

WEEK 31, 2020

THE EPOCH TIMES

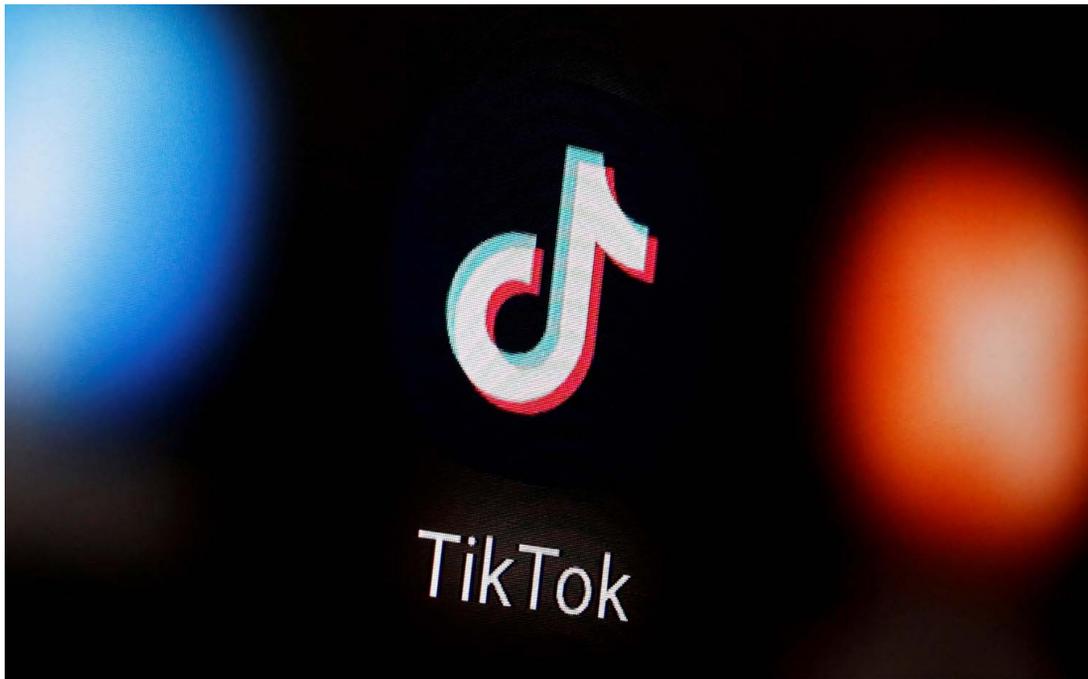
# CHINA INSIDER



## ‘MISSION OF OUR TIME’

US CALLS ON FREE WORLD TO  
DEFEND AGAINST THE CHINESE  
COMMUNIST THREAT

See Page 6



A TikTok logo displayed on a smartphone on Jan. 6, 2020.

## ESPIONAGE

# TikTok Is Spyware for the Chinese Regime, Cyber Experts Warn

CATHY HE

**T**ikTok, the short-video app used by millions of mostly young Americans, cannot be trusted due to its links to the Chinese regime and should be banned, cybersecurity experts warned.

The app, owned by Beijing-based internet giant Bytedance Technology Co., has come under intense scrutiny after the Trump administration confirmed that it was mulling a ban on TikTok and other Chinese apps' U.S. operations on security grounds. Critics warn that the app could be used as a spying tool for the Chinese Communist Party (CCP), and users' content could be censored if the Party deems them politically sensitive.

The company has denied these claims and sought to distance itself from its Beijing owner, pointing to its American board members and new chief executive. It says its servers are located in the United States and Singapore, and that it would not share user data with the Chinese regime if requested.

**Not to Be Trusted**

Chinese security laws compel companies to cooperate with intelligence agencies when asked.

Casey Fleming, CEO of intelligence and security strategy firm BlackOps Partners, described TikTok's claim that it could simply refuse to comply with such laws as "propaganda and gaslighting."

Every Chinese company, citizen, and even U.S. companies operating in China are required to abide by local intelligence and security laws, he told The Epoch Times.

Fleming said Americans commonly make this mistake when viewing the Chinese regime: "We believe China is the same as the U.S. or the free world. We believe that their intentions and goals are the same." But this "could not be more wrong," he said. The CCP has a handle on every aspect of society in China, and is engaged in a program of "unrestricted warfare" to supplant the United States to become the world's sole superpower, according to Fleming.

"All technology coming out of China—either manufactured in China, created in China—is controlled by the CCP," he said.

Mark Grabowski, an associate professor specializing in cyber law and digital ethics at Adelphi University, described TikTok as "Chinese government malware masquerading as a social media app."

He noted that the app's privacy policy is expansive, allowing it to collect and access vast swathes of information on a user's phone. It collects a range of data including a user's web browsing history, geolocation data, and what other apps a user is running.

"The app collects way more data than it needs to," Grabowski said in an email. "For example, it's odd that TikTok does GPS [Global Positioning System] tracking since TikTok videos don't display location information."

**If you want to spy on a country, why send in a spy the old-fashioned way? Why not just send in a great app and make it go viral?**

Gary Miliefsky, cybersecurity expert and publisher of Cyber Defense Magazine

Gary Miliefsky, a cybersecurity expert and publisher of Cyber Defense Magazine, agreed: "When I look at the features of TikTok, I would say that they don't need all those permissions."

