

In recent years, high-profile cases of industrial espionage by the communist Chinese regime have prompted the Trump administration to take a multi-pronged approach to crack down on Chinese theft of U.S.

# **Involving China's Student Spies**

Recent extradition of intelligence officer highlights multiple cases of industrial espionage by the Chinese communist regime in the Chicago area

pionage case in which to the United States from Belgium to stand trial has uncovered more 10 that year. details to the saga, including an email implicating a Chinese exchange student working on the Chinese regime's behalf.

In recent years, the United States has launched a multi-pronged Science and Technology (JAST). counterespionage campaign to tackle espionage cases by the Chinese Communist Party (CCP) regime. As the Trump administration highlights the large-scale Chinese theft of U.S. intellectual property in its negotiations with Beijing, the Justice Department changing ideas" or giving lectures has been stepping up its investigation and prosecution of individu-regime in its foreign intelligence

"We cannot tolerate a nation stealing our firepower and the fruits of our brainpower," said John Demers, the Assistant Attorney General of the National Security Division last year when dealing with a case involving CCP intelligence officials stealing U.S. trade secrets. The methods involved in these cases are diverse and often interrelated. A Sept. 26 report by the Chicago Department last year.

## Aerospace Espionage On Oct. 9, 2018, the United States

secured the extradition of Xu Yanjun, a Chinese intelligence official, from Belgium, where he had been apprehended for attempting to obtain industrial secrets from American aerospace companies under a false identity. It is the first success-

of a transnational es- documents. He is identified as the deputy director of the Ministry of a Chinese intelligence State Security's Jiangsu provinofficial was extradited cial department. Xu was charged with stealing trade secrets on Oct.

> The prosecutor alleged that Xu used names such as "Qu Hui" and "Zhang Hui" to carry out his espionage work and posed as a representative of the Jiangsu Association for

According to the indictment, since 2013, Xu had targeted top American airlines and industry experts for "highly sensitive" technical information and invited employees of American companies to China under the pretext of "ex-

In early 2017, Xu's associates contacted an ethnic Chinese aerospace engineer from General Electric (GE) via LinkedIn, also known as "A." The engineer was deeply involved in the design and analysis of GE's new commercial jet engine, a technol-

ogy which is the prime target of the

Communist Party's agents. Later, the engineer was asked to make an experience exchange report in Nanjing, China, which is the provincial capital of Jiangsu. Tribune revealed links between Before going to China, he loaded individuals indicted in these two five GE aerospace documents onto cases, made public by the Justice the hard drive of his personal laptop. The Chinese side promised him \$3,500 for the lecture and covered the costs of his airfare and

> A few months later, the aerospace engineer told the FBI his speech at the Nanjing University of Aeronautics and Astronautics encountered some initial technical problems. Staff at the university,

accommodation.

made by the U.S. justice system. tion Technology, told him that the in August 2013, where he studied All were seen as targets of the The Chinese characters for Xu's projector wouldn't work, so he al-The FBI's investigation name were not provided by court lowed them to insert a USB drive into his personal laptop, which contained the confidential GE

documentation.

Further investigation by the FBI found ongoing "criminal activity" on the engineer's social media accounts, including that involving

The FBI identified Xu as the "real user" of an iCloud account containing a record of Xu's covert activities and the technology he wanted to collect.

On Jan. 23 and Feb. 3, 2018, Yanjun Xu asked "A" via email to collect GE's technical documents on engine production and design, including "containment analysis"

In March 2018, Xu emailed the engineer and suggested that he download GE aviation records and "more data... Including any relevant design," following which the two agreed to meet in Belgium. The U.S. Office of the Attorney General began preparing prosecution documents to indict Xu and A" about "midterm exam ques-

provide them to Belgian authorities. Xu arrived in Brussels on April 1, 2018, but instead of the GE engineer, he was greeted by Belgian three years. police and FBI agents, and put in

"U.S. aerospace companies invest decades of time and billions of dollars in research," Benjamin Glassman, the U.S. attorney for the Southern District of Ohio, said at the time of Ji's indictment. "In contrast ... a Chinese intelligence officer tried to acquire that same, hard-earned innovation through theft."

The investigation into Xu also opened the door to other cases of Chinese economic theft, as reported by the Chicago Tribune. U.S. investigators took note of 27-year-old Ji Chaoqun, a Chinese man who which is controlled by the Chinese had begun attending Chicago's ful extradition of a Chinese official Ministry of Industry and Informa- Illinois Institute of Technology for U.S. defense contractors.

Another Meaning for 'Midterm'

Ji because of his correspondences with Yanjun Xu uncovered in the investigation of the latter. From December 2013 to July 2015, Ji and "intelligence officer A" exchanged about 36 text messages, FBI agent Andrew K. McKay said in a declassified court document.

