 1 million China-based users' data to China from the United States, and provide Chinese security authorities special access to Zoom's systems, according to the FBI agent.

> Jin's case doesn't appear isolated. The court complaint details a series of other incidents from June 2019, when the company complied with data or censorship requests from Chinese authorities—notably in relation to accounts outside of China. A constant theme underlying these requests was that Zoom would be shut out of the Chinese market if they didn't cooperate.

Zoom's China service was eventually reinstated in November 2019.

Growing CCP Controls

After Zoom's popularity exploded amid the COVID-19 pandemic, Chinese authorities imposed tighter controls on the company, the complaint said. They demanded Zoom develop the capability to shut down "illegal" meetings or accounts within one minute of receiving a direction from authorities—known as the "one-minute processing requirement."

This requirement extended to discussions by overseas users. In an April 29 exchange with the U.S. colleague mentioned in the complaint, Jin explained that the "requirement is that [the Zoom employee] must have the authority to directly handle it, and it must be handled within one minute ... otherwise will be [rated] as security non-compliant."

Censorship and other demands by Chinese security agencies were also to be kept secret, Jin explained to his U.S. colleague, according to the court document.

While Jin didn't have access to data on Zoom's U.S. servers, the FBI agent said that the U.S.-based colleague sought to allow Jin access to such data for compliance with the Chinese regime's instructions. In one discussion in April, the U.S. employee suggested that another U.S.-based worker could provide Jin access to a "remote" machine in the United States hooked up to the U.S. servers and systems.

Jin replied that the matter needed to be handled confidentially outside of usual company procedures, and that he wouldn't be able to document his actions in a report.

Holding Companies Accountable

Zhou Fengsuo, founder of the U.S.-based advocacy group Humanitarian China, hosted the May 31 event, which had some 4,000 participants tune in from around the world. He recalled that many scheduled speakers from China sent pre-recorded messages that day due to pressure from authorities. Many were detained nonetheless.

The prosecution is "the first step toward upholding justice" and should serve as a warning to other companies that sacrifice values for profit, he told The Epoch Times in an interview.

Companies such as Zoom wield formidable economic sway in U.S. industries, making it even more crucial to step up scrutiny and hold them accountable over such complicity with Beijing, he said.

"Any company—doesn't matter if you are based in the United States or China. ... They become a part of the regime's machinery in suppressing pro-democracy activists and encroaching on human rights," Zhuo said.

John C. Demers, assistant U.S. attorney general for national security, echoed that point in a statement, saying that "no company with significant business interests in China is immune from the coercive power of the Chinese Communist Party."

In another example highlighting challenges facing U.S. companies operating in China, the former chief trust officer of Airbnb abruptly resigned in 2019 over concerns about how much data the rental platform was sharing with China, The Wall Street Journal recently reported.

William Evanina, director of the National Counterintelligence and Security Center, said at a panel discussion earlier this month that Americans should be more aware about this issue.

"When we sign up for these companies ... these apps, are we OK with our data going over to a communist country for utilization by the intelligence services?" Evanina asked.

Eva Fu contributed to this report.

CHINESE INFLUENCE

Leading US Firms House Chinese Communist Party Units: Leaked Database

EVA FU

Hundreds of Chinese Communist Party (CCP) members are embedded within the Chinese divisions of major U.S. corporations, from IBM to PepsiCo to 3M, a leaked CCP-member database revealed.

The existence of Party units within foreign companies in China is hardly surprising, given that the regime mandates any organization with at least three CCP members to form a Party branch. But the 1.95 million CCP member list, which includes names, levels of education, ethnicity, and the Party branches they belong to, was to date the biggest revelation about the scale of the CCP's influence on international companies.

Most of the members in the database are from the country's southeastern coastal metropolis of Shanghai.

As of 2016, around 75,000 foreign businesses—over 70 percent of the roughly 106,000 foreign firms in China—have established CCP units, according to state-run media People's Daily.

Armonk, New York-based tech firm IBM has at least two dozen Party units with 808 members in China.

3M, a manufacturer of consumer and health care goods, including N95 respirators and other medical products critical to preventing the spread of COVID-19, employs at least 230 CCP members within five Party units.