In 2014, Miliefsky discovered that many of the top mobile flashlight apps in the Google Play store were designed by cybercriminals or linked to China and Russia. In the case of one of those apps, he found that it was turning on the user's microphone and connecting to servers in Beijing. Miliefsky believes TikTok is a scaled-up version of these flashlight apps: "It is probably a very robust piece of spyware."

"If you want to spy on a country, why send in a spy the old-fashioned way? Why not just send in a great app and make it go viral?" he told The Epoch Times.

TikTok did not respond to a request for comment about security concerns.

**Growing Opposition**

Governments and organizations have started taking action against the app.

India in June banned TikTok and 58 other Chinese apps, saying they posed threats to the country's "security and sovereignty." The Pentagon last December ordered military personnel to delete TikTok from government devices. U.S. lawmakers in March introduced a bill to bar federal employees from using the app on government-issued phones.

Wells Fargo recently instructed employees to remove TikTok, while the Democratic and Republican national committees have warned their staff against using the app.

Meanwhile, a U.S. panel is conducting a national security review of ByteDance's \$1 billion acquisition of social media app Musical.ly—which was rebranded to TikTok—in 2017.

In 2019, TikTok paid a \$5.7 million fine to settle U.S. government charges that it had illegally collected personal information from users under the age of 13 in violation of child privacy laws. Federal agencies are currently looking into whether the company has complied with this agreement, according to Reuters. South Korea recently fined TikTok over similar privacy breaches.

Elements of activist hacking group Anonymous also recently turned its attention on the social media app. A Twitter account linked to the group posted on July 1: "Delete TikTok now; if you know someone that is using it, explain to them that it is essentially malware operated by the Chinese government running a massive spying operation."

The tweet shared a Reddit post by an engineer who claimed to have reverse-engineered the app and found that it was collecting an enormous amount of personal information—much more than other social media apps like Facebook and Twitter—and went to great lengths to hide this. This information has not been confirmed by security researchers. The Reddit user "bangorlol" has since created a subreddit

to share data for independent researchers to investigate.

A report by security research firm Penetration found that the app does an "excessive amount of data harvesting."

"From our understanding and our analysis it seems that TikTok does an excessive amount of tracking on its users, and that the data collected is partially if not fully stored on Chinese servers with the ISP [internet service provider] Alibaba," the report said. Alibaba is a major internet company in China.

Recently, TikTok users ran an iPhone software that lets them know when an app is collecting their data, and found that TikTok was copying their keystrokes every few seconds. The company said it was actually an "anti-spam" feature and issued an update removing it. Back in March, it was caught by security researchers doing the same thing, and had said it would stop the practice within "a few weeks."

**Feeding Big Data**

Fleming said that personal data collected by TikTok and other Chinese apps is being "absorbed into big data and scraped with artificial intelligence by the CCP." This massive pool of information can then be tapped into to carry out economic or political espionage, he said.

In recent years, the regime has stolen huge amounts of Americans' personal data.

In 2014, Chinese hackers stole from the U.S. Office of Personnel Management sensitive personal information detailed in the security clearances of millions of current and former federal employees. That same year, Chinese hackers breached Anthem Inc., a health insurance company, to steal the personal records of 80 million people. This year, four Chinese military officers were indicted for the 2014 hack of credit-reporting agency Equifax, which resulted in the theft of 145 million Americans' financial records.

Grabowski said among the tens of millions of young TikTok users in America, many are targets that the CCP is keen to spy on or exploit for blackmail. These include "congressional staffers, Silicon Valley engineers, research lab assistants and journalists," he said.

"They potentially have access to sensitive government, industry and R&D information—and so does TikTok by extension," Grabowski added.

Fleming said that TikTok as well as any other Chinese-developed app—such as video conferencing app Zoom, a U.S. company whose software is developed in China—should be banned in the United States.

Citing the Chinese regime's actions over the past six months, including its coverup of the CCP virus outbreak, implementation of a draconian security law in Hong Kong, and growing aggression in the South China Sea and towards Taiwan, Fleming posed the question: "Do these actions speak to you as a trusted technology partner?"

## ANALYSIS

# Could TikTok Investors Be Mulling a US Buyout of Chinese App?

FAN YU

**News Analysis**  
Investors in Chinese startup ByteDance Technology Co. are watching with increasing concern as countries around the world are closely scrutinizing the company's popular social-video app TikTok because of security and intelligence concerns.

TikTok, an app popular with teenagers to share user-created short videos, has come under fire for its potential as an espionage tool for the Chinese Communist Party (CCP). While ByteDance has frequently denied that it would hand such information to the CCP, TikTok has been banned by India, while companies including Wells Fargo have warned their employees about installing the app on company-issued smartphones.

The app company has repeatedly sought to distance itself from Beijing, pointing to its U.S. board members, the segregation of data, and the recent appointment of former Walt Disney Co. executive Kevin Mayer as TikTok's CEO. Earlier this year, TikTok reportedly held discussions with the UK government about relocating its headquarters to London as part of TikTok's strategy to convince foreign governments of its independence from the communist regime; London is one of a handful of cities under consideration.

But security concerns related to TikTok are real, and such public platitudes are unlikely to convince governments to permit widespread usage of the app. A former internet censor in China recently told The Epoch Times that he was once interviewed by ByteDance for the role of monitoring and censoring videos posted by TikTok users.