"Intelligence officer A" refers to

Ji Chaoqun was arrested in Chicago on Sept. 25, 2018, and charged with acting as an illegal agent on behalf of a senior MSS intelligence official in Jiangsu Province. The prosecutor alleged that Ji had received covert instructions from Chinese intelligence agents, and that he had hidden his contacts with these agents when undergoing a U.S. military background

In Ji's electronic accounts, federal authorities were drawn to an email addressed to "intelligence officer tions." In the email, Ji indicated "exam questions" over a period of

However, the email attachments Ji sent to Xu had nothing to do with midterm exams, but instead contained background information on eight American scientists and engineers also residing in the United States.

According to a federal criminal

on these eight individuals at the direction of a high-ranking Chinese intelligence official, so that they could be recruited as spies. These eight people were originally from Taiwan or mainland China. All of them were employed in or had worked in the field of science and technology, and seven had worked

electrical engineering on a F1 visa. CCP's new-generation espionage activities, the federal complaint stated. These spy operations are The investigators were alerted to part of the Party's strategy to win overcome the United States without active warfare.

Week 44, 2019 THE EPOCH TIMES

According to the FBI, the CCP's spy agencies typically focus their recruitment efforts on ethnic Chinese for cultural and linguistic reasons. Given his position as an international student, Ji Chaoqun was in an ideal person to reach these individuals.

Court records show that the Chinese agents focused on stealing secrets from major U.S. aerospace companies, and contacted Ji seven months after he began his studies.

Ji graduated in 2015 and, a year later, joined the U.S. Army Reserve via a program called Military Accessions Vital to the National Interest (MAVNI), which had been started in response to an acute shortage of manpower.

Ji made three trips to Beijing and met intelligence officials at a hotel. "Based upon my training and experience," the FBI agency McKay wrote in court records, "conductthat he had attached eight sets of ing meetings in hotel rooms is an indication of intelligence officer tradecraft because meetings in hotel rooms provide a discreet, private place for the intelligence officer to recruit or debrief his/her intelligence asset."

John Lausch, the United States attorney for the Northern District of Illinois, spoke to the Chicago Tribune about the significance of complaint, Ji collected information Ji's case. He noted that Ji had come to the United States on a visa intended for his studies, only to be used by Communist Party agents as an intelligence asset.

Steven Dollear, an assistant U.S. attorney, said that while Ji was not charged with collecting military secrets, he would have had access to such information at that time. Joining the U.S. military increased the

scope of Ji's access to information, especially since he had also received training by Chinese intelligence officials, making him a greater threat to U.S. national security.

Ji has pled not guilty to all charges.

## **Fake Employment and Immigration Fraud**

Ji's criminal case also touched on a large-scale immigration fraud scheme involving a federal program that allows international students to work in the United States in fields related to their studies upon graduation.

After receiving his master's degree in electrical engineering in 2015, Ji remained in the United States through a temporary work program called the Optional Practical Training (OPT) program. The OPT program allows recently graduated international students to stay and work in the U.S. for one year in order to put their knowledge into marketable practice. It is widely seen as a step towards converting their residence status to the H-1B work visa. Since 2016, graduates in science, technology, engineering and mathematics (STEM) fields have been allowed to extend their internships by two years.

Ji claimed to have landed a job as a software engineer at a company called Findream LLC. The company, which describes itself as an emerging technology company based in Mountain View, California, is one of two companies run by Chinese businesswoman Weiyun Huang, also known as Kelly Huang. Her other company is called Sinocontech.

However, "Findream LLC." and "Sinocontech" do not actually exist. Federal authorities say the companies were used to provide false employment credentials for Chinese students studying abroad, so that they could stay in the United States after they graduate.

Huang, now aged 30, is charged

The LEAP-1A engine,

developed by CFM, a joint venture between France's Safran and General Electric, during its handover ceremony in Colomiers, outside Toulouse on April 15, 2016.

documents, according to a federal indictment that was made public on July 26. Huang earned \$2 million from 2,600 students who received false employment certificates through her fake companies. Federal authorities say Ji is one of Huang's clients, as Ji had admitted to FBI agents that he had paid "Findream" \$900 and never did

any work for that firm. According to attorney Robert Rouse, law enforcement is tracking the 2,600 individuals involved in the fraud scheme to determine appropriate future steps.

with conspiracy and fraud to pro-

vide false employment records,

financial statements, and tax

# Tip of the Iceberg

MANDEL NGAN/AFP/GETTY IMAGE

While Ji's case is the latest in a series of communist Chinese espionage cases in Chicago, the Party's espionage operations have targeted some of the city's top companies for over a decade, from financial companies like the Chicago Mercantile Exchange, to manufacturers like subsidiaries of Caterpillar Inc.

Beyond the aerospace industry, as given in the case above, U.S. officials have warned that the CCP regime is intent in acquiring advanced transport technology on subways, passenger rail, and freight trains.

On July 11, the Justice Department issued a news release alleging that Xudong Yao, 57, a Chinese software engineer at a locomotive Robert Grant, the former director of the manufacturer in suburban Chica-FBI's Chicago office go, was suspected of having stolen trade secrets from the company and taken them to China. He was charged with nine counts of stealing trade secrets.