PepsiCo, the multinational snack and beverage company, has 45 employees listed under the company's Party branch committee.

Dow Chemical Co., one of the world's three largest chemical producers, lists 337 CCP members in four Party committees.

Other notable U.S. firms on the list include Westin Hotel & Resorts, owned by Marriott International (23 members); analytics firm Nielsen Holdings (94); leading food company Mars (14); and insurance provider MetLife (31).

The U.S. companies and Party branches mentioned are by no means exhaustive. As of 2016, around 75,000 foreign businesses—accounting for over 70 percent of the roughly 106,000 foreign firms in China—have established Party units, according to state-run media People's Daily.

The development of CCP units picked up pace from 2002, after Beijing's top leadership "wrote the obligations of nonpublic firms' Party organizations into the Party charter, providing evidence for the nonpublic firms' Party organizations to host activities and play their roles," according to Chinese media reports from 2002.

State media reported that the country currently has nearly 92 million CCP members. While the database represents only a small fraction of the total membership, it's a key piece of the puzzle for uncovering the regime's penetration of international companies, said Bill Gertz, national security correspondent for The Washington Times, in an interview.

Early this month, the Trump administration imposed travel restrictions on CCP members and their immediate families, reducing the maximum duration of stay for those with B1/B2 visitor visas to one month from 10 years.

The Party Network

Creating more Party units within companies in China has been one of the top priorities for the CCP's Organization Department, a core Party organ that oversees staffing of government officials nationwide, according to Qi Yu, a former deputy head of the department.

Qi, who currently serves as the Party committee secretary at the Chinese foreign ministry, said at an October 2017 news conference in Beijing that the regime requires corporate Party organizations to "organically integrate Party activities with the firm's production in order to support companies' healthy development," according to People's Daily.

Most Party organization activities center around patriotic education to ensure employees toe the Party line.

Mars's Shanghai Party branch, for example, marked this year's traditional Chinese Mid-Autumn Festival by providing products to an event organized by local authorities meant to promote the CCP's history in the region.

Gertz said "membership in the Chinese Communist Party makes those people devoted not to the nation of China, or to the people of China, but to the political party of the CCP," calling such efforts the CCP's "ideological drive" to "basically take over the world."

"They [CCP members] see themselves as besieged by the capitalist world, they see themselves as, basically, at ideological war with a noncommunist world," he said on The Epoch Times' "American Thought Leaders" program.

"Now the West, the free world, needs to wake up and start fighting back against the Chinese Communist Party."

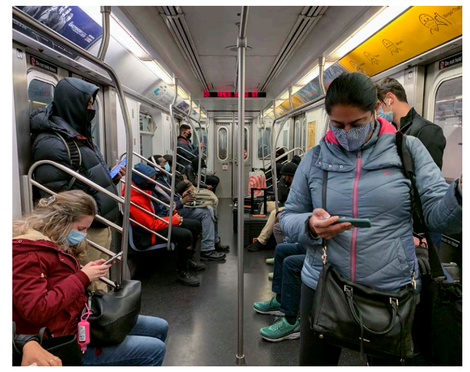
Officials at IBM, PepsiCo, 3M, Dow Chemical, Marriott, Nielsen, Mars, and MetLife didn't immediately respond to a request by The Epoch Times for comment.

Nicole Hao contributed to this report.

-/AFP VIA GETTY IMAGES

A woman walking past Marriott signage in Hangzhou city, Zhejiang Province, China, on Jan. 11, 2018.

CHUNG I HO/THE EPOCH TIMES



In 2018, two Caribbean operators were involved in a series of attacks on U.S. phone users targeted by China Unicom, suggesting coordination between these networks.

Passengers look at their phones while taking the subway in New York on Nov. 14, 2020.

SURVEILLANCE

China Engaged in 'Mass Surveillance' on US Mobile Phones: Report

CATHY HE

The Chinese regime exploited vulnerabilities in the global mobile telecommunications network to conduct "mass surveillance" on Americans, according to a recent report by a cyber research firm.

By analyzing signals data, the report by Washington-based Exigent Media found that Beijing, working through state-owned telecom operator China Unicom, was the leading source of attacks against U.S. mobile users over 3G and 4G networks in 2018.