Assuming that company executives are truly set against sharing data with the CCP, it's still not up to them. Every Chinese company, public or private, government-owned or non-government-owned, is required to abide by the CCP's intelligence, censorship, and security laws.

In a much more widely reported case of TikTok kowtowing to the CCP, ByteDance founder Zhang Yiming had to issue a letter of self-criticism in 2018 after running afoul of Chinese internet content censors.

"Our product took the wrong path,

**Assuming that company executives are truly set against sharing data with the CCP, it's still not up to them. Every Chinese company, public or private, government-owned or non-government-owned, is required to abide by the CCP's intelligence, censorship, and security laws.**

and content appeared that was incommensurate with socialist core values," Zhang wrote at the time.

**Massive Value Destruction**

The Trump administration is considering a ban on TikTok in the United States—a move that would threaten the app's future growth and perhaps its existence. It's enough of a threat that could cause existing ByteDance investors to debate options to ring-fence the app and save its value.

ByteDance is a private technology startup with some powerful and influential investors. In its latest fundraising round in 2018, it raised money from Japanese conglomerate SoftBank Group and U.S. private equity firms KKR and General Atlantic. That round valued ByteDance at \$75 billion.

The company's most recent valuation is reported to be as high as \$100 billion, according to the South China Morning Post, citing people familiar with the most recent private share transactions.

That's a staggering valuation. But consider this: TikTok has 800 million estimated average monthly users, and the app was downloaded more than 738 million times in 2019, according to the website BusinessofApps. In the United States, it was downloaded more than 46 million times in 2019.

The app has been downloaded 2 billion times globally and 165 million times in the United States, according to Caixin, citing data from Senso Tower.

Those are all metrics that support TikTok's popularity and its supposed economic value. Politics and security concerns aside, TikTok has an established platform with user-generated content that is valuable to advertisers.

But ByteDance investors can only fully realize that value if the app continues to grow, adds users, and eventually goes public, or is bought out.

**A US Buyout to Save the App?**

But the increasing worldwide scrutiny, due to the app's Chinese background and association with the CCP, is a grave threat to achieving those lofty goals, and a U.S. ban would be catastrophic. That's why ByteDance has spent \$500,000 in the second quarter of 2020 on lobbying efforts

in Washington, according to the firm's lobbying disclosure reviewed by Bloomberg.

Investors are mobilizing to save TikTok from getting the Huawei treatment, which would instantly destroy the company's value.

According to technology industry website The Information, certain U.S.-based investors are actively discussing a buyout of the TikTok app from ByteDance. Investors including venture capital firm Sequoia Capital and existing investor General Atlantic have held discussions with the U.S. Department of Treasury (which oversees the Committee on Foreign Investment in the United States) and other federal regulators about the future ownership, data, and technology requirements that would satisfy federal government concerns about the app.

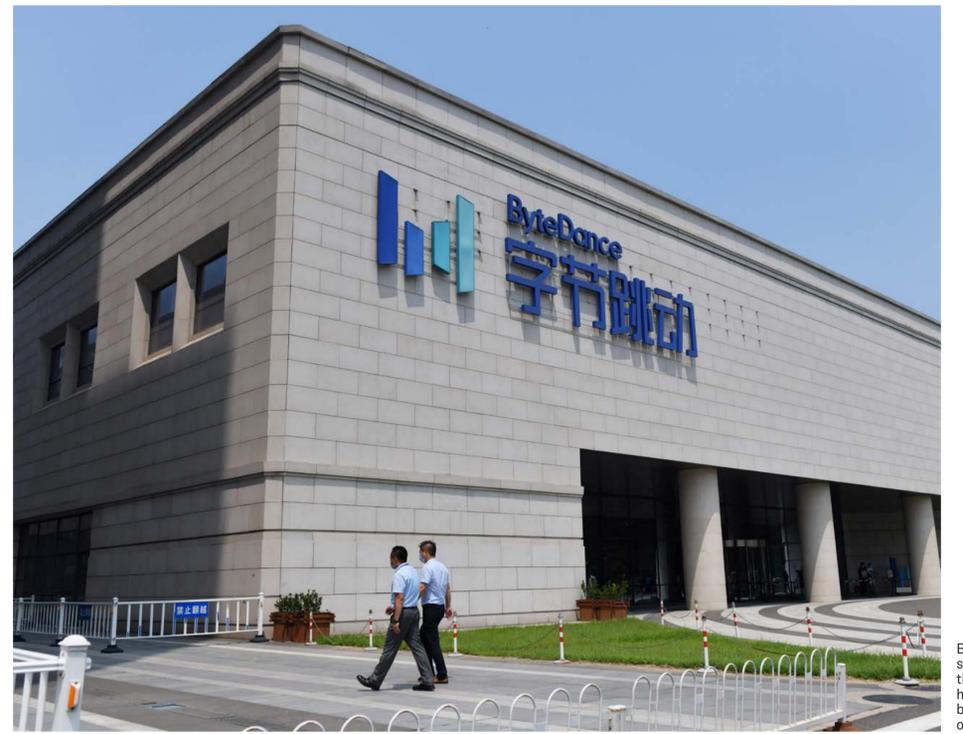
ByteDance also appears to be preparing for an eventual divesting of TikTok. Alex Zhu, the former CEO of TikTok, has been tasked by the parent company to scour for new technology investments, according to a CNBC report. ByteDance's most recent acquisition was a deal in May to purchase Baikemy.com, a health content website. In this sense, ByteDance may view itself as TikTok's parent company but as a holding company for startup assets, of which TikTok is a portfolio company that may eventually exit.