Yao was born in China and became a naturalized U.S. citizen, according to the press release and

an FBI wanted poster. The indictment shows that Yao began working for the locomotive manufacturer in August 2014 and, within two weeks of his employment, allegedly downloaded more than 3,000 unique electronic files related to the company's locomotive operating system. Over the next six months, Yao downloaded a number of electronic files containing other trade secrets, including technical documents and

Yao flew from China to Chicago's that developed products for the Division and head of the China Ini-O'Hare International Airport on Chinese People's Liberation Army tiative, told the Chicago Tribune Nov. 18, 2015. He was suspected of (PLA). Hanjuan Jin was arrested on having taken the stolen informa- Feb. 28, 2007, when customs offi- by the Chinese regime have cost tion, including nine complete copcers at Chicago's O'Hare Internaies of the Chicago manufacturer's tional Airport spotted the Motorola control system source code and a documents along with more than system design manual explaining how the code works, before returning to China.

In 2015, naturalized U.S. citizen Chunlai Yang pleaded guilty to of how, in addition to specialized of theft of intellectual property." stealing trade secrets from the Chicago Mercantile Exchange (CME), where he worked as a senior software engineer. He was sentenced States and their contacts in order to four years' probation.

Court records show that Yang

was accused of downloading more than 10,000 source code files from CME's internal system and planning to set up his own financial trading company, Tongmei Futures Exchange Software Technology in China, according to Chicago Tribune's report. The company was tasked with increasing trading volume on an electronic exchange controlled by the Chinese regime.

In Yang's ruling, federal prosecutor Barry Jonas told the judge that Yang sought to transfer CME's proprietary software to multiple financial exchanges in China.

"We're talking about a country here who has a reputation, who it's commonly known, they're into economic espionage, especially reaching into the United States," Jonas said, according to court records. "Economic espionage, computer intrusion, these are cybercrimes. These are the crimes of the future that are just growing leaps and bounds in society, and they have a direct negative impact on the U.S. economy, both commercially, as well as national security."

# Every person in China is incentivized to collect intelligence, from waiters to 19-year-old college students studying in the United States.

Not all spies in the Chicago area recruited by the CCP's intelligence apparatus are mainland Chinese. In 2009, a chemist from Taiwan was charged with stealing the formulas for 160 paints and colors from his employer, Valspar. The suspect, a naturalized U.S. citizen, planned to take the formulas to China and turn them over to a rival company, where he would be given a position. However, the FBI arrested him before he boarded his flight to Shanghai. He pled guilty to his charges.

The year prior, a Chinese woman working as a software engineer at Motorola was charged with stealing the company's secrets and transferring them to a Chinese telecommunications company \$30,000 in cash as she attempted to leave for China.

operatives, the Chinese regime makes use of many untrained individuals residing in the United to steal technology and other industrial secrets.

# 'China Initiative' to Counter a Longstanding Threat

According to Marc Raimondi, a spokesman for the Justice Department, the People's Republic of China is the culprit behind the majority of cases involving theft of economic or trade secrets. It was "important to note that there is a nexus to the Chinese Government in 80% of our economic espionage cases and over 60% of our trade secret theft cases," Raimondi wrote in an email to Chicago Tribune.

In addition to recruiting businessmen and students like Ji Chaoqun to gain access to American technology, the CCP has also used recruitment programs like the "Thousand Talents Program" to attract overseas high-tech workers to work in China, which has caught the attention of the FBI.

Robert Grant, the former director of the FBI's Chicago office, said that the CCP indoctrinates the Chinese people to think it is "the duty and responsibility of citizens" to help develop the economy and military of the People's Republic.

"Every person in China is incentivized to collect intelligence, from waiters to 19-year-old college students studying in the United States," Grant said.

Ji Chaoqun's case marks an area of growing concern for U.S. authorities: the CCP government's complex and long-term operation to have spies and foreign agents steal innovative ideas and technology from foreign companies and defense contractors.

Partially in response to the PRC's rampant intellectual property theft, the Trump administration imposed a series of tariffs on Chinese goods starting last spring. In fall 2018, a few weeks after Ji's case came to light, the Trump administration launched a China Initiative to combat economic theft.

The Initiative seeks to identify and deal with priority trade secret cases; develop enforcement strategies to address problems of researchers in laboratories, defense industries, and universities who may be persuaded by the CCP to transfer technology illegally to the PRC. The China Initiative also aims to educate American colleges and universities about the

John Demers, Assistant Attorney General of the National Security investors money and put Americans out of work.

"China is the number one intelligence threat to the U.S. right now," Demers said. "On the economic U.S. prosecutors working on side ... it's far and away the num-Jin's case held it up as an example ber one threat to the U.S. in terms

> This article first appeared in the October 2019 issue of Truth China, a magazine published by the Chinese-language edition of The Epoch Times.



# Is China's Invasive New Cybersecurity Law Another Backdoor to American **Intellectual Property?**



A Chinese woman looks at her phone as Chinese Paramilitary police stand guard in Tiananmen Square, Beijing, on Dec. 9, 2015.