The regime exploited well-known network vulnerabilities, which allowed it to track, monitor, disrupt, and intercept communications of U.S. phone subscribers while they traveled abroad. The vulnerabilities are centered around the legacy mobile SS7 signaling system, described in the report as "a patchwork system enabling network operators around the world to communicate with each other for international roaming services."

The Chinese cyberattacks targeted tens of thousands of U.S. mobile users from 2018 to 2020, Gary Miller, the report's author and a former mobile network security executive, told The Guardian.

"Once you get into the tens of thousands, the attacks qualify as mass surveillance, which is primarily for intelligence collection and not necessarily targeting high-profile targets," Miller said. "It might be that there are locations of interest, and these occur primarily while people are abroad."

That the attacks were routed through a state-controlled operator indicates a state-sanctioned espionage campaign, Miller told the outlet.

The analyst also found that in 2018, two Caribbean operators were also involved in a series of attacks on U.S. phone users targeted by China Unicom, suggesting coordination between these networks. The two operators were Cable & Wireless Communications (Flow) in Barbados and the Bahamas Telecommunications Company (BTC).

The report found that from 2019, attacks from China decreased, while those originating from the Caribbean networks shot up—suggesting that Beijing was attempting to mask its activities through foreign operators.

"China reduced its attack volumes, favoring more targeted espionage, likely using proxy networks in the Caribbean and Africa to conduct its attacks, having close ties in both trade and technology investment," the report stated.

Citing Beijing's expanded investment in the Caribbean, such as Chinese telecom giant Huawei's partnership with BTC on the Bahamas' 4G rollout, the report questioned whether this indicated a "strategic signals intelligence alliance between China and the Caribbean."

The report added it was likely that Caribbean operators have sold or leased network addresses to Chinese entities, allowing them to conduct espionage, potentially without the operators' knowledge.

Cable & Wireless, the company that owns Flow and BTC, said in an emailed statement to The Epoch Times that it was "carefully reviewing the information in the media reports."

The company added that it continuously monitors its networks across all its markets including Barbados and Bahamas and has "robust security policies and protocols in place to protect the data of our customers."

China Unicom in a statement to The Epoch Times said it "strongly refutes the allegations that China Unicom has engaged in active surveillance attacks against U.S. mobile phone subscribers using access to international telecommunications networks."

In April, the U.S. Federal Communications Commission (FCC) warned that the U.S. operations of China Unicom and two other state-controlled telecoms could be shut down, citing national security risks.

FCC Chairman Ajit Pai said federal agencies were "deeply concerned" about the companies' vulnerability to the "exploitation, influence, and control of the Chinese Communist Party."

Report author Miller found that attacks on U.S. mobile users continued in 2020, originating from Chinese and Hong Kong sources, as well as other countries.

"Unfortunately, these attacks will continue globally between mobile operators until full accountability, reporting of the attacks, penalties, and control of external 'partners and customers' who are provided with access to networks are exercised," Miller told The Epoch Times in an email.

"This needs to happen immediately."

TECHNOLOGY TRANSFER

Leaked Documents Reveal Chinese Regime's Orders to Steal Foreign Technologies

ALEX WU

A series of leaked government documents recently obtained by The Epoch Times reveal that Chinese authorities have funded projects that are aimed at obtaining foreign advanced technologies through partnerships with international research institutions. Public records show that China's Ministry of Science and Technology is behind the efforts.

Budget for 'Transferring' Foreign Technologies

Hebei International Talent Exchange Association (also known as International Technology Transfer Center) was established in 1988 in Hebei Province. It has more than 200 international technical projects and more than 300 foreign experts, covering more than ten fields, including artificial intelligence (AI), information communication, biology, medical, and health.