A deal for TikTok wouldn't be easy to pull off; the parties would have to thread the needle on a valuation that would be palatable to existing ByteDance investors as well as presenting enough future upside for its new owners. And without the crown jewel of TikTok, would existing ByteDance investors stick around?

Regardless, a U.S.-led buyout to ring-fence TikTok away from ByteDance could work—assuming the U.S. government could get comfortable with the app, for example, after its code is scrubbed to ensure zero access of the app from CCP or Chinese sources.

It may be the most constructive scenario for all parties. Existing ByteDance investors would be paid out, its users would have greater assurance that they aren't spied on by the CCP, and it would allow TikTok to continue its growth.

GREG BAKER/AFP VIA GETTY IMAGES



ByteDance staff walk past the ByteDance headquarters building in Beijing on July 8, 2020.

## SURVEILLANCE

# Leaked Government Documents Reveal How Chinese Regime Closely Monitors Falun Gong Adherents

GU QING'ER

21 years ago, the Chinese Communist Party (CCP) began its brutal persecution of Falun Gong and has not let up since. The Epoch Times obtained a series of internal government documents revealing how the Chinese regime has targeted Falun Gong practitioners over the years, and during the recent pandemic.

A meditative practice involving slow-moving exercises and moral teachings, Falun Gong quickly grew in popularity, to roughly 100 million adherents by 1999, according to official estimates at the time. Then-Party leader Jiang Zemin considered the group's popularity a threat to the atheist regime's rule, and in July 1999, launched a nationwide campaign to round up and throw practitioners into prisons, labor camps, and psychiatric wards in an attempt to coerce them into renouncing their faith.

Millions of adherents have been detained, with hundreds of thousands tortured, according to estimates by the Falun Dafa Information Center.

Thousands have since died under torture, according to Minghui.org, a U.S.-based website that documents the persecution in China.

## A Key Target to Be Contained

One document dated 2015, listed local key targets in the Rulin Sub-district of Beijing. Ahead of a world conference on the potato industry, two staff in the local government were assigned to monitor a Falun Gong practitioner surnamed Zhang, a resident of Shenfan Garden apartment complex. The names and contact phone numbers of the two staff were listed. Falun Gong was listed as a category to be monitored and the risk level classified as "unconventional."

In a separate document, authorities later increased the number of staff to monitor the same Falun Gong practitioner, to four staff.

Another document listed "key

targets" of the Shenfan Garden apartment complex. Falun Gong practitioners were placed in a category alongside other targets such as mental illness patients, people serving prison terms, people under criminal justice supervision, released inmates, petitioners (people who appeal their grievances to the government), and migrants. According to the document, 20 personnel take shifts to monitor the residential complex, with six assigned to supervise the key targets.

## Tightened Surveillance on Important Days

The Epoch Times also obtained an internal notice issued by a district-level Political and Legal Affairs Commission (PLAC) of Beijing on Aug. 30, 2019. The PLAC is a Party agency that oversees security apparatuses, such as local prisons, courts, and police. Local PLAC offices are often tasked with carrying out the persecution of Falun Gong practitioners.

This document from Mentougou district mandated 24-hour full coverage on the streets for the days of Sept. 30, Oct. 1, and Oct. 2, when the Party celebrated the 70th anniversary of its takeover of China.

The notice listed Falun Gong adherents as one group to be monitored and controlled during that period.

Another document recorded a Falun Gong practitioner surnamed Che was being followed by six assigned personnel in the Rulin area during the Two Sessions in 2017. The "Two Sessions" is an annual meeting of the CCP's rubber-stamp legislature and its advisory body to enact policies and agendas.

The Party's 19th National Congress was held in Beijing from Oct. 18 to 24, 2017. The conclave takes place once every five years, to determine the next succession of Party leaders.

A document regarding a "security work plan" during the meeting was issued by the Rulin local government on Sept. 22, 2017. The

plan was deployed by the Ministry of Public Security (police) from August to October that year. It required that communities in Rulin fully cooperate by implementing strict control tactics such as "knocking on doors" and having "multiple stalkers on one target." Daily meetings and discussion were required.

Since February 2017, Chinese police carried out a "knocking on doors" directive to harass Falun Gong practitioners, according to Minghui.org. This occurred in 28 provinces and regions. Local police would collect personal information by taking pictures, monitoring practitioners, and forcibly videotaping them. Falun Gong practitioners were sometimes abducted or had their homes ransacked.

## Surveillance in the Name of Pandemic

Most recently, on June 18, a set of documents from the "Safe Construction Office" of Changping district, Beijing revealed that authorities were targeting Falun Gong practitioners during the pandemic.

In the first half of 2020, the office issued notices to prevent Falun Gong from "doing investigations or inquiries" about the local pandemic; prevent "infiltration" from Falun Gong practitioners, stop practitioners from "exploiting the pandemic for reverse propaganda," according to the documents.

The report also explained that, during the Two Sessions held this year in late May, every "key target" Falun Gong practitioner was monitored by six personnel on a 24-hour watch, including two cadres in the neighborhood and practitioner's family members, to ensure the practitioner is closely monitored at home and outside the house.