# **JULIO RIVERA**

t's the worst-kept secret in international business. China is robbing America blind As the Trump administration at-

tempts to navigate the choppy waters of negotiating with a trade partner that is less than transparent, the possible ramifications of China's new cybersecurity law are more than enough to keep international businesses that operate in the so-called "People's Repub-

lic" in a state of perpetual high anxiety. China's new cybersecurity laws under its Multi-Level Protection Scheme 2.0 (MLPS) will require that all internet service providers and mobile data providers require facial scans to sign up customers for new services. The laws will go into full effect on Dec. 1, 2019. This means that every new cell phone number assigned in China will be associated with a facial scan.

That's in addition to the Chinese Ministry of Public Security's mandate that all data on Chinese networks and systems be available for the Chinese regime to audit at will. Although the Chinese regime claims that the new law is not meant to suppress citizens or to be invasive, many are skeptical as to the true nature of the state's intent

Guo Qiquan, a Chinese politician who had a part in devising the new law, said, "It will cover every district, every ministry, every business and other institution, basically covering the whole society. It will also cover all targets that need cybersecurity protection, including all networks, information systems, cloud platforms, the internet of things, control systems, big data and mobile internet," according to the South China Morning Post.

That, in essence, subjects all entities operating in China, whether public or private, to an intrusion that encompasses the totality of all data, including proprietary business secrets, that can be used in a multitude of ways by belligerents within the Chinese regime.

This should be of particular concern to customers of international businesses with operations based in China, as the new laws give the regime carte blanche over sensitive in-

An investigation found that these 'spy chips' had been installed into devices that were purchased by nearly 30 companies, including government contractors, Amazon, Apple, and even financial

institutions.

NICOLAS ASFOURI/AFP/GETTY IMAGES

businesses with ties to China, which may not even have operations located within the country.

This is just the latest attempt by the of its espionage programs. Over the time now. "spy chips" had been installed into devices that were purchased by nearly 30 companies, including government contractors, Amazon, Apple, and even financial institutions.

formation related to foreigners and

The Chinese regime also engaged in military espionage, as Chinese statetion related to the U.S. Naval Undersea to happen. Warfare Center.

One of the most dangerous byprod- Julio Rivera is the editorial director ucts of Chinese state-sponsored hacking is the rise of "hacking for profit" campaigns executed by unchecked criminal networks that have been trained by the Chinese regime.

These groups are noted for their socalled software supply-chain hacks. not necessarily reflect the views of

of a software developer is hacked, and malware code is planted onto apps and software that is potentially used on millions of devices. Hacking groups such as China's ShadowHammer have Chinese regime to further the scope been executing these attacks for some

past few years, these operations have Perhaps the simplest answer to included the distribution of electronic this new expansion of governmental hardware that had been manufac- strong-arming for non-Chinese inditured with a preinstalled spy chip. viduals and entities is to wholly cut ties An investigation found that these with China. Don't buy Chinese, don't do business with Chinese companies or businesses with ties to the "Sleeping Dragon," and you have a better chance of not having your information fall into unscrupulous hands.

The only other alternative, one that would be an impossibility for most inbacked hackers penetrated a U.S. Navy dividuals and businesses, would be to contractor and stole 614 gigabytes of cut technology out of their lives. For data containing classified informamost people in 2019, that's not going

> for Reactionary Times. A conservative columnist and commentator, he works as a business strategist.

Views expressed in this article are the opinions of the author and do These attacks occur when the network The Epoch Times.



A man uses a smartphone outside an Apple store in Beijing on Jan.

**CHINESE ESPIONAGE** 

# US Administration's War on Chinese Espionage Tackles IP Theft Schemes

## **CATHY HE**

News Analysis

tealing innovations from the United States is a key part of the Chinese regime's bid to become a global competitor in

The campaign to steal information is aggressive; Chinese spies now make up about 90 percent of perpetrators in U.S. espionage cases, according to the Washington-based think tank Center for Strategic and International Studies.

Earlier this year, an adjunct professor at the University of California-Los Angeles was convicted for his role in an elaborate scheme to fraudulently acquire sensitive microchip technology from a U.S. firm, and illegally export it to China.

The semiconductor chips in question have both commercial and military applications, including in missile guidance systems for the U.S. military.

Yi-Chi Shih, 64, a dual U.S. and Taiwanese citizen, in violation of U.S. export controls, managed to ship the chips to a Chinese company that he oversaw, which was building a factory in the southwestern city of Chengdu to produce the same type of devices.

Court documents show that the company was planning to make the chips for the Chinese military to be used for missile guidance.

Shih's case is but one of a growing list of federal prosecutions in recent years against Chinese espionage-a blanket term encompassing theft of trade secrets, illegal export of technologies critical to national security, cyberhacking, and traditional spying.

More than 80 percent of all economic espionage charges brought by federal prosecutors since 2012 implicated China, according to the theft as it is guidance to innovate," U.S. Department of Justice, which Demers said in his December teslast November launched the "Chitimony before the Senate." na Initiative" to combat the threats posed by Chinese espionage and U.S. senior intelligence official and other forms of Chinese infiltration author of "Chinese Intelligence into U.S. society.