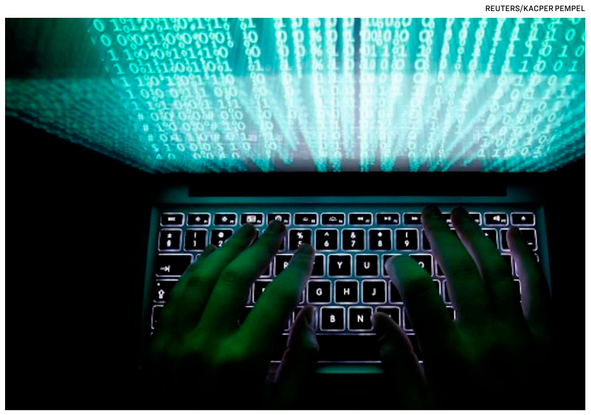
The organization issued a report, "Hebei Provincial Budget Project Performance Evaluation Form" on Nov. 17, in which it explicitly states that the group aims to "introduce foreign advanced technology ... and realize technology transfer [to China]."

To achieve that goal, the document specified that the organization would expand cooperation channels with at least 50 international organizations; set up a minimum of four international scientific and technological cooperation activities; maintain at least 50 foreign technology projects; obtain at least five cooperation intention agreements; and target 60 to 80 foreign technical experts for recruitment.

The report laid out a 1 million yuan (about $153,000) budget for the association to recruit talent from overseas and fund the projects they would set up in Hebei. It also projected a profit of 10 million yuan (about $1.53 million) that could be achieved by "transferring" foreign advanced technology to Chinese companies in Hebei.

The purpose of transferring foreign technology was mentioned in another report that was issued at the same time, titled, "Plan for the Use of Special Subsidy Funds for the Construction of Hebei International Science and Technology Cooperation Base." The foreign technology would upgrade Hebei's technology, improve products, and boost international competitiveness, the report said.

REUTERS/KACPER PEMPEL



Australia, New Zealand, Canada, and the United Kingdom have expressed serious concern over a group acting on behalf of the Chinese Ministry of State Security that is stealing commercial intellectual property in a malicious global hacking campaign, widely known as Cloud Hopper, as of Dec. 21, 2018.

U.S.-based China affairs commentator Li Linyi told The Epoch Times that the initiative is a lucrative scheme and a blatant plan to steal advanced technology and intellectual property from other countries to benefit the Chinese regime.

According to public records, Hebei International Talent Exchange Association operates under the state-run China Association for International Exchange of Personnel (CAIEP). CAIEP is directly managed by the State Administration of Foreign Experts Affairs, an agency under the Chinese regime's Ministry of Science and Technology.

Higher Education Institutions Are Required to 'Transfer' Foreign Technology

Hebei education authorities have also set requirements and goals for obtaining foreign technologies through its "2020 Work Plan of the International Technology Transfer Center of Hebei University of Technology," issued in 2019. The Epoch Times obtained a copy of this document.

Some of the instructions include establishing an international technology transfer center website; "vigorously introducing" international high-tech talents, high-level management teams and advanced technology resources; "all-round" strengthening of international cooperation and technology transfer; and "improving various working systems in the international technology transfer work."

The Hebei University of Engineering, for example, has set up partnerships with international schools to develop high-end scientific and technological projects, as outlined in its report, "Hebei International Joint Center Base Defense," issued on Nov. 21 this year.

Under the section "Cooperative Units and Research Teams" of the document, the university partnered with Le Mans Université and Université Paris-Saclay in France, University College London in England, and Nanyang Technological University in Singapore.

U.S.-based China affairs commentator Li Linyi told The Epoch Times that the initiative is a lucrative scheme and a blatant plan to steal advanced technology and intellectual property from other countries to benefit the Chinese regime.

The document noted that University College London is the world's top science and technology university, ranking among the top 10 universities in the world; and Professor P. Picart at Le Mans Université is an authoritative expert on digital holographic display.

Sounding the Alarm

In October this year, at the Chinese Communist Party (CCP)'s Fifth Plenary Session, Party leader Xi Jinping emphasized "independent science and technology" and "strengthening basic research and focusing on original innovation" in his speech.

Analysts observed that Xi's remarks are a response to the growing criticism from the international community regarding the CCP's theft of intellectual property and technology from Western countries, especially the United States.

On Dec. 9, U.S. Secretary of State Mike Pompeo delivered a speech at Georgia Institute of Technology, in which he called out the CCP's stealing of intellectual property and technologies from other countries. He stated, "Much of the high-end industrial base inside of China is based on stolen technology, or technology purchased from other nations. It's not homegrown."

Gu Qing'er contributed to this report.