According to the report, the Chengnan sub-district of Changping organized two teams to monitor local Falun Gong practitioners. One consists of 21 specialist cadres and the other 30 full-time patrolmen.

# American Companies Shouldn't Aid Communist China in Religious Suppression: Experts

EVA FU

U.S. companies should know what values they stand for and stop supplying technologies to an authoritarian Chinese regime that is increasingly using surveillance to suppress religions, Gary Bauer, commissioner at the U.S. Commission on International Religious Freedom, told The Epoch Times.

"Tech companies need to remember that they are American tech companies. And they should be sensitive to the values that we stand for," he said in an interview. "When we see some of these companies willing to cooperate with a communist authority, it's not acceptable."

Experts at a July 22 online hearing hosted by the commission described a dystopian surveillance state under Chinese communist rule, where authorities deploy high-tech cameras, facial recognition, phone apps, GPS tracking, and DNA collection to spy on and suppress religious communities.

A popular underground church in Beijing was shut down for refusing to install security cameras inside. In Tibet, people have been arrested for sharing photos of the Tibetan Buddhist spiritual leader Dalai Lama on social media. Most recently, the regime has imposed a national security law on Hong Kong, which empowers officials to censor online content and intercept communications, prompting fears among local faith groups of mainland-style persecution.

"No authoritarian state has leveraged digital technologies more successfully than modern China," said Chris Meserole of Washington-based think tank Brookings Institution during the hearing. "For religious groups targeted by the CCP [Chinese Communist Party], the result has been as devastating as it is tragic."

Some U.S. companies have played a part in fueling the regime's surveillance industry or complying with its censorship.



Surveillance cameras in Hangzhou, in east China's Zhejiang Province on May 29, 2019.

Apple, for instance, has removed or rejected thousands of apps from the Chinese version of its App Store at the behest of the Chinese regime, despite the company's recent call for a "more just world for everyone," noted Lob-sang Sither, a Tibetan-in-exile who heads the digital security program at the Tibet Action Institute, a human rights advocacy group.

**Tech companies need to remember that they are American tech companies. And they should be sensitive to the values that we stand for.**

**Commissioner**

Gary Bauer, commissioner, U.S. Commission on International Religious Freedom

Tech giants such as Intel and Nvidia have sold artificial-intelligence chips to surveillance equipment maker Hikvision, one of nearly 50 Chinese companies on a U.S. sanctions list for

their involvement in human rights violations in China's far-western region of Xinjiang, according to a November 2019 report by the Congressional-Executive Commission on China. Chinese authorities have detained an estimated 1 million Uyghurs and other Muslim minorities inside concentration camps, under the banner of combating "religious extremism."

The California State Teachers' Retirement System, the second-largest pension fund in the United States, owned about \$24.4 million worth of shares in Hikvision as of June 30, 2018.

In May this year, the U.S. administration blocked further investment by U.S. federal retirement funds into Chinese equities, citing "present significant national security and humanitarian concerns."

In a July 16 speech highlighting communist regime's threat to U.S. freedoms, Attorney General William Barr had similarly called out corporate America for "kowtowing" to Beijing, saying Hollywood and U.S. tech firms have been too eager to access the Chinese market and thus "allowed themselves to become pawns of Chi-

nese influence."

"For the sake of short-term profits, American companies have succumbed to [Chinese] influence, even at the expense of freedom and openness in the United States," he said.

For multinational companies that are already facing scrutiny, it's time to step back and reassess their stakes in China, said Bauer.

"If they're concerned about their brand, they need to understand that if it becomes obvious that they're cooperating with the Chinese communists to oppress, discriminate against people, that that is going to hurt their brand and their profits a lot more than if they irritate the Chinese Communist government," he said.

The proliferation of China's intrusive surveillance technology—already used in over 80 countries worldwide—has become difficult to ignore during the current virus pandemic, as Beijing began actively exporting its "health surveillance" software in the name of tracing virus patients, said Sheena Greitens, an associate professor in public affairs at the University of Texas at Austin.

Global regulations on the use and export of Chinese-manufactured surveillance tools are sparse, if any, with Chinese companies largely writing the rules, said Greitens. Left unchecked, such developments could further bolster global reliance on Chinese technology and normalize mass high-tech monitoring, especially in countries where civil liberties are already at risk, she added.

On July 21, the U.S. Senate Foreign Relations Committee issued a report decrying Beijing's concerted campaign to export its "digital authoritarianism," which, according to UC Berkeley researcher Xiao Qiang, has "created systemic competition with the United States and other democracies."

"At its core, this competition is over the value of basic human freedom and dignity," said Xiao during an online forum unveiling the report.

## FLOODS

# Thousands Trapped as Chinese Authorities Discharge Stormwaters Into Villages, Submerging Them

NICOLE HAO

To ensure that cities are not inundated by floodwaters, local authorities in central China have begun discharging excess rainwater accumulating in rivers and reservoirs into rural areas.

Farmland and houses across Jiangxi, Hunan, Anhui, and Hubei provinces were submerged in recent days.

Many flood victims were without shelter. They set up tents in elevated areas and prayed for survival.

Locals told The Epoch Times that in some cases, authorities gave them only a few hours to evacuate, so they only had a chance to take some clothing and a few valuables that were portable.

The Chinese regime has not released any figures on how many people's homes were destroyed due to the discharged water.

The Mengwa region of Anhui offers a window into what happened in the Chinese countryside.