Since January 2018, more than that he's compiled a database of 30 China-related espionage cases, 464 cases of China's overall esincluding those involving Chinese intelligence officers, former U.S. intelligence officials, Chinese nationals, and naturalized U.S. citizens from China, have made the headlines.

Meanwhile, the FBI has more than 1,000 active investigations he said, and in turn, about half of into intellectual property (IP) those are related to aerospace or theft, "almost all leading back to aviation technology. China," FBI Director Christopher Wray told U.S. senators at a congressional hearing in July.

# **Growing Recognition**

The ramped-up enforcement of pionage in recent years is the result of a growing recognition of the threats posed by the Chinese try of State Security [China's top communist regime, according to

"The awareness has been raised across the board," said Casey Fleming, espionage expert and CEO of BlackOps Partners, a consultancy specializing in guarding organizations against theft of interactions with representatives trade secrets, adding that senior of government and businesses, leaders across the private sector, he estimates that there are about government, and military are now 150,000 individuals operating realizing the true intentions of the on behalf of the Chinese regime Chinese regime.

He told The Epoch Times, "The Chinese Communist Party wants global superpower."

mers, the U.S. assistant attorney search. general for national security, as "rob, replicate, replace."

and, one day, the global market," Demers told the Senate Judiciary Committee in December 2018.

The Chinese regime, meanwhile, has consistently denied that it's stolen secrets from U.S. companies and institutions to further its

"They have a master shopping list by industry, with heavy emphasis on technology and finance," Flem-

Much of this shopping list can be found in Beijing's ambitious "Made in China 2025" industrial plan, which aims to transform the country into a high-tech manufacturing powerhouse by the year 2025. The policy targets 10 industries for development including robotics, aerospace, and biotechnology.

The plan is "as much roadmap to

Nicholas Eftimiades, a former Operations," told The Epoch Times pionage efforts around the world, based on public prosecutions. "Most of ... [the cases] fall into the

technologies identified in 'Made in China 2025," Eftimiades said. About 200 of those cases involve military or dual-use technologies,

# **Academic Espionage**

Eftimiades said the Chinese regime employs a "whole-of-society approach" in its efforts to acquire targeted technologies, mobilizing Chinese economic and other es- a range of entities, from state bodies down to the individual.

> "They use not only the Minisintelligence agency], the People's Liberation Army's military intelligence department, but [also] stateowned enterprises, academia, and individual companies," he said.

> Fleming said that, based on his professional experience as well as throughout the U.S. private sector, military, and government.

This figure, however, doesn't to replace the United States as a include Chinese students in the country, some of whom have been It aims to achieve that through a used by the Chinese regime to steal strategy described by John C. Detechnology and cutting-edge re-

For example, Liu Ruopeng came

to the United States in 2006 to "Rob the American company of its study for a doctorate at Duke Uniintellectual property, replicate the versity, working at a lab that cretechnology, and replace the Ameriated a prototype of an "invisibility can company in the Chinese market cloak" that could conceal objects Men work with a jet engine at from microwaves. Such technola General Electric (GE) facility ogy has potential applications for in Rio de Janeiro on June 8, mobile phones and antennas. 2016. Last year, a Chinese Liu took that technology back to China and established a research charged with stealing trade

> charge him with a crime. There are roughly 360,000 Chinese studying in the United States, according to the latest estimates by the Institute of International

> institute and a Hong Kong-listed

company based on such innova-

Education. While academic espionage only applies to a small minority of Chinese students, Eftimiades said, "the problem is that the including GE; Zheng Xiaoqing, a technologies that they take are naturalized U.S. citizen who was so devastating, and provide such indicted in April 2019 for alleged an economic boost or a military theft of GE's turbine technologies; boost to China, that its [impact] is and Ji Chaoqun, a Chinese national

demic espionage by working with academic and research institutions.

(NIH), the largest funder of bio-States, sounded the alarm in a letter to 10,000 partner institutions in August of last year, warning of the threat of IP theft and foreign Whole-of-Society Response interference.

In December, the NIH published cruitment program, the "Thousand Talents Plan," which aims to attract foreign experts to work in China. The report raised conused to transfer key research-ofgrants-to China.

The NIH has since started investigating NIH-funded foreign scientists at more than 55 U.S. institutions, Director Francis Collins told a Senate committee in April. Thus the firing of three Asian researchin Texas, and two Chinese-Americans at Atlanta's Emory University.

out to colleges and universities technologies. across the United States as part of the Chinese regime, the Associated Press recently reported.

In the past few months, a University of Kansas researcher was indicted for collecting federal grant money while working full time for a Chinese university; a Party is another level above that. California-based Chinese couple, both researchers, were charged with stealing trade secrets from fight again." a U.S. children's hospital where they had worked, for the benefit Epoch Times reporters Frank of their Chinese and U.S. biotech companies; and a former scientist to this report.

at the Los Alamos National Laboratory was charged with lying about his engagement with the Thousand Talents Plan.