The region, which is home to 195,000 residents, became submerged within hours after the Wangjia Dam in Funan County, Fuyang City, discharged water from the Huai River.

## State Propaganda

Recent state media coverage of China's severe flooding empha-



Firefighters are patrolling with boats at a flooded area near the Yangtze River in Zhenjiang, in China's eastern Jiangsu Province on July 20, 2020.

sized that the country has roughly 100 regions designated as "flood storage" areas, meaning, they are prone to flooding due to their low elevation and proximity to tumultuous rivers.

China's State Council made this distinction back in August 2012, noting that local governments would be allowed to discharge floodwater to these "flood stor-

age" regions when needed.

State media reports claimed that it was inevitable that residents in these areas would encounter flooding. "Storing the floods means you need to open your door and let the flood enter your house. The homes of hundreds of thousands of Anhui people have been submerged," a TV anchor from Anhui said during a

news program.

The anchor "praised" Anhui people for "saving the country" by sacrificing their homes and property.

## Ocean on Land

Xiao You, director of the Huai River commission within China's Water Resources Ministry, told state-run media Xinhua on July 23 that the Wangjia Dam was closed that day, after it had discharged water for over 76 hours. But authorities could open up the dam again in the future if the river's water level again rises due to heavy rainfall.

Xiao made no mention of what authorities would do to provide relief to the flooding victims.

In Guzhen township in Liu'an, Anhui, people told the Chinese-language Epoch Times that they were still stranded, as stormwaters had not receded in three days. "It is like a ghost town now," said Liu Gang, a business owner in Guzhen, in a July 22 phone interview.

Liu said several of his neighbors were missing, believed to have been washed away by the flood. Authorities cut off water and electricity, while the town accumulated flooded trash and mud.

"It's scary. The thieves went from house to house to steal things. Nobody is helping you," said Liu. He said thieves also broke into a local jewelry shop.

The flooding came unexpectedly because authorities suddenly discharged water from local reservoirs—leaving people with no time to prepare, Liu added. Authorities recently discharged more water from two reservoirs close to the town, meaning more flooding could occur.

"I feel that the authorities have abandoned us. They don't want to save us," Liu said.

Gu He is a resident of Dangtu county in Anhui. Gu said the

downtown area was inundated on July 17, while some rural areas were also submerged.

Gu complained that authorities discharged the river water without alerting people.

**Locals told The Epoch Times that in some cases, authorities gave them only a few hours to evacuate, so they only had a chance to take some clothing and a few valuables that were portable.**

Mr. Liu (no relation) operates a grocery store in Zhegao county, located in Chaohu city, Anhui. The county is situated by Chao Lake. On the early morning of July 19, authorities broke its banks and discharged the water to Zhegao, Huailin, and Gaolin towns without advance notice.

"You [officials] should tell us before you discharge the lake, then we can pack our valuable things," Liu criticized.

Liu said that the waters entered the town quickly. The flooding in his store reached 6.56 feet within three hours. He could not move the goods out and suffered at least \$15,000 in damages. A neighbor home improvement store lost about \$700,000.

"If the government gave us three hours, we could have put all the most valuable products on the truck and driven them out," Liu said.

Zhang Yu, a villager in Zhegao, told The Epoch Times a similar story as Liu. "We only had time to save our lives," he said. The water in Zhang's house reached 9.8 feet on July 22, with the first floor fully submerged.



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

# Pompeo Urges Nations to Defend Against Chinese Communist Threat to Freedom

CATHY HE

U.S. Secretary of State Mike Pompeo has implored democracies to work together to defend against expansive threats posed by the Chinese Communist Party (CCP), calling it a choice between “freedom and tyranny.”

“We, the free nations of the world, must induce change in the CCP’s behavior in more creative and assertive ways, because Beijing’s actions threaten our people and our prosperity,” Pompeo said during a speech at the Richard Nixon Presidential Library and Museum in California on July 23.

“The free world must triumph over this new tyranny,” he said, describing it as the “mission of our time.”

Pompeo called on Americans and partner countries to recognize that the CCP is fundamentally a Marxist-Leninist regime, saying the “ideology informs this decades-long desire for global hegemony of Chinese communism.” On this basis, the United States should approach the regime from the standpoint of “distrust and verify,” he said, adapting former President Ronald Reagan’s famous words regarding negotiations with the Soviet Union, “trust, but verify.”

**The truth is that our policies and those of other free nations resurrected China’s failing economy, only to see Beijing bite the international hands that were feeding it.**

U.S. Secretary of State Mike Pompeo

“The only way to truly change Communist China is to act not on the basis of what Chinese leaders say, but how they behave,” he said.

Pompeo’s remarks capped a series of speeches by top administration officials in recent weeks seeking to spotlight the CCP’s malign actions in the United States and around the world. It came as Washington pushes back against the Chinese regime for its technology theft, human rights violations, and military aggression.

This week, the United States, in an unprecedented move, ordered the Chinese Consulate in Houston to close by the afternoon of July 24, with Pompeo



U.S. Secretary of State Mike Pompeo speaks at the Richard Nixon Presidential Library, in Yorba Linda, Calif., on July 23, 2020.

accusing the facility of being a “hub of spying and intellectual property theft.” The Justice Department also confirmed on July 23 that the San Francisco consulate is harboring a wanted Chinese researcher, who’s been charged with failing to disclose in her visa application that she was a member of the Chinese military.

Three other Chinese nationals were recently arrested on similar charges of visa fraud, the department said.

The Justice Department also announced on July 21 an indictment against two Chinese hackers accused of a decade-long campaign to steal trade secrets from defense contractors and hundreds of firms around the world—most recently in an attempt to acquire COVID-19-related research.

“Frankenstein” Pompeo said that in the more than four decades since the United States normal-

ized relations with the CCP, China has not liberalized as many had hoped.

“The truth is that our policies and those of other free nations resurrected China’s failing economy, only to see Beijing bite the international hands that were feeding it,” he said.

“President Nixon once said he feared he had created a Frankenstein by opening the world to the CCP. And here we are.”

Richard Nixon, who was president from 1969 to 1974, paved the way for the

formalizing of U.S. diplomatic relations with the Chinese regime in 1979 by setting up a series of meetings with Chinese officials, including a visit to Beijing in 1972.

**Not a ‘Normal Country’** Pompeo said people and countries “have to tell the truth” about the CCP. “We can’t treat this incarnation of China as a normal country just like any other.”

For instance, in the area of trade, Beijing “treats international ... agreements as suggestions, as conduits for global dominance,” he said.

Doing business with CCP companies also isn’t the same as normal commercial engagements, Pompeo noted, saying these companies “don’t answer to independent boards, and many of them are state-sponsored and so have no need to pursue profits.”

He cited the example of telecom giant Huawei. The administration has called the company “what it is—a true national security threat,” he noted. The United States has raised concerns that Huawei and other Chinese tech firms may be used by Beijing for spying, given that all Chinese companies are beholden to the Party.

“If our companies invest in China, they may wittingly or unwittingly support the Communist Party’s gross human rights violations,” he said.

The administration has blacklisted dozens of Chinese firms over their role in aiding the regime’s repression of ethnic minorities in the region of Xinjiang.

In the same vein, Pompeo said that many Chinese students and employees “come here to steal our intellectual property and to take this back to their country.”

Trump in May barred entry to Chinese graduate and higher-level students affiliated with Chinese military institutions, in an effort to counter the regime’s state-sanctioned theft of American intellectual property.

**Empowering the Chinese People**

The United States must also “engage and empower the Chinese people,” whom Pompeo called a “dynamic, freedom-loving people who are completely distinct from the Chinese Communist Party.”

He said the “biggest lie” the CCP tells is “that they speak for 1.4 billion people who are surveilled, oppressed, and scared to speak out.”

“On the contrary, the CCP fears the Chinese people’s honest opinions more than any foe,” Pompeo said.

He criticized the regime’s suppression of those voicing views unacceptable to the Party, such as dissidents and the whistleblower doctors who sounded the alarm about the CCP virus during the pandemic’s early stages.

“For many decades, our leaders have ignored, downplayed, the words of brave Chinese dissidents that warned us about the nature of the regime we’re facing,” he said.

“We can’t ignore it any longer.”

ESPIONAGE

AP PHOTO/DAVID J. PHILLIP



A firetruck parks outside the Chinese Consulate in Houston on July 22, 2020.

## Houston Chinese Consulate Likely Burned Secret Reports on Spy Operations: Former Chinese Diplomat

CATHY HE

The Chinese consulate in Houston that was recently forced to close likely burned secret documents detailing spy operations and instructions from the Chinese regime’s leadership, according to a former Chinese diplomat.

This week, the Trump administration in an unprecedented move ordered the Chinese consulate in Houston to shut its doors, accusing it of being a “hub of spying and intellectual property theft.”

Local firefighters on Tuesday night responded to public complaints of a fire burning at the Chinese consulate, although they weren’t allowed access to the facility. “It appears to be open burning in a container within the courtyard of the Chinese consulate facility,” Houston fire chief Samuel Samuel Pena told local outlet KTRK on the time.

Chen Yonglin, a former senior diplomat at the Chinese consulate in Sydney, Australia, who defected in 2005, told The Epoch Times the staff was likely burning files on a range of sensitive issues from espionage operations to directives from the Chinese Communist Party’s (CCP) central organs.

**The consulate was of high strategic importance to Beijing, Chen Yonglin said, because of the high-tech sectors that are based in the Houston region, including the aeronautical, biomedical, and petroleum industries.**

He said they would have been destroying documents classified as “secret” or “confidential.” This would include reports from spies within the Chinese community; intelligence reports on overseas bodies critical of Beijing, including persecuted spiritual group Falun Gong; and internal policy documents from central authorities.

These are the kinds of documents that the CCP “would really not be willing” to have released, Chen said. The Chinese regime has a higher classification of “top secret,” he noted, but the circulation of those documents is restricted to top CCP leaders. Those documents were thus unlikely to be housed at the consulate, Chen said.

When Chen defected more than a decade ago, he revealed that the regime had 1,000 spies in Australia. He said that Chinese consulates and

embassies are mandated to influence local officials and elites. They also mobilize overseas Chinese students and members of the Chinese community to advance the CCP’s agenda.

Chen agreed with Senator Marco Rubio’s (R-Fla.) characterization of the Houston consulate as a “central node of the Communist Party’s vast network of spies and influence operations in the United States” following news of the U.S. order.

The consulate was of high strategic importance to Beijing, Chen said, because of the high-tech sectors that are based in the Houston region, including the aeronautical, biomedical, and petroleum industries. Describing the CCP as a “parasite,” Chen said the Party relies on stealing American technology in these advanced fields to fuel its technological and economic growth.