## **Growing Sophistication**

Chinese espionage methods have become more sophisticated, Eftimiades said, notably in how the Chinese regime has integrated human intelligence operations with cyber espionage.

An example of this integrated human-cyber approach was recently uncovered in a report by U.S.

cybersecurity firm CrowdStrike. After analyzing federal indictments from 2017 to 2018, the firm concluded that the Jiangsu Province bureau of the MSS (known as

JSSD) orchestrated an elaborate plan to steal aviation technology. The operation, the report said, involved a hacking component that was supported by a range of human operatives, including intelligence officers, security researchers, and staff at foreign companies

recruited by the MSS. An October 2018 federal indictment charged 10 people with trying to steal know-how for making turbofan engines: two officers at the JSSD, five computer hackers, a malware developer operating at the direction of JSSD, and two tions. The FBI investigated Liu's Chinese employees at a French activities but ultimately didn't aerospace manufacturer's office

in Suzhou City, Jiangsu Province.

CrowdStrike's analysis led it to conclude that the indictment was related to three other cases: a JSSD officer named Xu Yanjun, who was arrested in Belgium and extradited to the United States in October 2018 on charges of stealing aviation secrets from foreign companies, He noted that it has only been ficer who was charged with cowithin the past year that the U.S. has vertly working for the JSSD to help stepped up its efforts to tackle acatry and recruit foreign engineers

and scientists. The cyber firm concluded that The National Institutes of Health they were all part of the same scheme, with Xu tasked with remedical research in the United cruiting Chinese nationals living overseas to serve as co-conspirators in the operation.

Echoing comments made by senior U.S. officials, Eftimiades said a report placing the spotlight on that the United States will have to the Chinese state-sponsored re- adopt a similar whole-of-society approach to fight the Chinese regime's transgressions.

"It can't just be done by the government alone–It's got to be done cerns that the program could be with the government in partnership with industry and academia," ten produced with federal research he said. "While the government is very, very used to protecting its own secrets, it's not so used to helping American industry protect their secrets."

The private sector and academia need to be trained and educated far, the investigations have led to on the threats, and also share relevant information with each other. ers at a top cancer research center The government could also help industry and academia set better standards to vet people for insider The FBI has also been reaching access to critical information and

Fleming said that every Ameria campaign to combat IP theft concan needs to understand that ducted by researchers that benefits China is a communist country, governed by a party that has been running a covert war against the

United States.

While most Americans may subscribe to the concept of "win or lose," he said "the Chinese Communist

"They believe in 'live or die:' 'I must live. You must die, never to

Fang and Nicole Hao contributed

Since January 2018, the U.S. Department of Justice has prosecuted more than 30 Chinarelated espionage cases.



intelligence officer was secrets from Western aviation companies, including GE.

**RELIGIOUS FREEDOM** 

# Google Features Chinese Communist Party's Message About Religion

# **EMEL AKAN**

ASHINGTON–The official press office for the spiritual practice Falun Gong is sounding a warning: Beijing attempts to influence U.S. public opinion by using a distorted and biased narrative that portrays an ideal view of the Chinese Communist Party when it comes to religious freedom.

The Party employs this strategy using major search engines, including Google, Bing, Yahoo, Ask, and Duckduckgo, researchers say.

When asked about Google's role in spreading Communist Party propaganda that distorts the Party's record on religious freedom and attacks Falun Gong, U.S. Ambassador-at-Large for International Religious Freedom Sam Brownback put the issue in a larger context. He said China's growing influence has become a major concern in the United States and may demand a response from Congress or the administration.

"There's a robust debate in the country right now, whether it's the tech companies or sports entities. This is a big, robust debate. These issues should be brought up and they should be discussed," he said at a press briefing on Oct. 25, ahead of International Religious Freedom Day.

Oct. 27 marked the 21st anniversary of the International Religious Freedom Act of 1998, which was passed to endorse religious freedom as a foreign policy of the United States.

"We stand for freedom of speech. We stand for freedom of religion," Brownback said, noting that the government should protect those basic human rights. But these principles also apply to individuals and companies in the United States, he said.

Brownback said the "robust discussions" are important for "reaffirmation of these basic principles" and may sometimes prompt Congress or the administration to take action.

# Religious Freedom in China

The Chinese regime tries to exploit Google, the world's leading search engine, to influence the American public, according to Falun Dafa Information Center (FDIC) researchers.

For example, when a user searches for "religious freedom in China," Google guides the user by presenting the "People also ask" box. In this box, Google typically lists the most common questions matched up with what the search engine deems to be the most credible answer.

It's my hope that the Chinese will agree at some point in time to start directly addressing with us and with other communities around the world their horrific record on religious freedom, on religious persecution that they're doing.

Sam Brownback, U.S. ambassador-at-large for international religious

A parade to celebrate

in New York on May

World Falun Dafa Day,



Brownback, U.S. ambassadorinternational religious freedom at the State Department in

One of the questions presented by Google is "Does China have freedom of speech and religion?"