FBI Director Christopher Wray recently said the agency has more than 2,000 investigations across the country linking to China. He described the CCP’s state-sanctioned theft of U.S. technology and trade secrets as being on a scale “so massive that it represents one of the largest transfers of wealth in human history.”

In a briefing on Friday, a senior State Department official said the Houston consulate has been involved in attempts to steal U.S. research into COVID-19 vaccines.

A Justice Department official said that while it’s accepted that all diplomatic missions conduct some level of espionage activity, the operations run out of the Chinese consulate in Houston “went well over the line of what we’re willing to accept.”

According to the New York Times, David R. Stilwell, the State Department’s head for East Asia and the Pacific, said the Houston consulate “has a history of engaging in subversive behavior,” and was the “epicenter” of the Chinese military’s efforts to steal American research.

Citing a law enforcement document, the New York Times reported that FBI investigations implicated the Houston consulate in attempts to steal medical research and other sensitive information from institutions in the area; endeavors to pursue more than 50 researchers and academics to join Chinese recruitment programs designed to facilitate the transfer of sensitive research to Chinese institutions; and coercion of Chinese nationals in the United States who are wanted by the regime.

Stilwell also said the Houston consulate general and two other diplomats were recently caught using false IDs to escort Chinese travelers to a charter flight at George Bush Intercontinental Airport in Houston, Texas, the New York Times reported.

# Killing of 20 Indian Soldiers by China Brings India Closer to US

VENUS UPADHAYAYA

The recent border conflict that resulted in the death of 20 Indian soldiers on the India-China border has changed the region’s power dynamics, according to experts, who say the conflict has made it impossible for India to ever go back to a pro-China narrative, bringing it closer to the United States.

Chandra Mishra, a New Delhi-based former journalist and current political analyst, told The Epoch Times that India has no option left but to seek U.S. support to stand up to Chinese hegemony.

“As PM Modi’s BJP [Bharatiya Janata Party] is a nationalist party, and his main vote bank is based on staunch patriotism, the aggression of China on its border is bound to affect his iconic image in the country, and hence the outcome on the 2024 election,” said Mishra.

This emerging internal political situation, intense anti-China sentiment due to the outbreak of COVID-19 in Wuhan, and the Galwan incident on June 15 that involved the killing of Indian soldiers have had an irreparable impact on the democratic country’s relationship with its communist neighbor.

“It will be difficult for any Indian government, let alone one led by someone who



Congress workers and supporters light candles to pay tribute to the soldiers who lost their lives following a recent clash between India and China, in Kolkata, India, on June 17, 2020.

has talked about making India powerful, to say we can go back to the old policy on China,” said Aparna Pande, director of the Initiative on the Future of India and South Asia at the Hudson Institute. “The key question, however, will be that Delhi will need to think strategically to sustain the economic and military dimensions.”

To prevent further escalation, the militaries of the two countries have created a buffer zone where the bloody conflict took place, and five meetings have taken place between the two countries’ top-level brass, but no resolution has yet been achieved.

“Talks are underway to resolve the border dispute, but to what extent it can be resolved, I cannot guarantee. I can assure you, not one inch of our land can be taken by any power in the world. If a solution can be found by talks, there is nothing better,” said India’s defense minister, Rajnath Singh, while visiting the region on July 17.

**US and India Need Each Other**

China’s increasing aggression on the disputed territory with India was a bullying tactic to prevent India from forming closer relations with the United States, according to experts. With the killing of 20 Indian soldiers, however, it has ended up doing the opposite—bringing India and the United

States closer than ever before.

“China’s continued aggressive behavior, twice in three years, has convinced most people in Delhi that balance between the U.S. and China isn’t the way to go. China may have thought it has taught India a lesson and India will now move away from the U.S., the opposite is what will happen. India is and will further deepen partnerships with the U.S. and Asian allies,” Pande said.

**It will be difficult for any Indian government, let alone one led by someone who has talked about making India powerful, to say we can go back to the old policy on China.**

Aparna Pande, director, Initiative on the Future of India and South Asia at the Hudson Institute

Mishra said India, with its 1.32 billion consumers, is the largest market in the world, unlike China, which isn’t an open market.

“China, being the big brother in the South Asia region, wants to have absolute control over the market here and sees the U.S. as a

threat,” he said while explaining reasons behind China’s bullying tactics on the disputed border.

“This is a critical juncture in world politics when both the U.S. and India need each other. Because, if China is allowed to establish its monopoly in South Asia, it will be strong enough to challenge the global leadership of the U.S.”

Pande said the two countries’ need for each other would translate into the United States helping India to stand up militarily and economically to China in the region, and that alone will be a help to the United States.

“The U.S. can help India by supplying it more defense equipment, more supply parts for defense equipment, defense equipment both for mountainous terrain and the sea and to boost India-U.S. naval collaboration to put pressure on China,” Pande said.

She said, economically, the United States should help India by encouraging companies that are leaving China due to the COVID-19 pandemic to invest in India.

“The United States should boost high tech collaboration and, through partners and agencies like World Bank or International Monetary Fund or Asian Development Bank, help build infrastructure in India and South Asia [instead of China doing so via the Belt and Road Initiative].”



# Bring Home the Magic of Shen Yun!