And the response to the question is: "The 1982 Constitution provides its citizens the right to believe in any religion, as well as the right to refrain from doing so: Citizens of the People's Republic of China enjoy freedom of religious belief."

A similar issue arises when searching for "Falun Gong," an ancient spiritual discipline brutally suppressed in China. Google lists the question "Is Falun Gong Buddhist?" and the top answer takes the user to a Chinese regime website that attacks the meditation practice, according to FDIC spokesperson Erping Zhang.

"This is akin to directing users to a neo-Nazi website to learn about the finer points of Judaism," said Zhang. "These answer boxes are supposed to direct you to what Google considers to be the foremost authority on any given topic. Does this mean Google believes the Chinese regime to be the most 'authoritative' on the topic of Falun Gong and religion?"

Zhang said FDIC raised that issue with Google a few weeks ago and still hasn't received a response.

Google's search results for "Falun companies." Gong" in the UK include the same United States.

For searches in the Chinese lanslanted toward the Chinese regime's views. On some pages, Chinese Communist Party-controlled sites make up the majority of search results. This pattern is observable across several search engines, including Bing, Yahoo, Ask, and Duckduckgo, according to FDIC.

# **Increased Pressure on Beijing**

The Trump administration has stepped up its criticism of China in recent months for its detention of more than a million Uyghur Muslims in socalled re-education camps in China's northwestern region of Xinjiang.

Brownback said the United States would continue to press China to end the persecution of not just Muslims but also Christians, Tibetan Buddhists, and Falun Gong practitioners. He hoped that these pressures would

"It's my hope that the Chinese will agree at some point in time to start directly addressing with us, and with other communities around the world, their horrific record on religious freedom, on religious persecution that they're doing," he said.

The Trump administration made religious freedom a priority at this year's United Nations General Assembly (UNGA), and China was the main target. Brownback said it was the first time a state hosted a religious event at the UNGA.

Vice President Mike Pence in a recent policy speech also raised concerns about China's human rights abuses and its growing influence on U.S.

"Today, China is not only exporting Chinese Communist Party-controlled hundreds of billions of dollars in unwebsites as appear in searches in the fairly traded goods to the United States, but lately, China has also been trying to export censorship-the hallmark of guage, the results are even more its regime," he said on Oct. 24. "By exploiting corporate greed, Beijing is attempting to influence American public opinion, coercing corporate America."

> Pence scolded U.S. corporations such as Nike and also the National Basketball Association for siding with the Chinese regime.



## **BOOK REVIEW**

# Dancing Through the Darkness of Mao's China

Book Review: Tia Zhang's journey of pain and triumph is brilliantly told in 'Dancing Through the Shadow

## **RYAN MOFFATT**

ometimes the impact of mass tragedy gets lost in the statistics. When death tolls are in the tens of millions, such large-scale suffering becomes remote and untouchable. The human capacity for empathy has reached its limit.

On the other hand, personal accounts of those who lived through atrocities do more to shed light on them than any sterile statistic could. One such story is told by Agnes Bristow in "Dancing Through the Shadow," a first-person account of life in Mao Zedong's China.

The book tells the true story of Tia Zhang, a ballet dancer who came of age during the time when Mao's grip was slowly strangling the country. The simple yearnings and trappings of childhood, adolescence, and motherhood are beautifully woven together against a backdrop of totalitarian brutality. It's a remarkable novel that humanizes the plight of a nation coming to terms with its new reality as a socialist state.

The communists took power in China in 1949, ending a decadeslong civil war that had left the country weary and looking for change. At first there is hope that the new government will improve life for the average citizen.

Instead, China under Mao's leadership begins a descent into violent revolution that would result in one of the century's greatest humanitarian disasters. The statistics are staggering. Conservative estimates put the death toll at 65 million. The Great Leap Forward, Mao's attempt to collectivize agriculture, resulted in the worst famine in history. Forty-five million people were beaten, starved, or worked to death.

This is the world in which Tia Zhang has to make her way.

# From Prosperity to Destitution

Tia's father was a high-ranking official with the Kuomintang, the governing party at the time, and provided a lavish life for his family, complete with a residence in the heart of Beijing. It was a harmonious existence far removed from the dangers that lurked just around the corner. The oldest of her siblings, Tia was coddled and disciplined in strict Chinese traditions, groomed by her mother to be a lady and destined for a life of privilege and

That fate was irretrievably altered when the communists arrived in Beijing and the Kuomintang suddenly and unexpectedly ceded power. Hopes that the communists will offer a reprieve from the strife of war and the promised utopia will be ushered in are quickly dashed when it becomes apparent that anyone once loyal to the Kuomintang is destined to suffer for it.

In a desperate bid for freedom, 10year old Tia and her family attempt to move to the safe haven of Taiwan. But a harrowing near-death journey shatters that prospect and the family is forced to relocate to Qingdao and eventually back to Beijing, where their life of privilege unravels into one of destitution.

It becomes increasingly apparent that there is no escape from the Communist Party's grasp, especially for a family like Tia's that once held a privileged position in the ranks of the Kuomintang.

# **Hope Through Dance**

Life carries on, however, and even when Mao's Great Leap Forward caused millions across the country to starve, Tia's family finds a way to survive. The daily struggle to meet the basic necessities of life affected the entire nation, and Tia's family was no exception.

Through hard work and talent, Tia secures a coveted spot in Beijing's Ballet Academy, staffed with professional dance teachers from Soviet Russia. The school operates

The Great Leap Forward, Mao's attempt to collectivize agriculture, resulted in the worst famine in history. Fortyfive million people were beaten, starved. or worked to death.



Tia Zhang

With extreme ideologies on the rise in the West, Tia's story serves as a reminder of the human cost beyond the statistics.

A photo of Tia

Zhang from the

book "Dancing

Through the

cover of the new

dance studio, but Tia nonetheless receives a first-class dance education. Dance was used as a tool for communist propaganda, and because the school was favoured by Mao's wife, Jiang Qing, Tia had the opportunity to perform for Mao and his dignitaries. The stark contrast between lavish Communist Party banquets and the starving population left a lasting impression on Tia, foreshadowing her disillusion with

more like a military academy than a

the Party and communism. By the time Tia had become an assistant instructor at the academy, Mao had unleashed his Red Guards. Like a plague, this frenzied group of students and children of Party officials brought mayhem to the country in a wave of revolution and violence. The Red Guards were brainwashed from childhood to be Mao's devoted servants. They were the perfect vehicle for his Cultural Revolution as they marched the streets, berating and beating anyone

without fear of repercussion. At one point, the ballet academy is overrun by its Red Guard students, who brutally beat the senior

teachers and berate the assistants, punishing them severely for their education methods by forcing them to clean latrines and perform the most degrading duties.

Tia suffers her fate in silence, complying with the demands of her brainwashed students. Like many others, she is forced to bury her empathy and face the world with as much indifference as she can muster.

During all the turmoil she finds love, but has to face the disapproval of her family and traditionalist mother who wanted her to have an arranged marriage.

This would be difficult enough without Mao's policies and the ever-present threat of being sent to a labour camp or worse. Love was a risky proposition in Mao's China and both Tia and her husband would spend hard time in China's labour camp system.

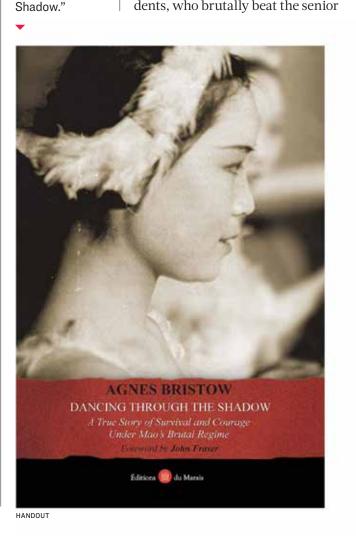
The novel follows Tia through each stage of her life as she navigates motherhood, marriage, and an escape from communist rule. All the while Mao hangs like a shadow in the background, dictating the terms and conditions through which Tia must find her way.

# **Lessons From the Shadows**

Tia's journey is one of pain, triumph, and a true testament to the human spirit. At once tender, traumatic, and terrifying, the story is gripping enough to warrant the level of detail Bristow uses as she expertly combines Tia's experience with enough political analysis to shed light on life under Mao and how his policies resulted in such a high death toll. It is difficult to fathom the desperation of a populace forced to react in fear to nearly every happenstance.

This book is a worthy read for those who entertain any romantic notions about communism or Marxism. With extreme ideologies on the rise in the West, Tia's story serves as a reminder of the human cost beyond the statistics. Many Chinese of that generation will be able to identify with her plight.

The book is ultimately about love, loss, courage and the intricacies of life amplified by the desperation of circumstance. Tia's story is a truly beautiful vehicle for exploring the human cost of political ideologies taken to the extreme, where the human spirit is put to the test.





**TRUTH and TRADITION** 

# COVERING IMPORTANT NEWS OTHER MEDIA IGNORE

LEADING REPORTING ON

THE CHINESE COMMUNIST THREAT

FOR THE PAST 18 YEARS

The Epoch Times not only reports reliably on U.S. politics and the Trump administration, but also publishes authoritative China news, covering topics including:

- Impact on the United States
- · Business and economy
- Communist infiltration of our government, businesses, schools, universities, popular culture, and more
- Disinformation surrounding U.S.–China trade relations
- Security and espionage
- Influence on media and Hollywood
- Overseas interference and United Front activity

The Epoch Times has also championed a new method of investigative journalism, steeped in the discipline's traditions of truth and responsibility. Combining this method with quality design, our journalists expose corruption and subversion in U.S. politics, and other important issues. Our investigative infographics have included:

- Illegal Spying on President Trump
- Hillary Clinton and the Uranium One Deal
- China's Military Expansion Into Space
- The Secret Propaganda War on Our Minds
- Spygate: The True Story of Collusion
- Clinton Foundation 'Pay to Play' Model Under Investigation

TheEpochTimes.com/about-us