WEEK 42, 2021

THE EPOCH TIMES

CHINA INSIDER

CYBER THREAT

CHINA COULD BE EXPLOITING INTERNET SECURITY PROCESS TO STEAL DATA, CYBER EXPERTS WARN

See Page 2

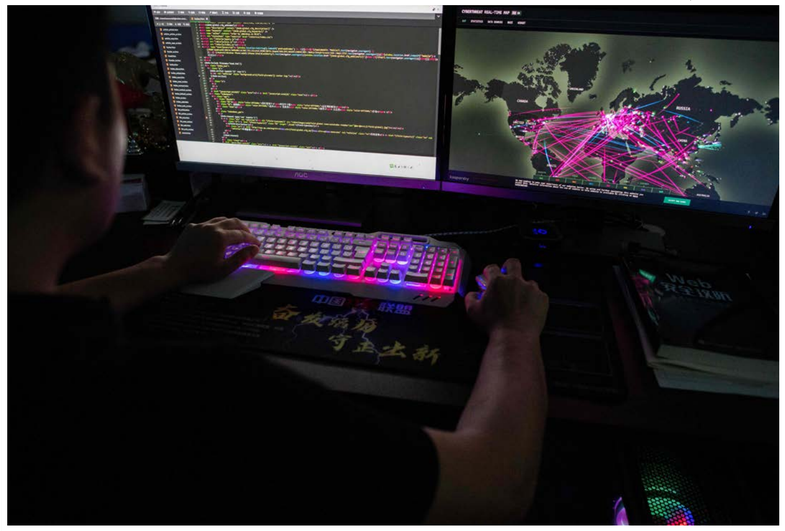
ALL IMAGES BY SHUTTERSTOCK; PHOTO ILLUSTRATION BY THE EPOCH TIMES

CYBERSECURITY

China Could Be Exploiting Internet Security Process to Steal Data, Cyber Experts Warn

J.M. PHELPS

NICOLAS ASFOURI/AFP VIA GETTY IMAGES



A member of the hacking group Red Hacker Alliance views a website that monitors global cyberattacks, at the group's office in Dongguan, Guangdong Province, China, on Aug. 4, 2020.

To access data from unsuspecting users, the Chinese Communist Party (CCP) could be exploiting a universal authentication process that's thought to be secure, but in reality may not be, cybersecurity experts have warned.

While encryption remains the preferred method to secure digital data and protect computers, in some cases, the very digital certificates used for authentication on the internet are allowing the Chinese regime to infiltrate various computer networks and wreak havoc, they said.

Bodies around the world, known as "certificate authorities" (CA), issue digital certificates that verify a digital entity's identity on the internet.

A digital certificate can be compared to a passport or a driver's license, according to Andrew Jenkinson, CEO of cybersecurity firm Cybersec Innovation Partners (CIP) and author of the book "Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyberwarfare."

"Without it, the person or device they are using cannot be according to industry standards, and vital data encryption could be bypassed, leaving what was assumed to be encrypted in plain text form," Jenkinson told The Epoch Times.

Through cryptography, digital certificates are used to encrypt internal and external communications that prevent a hacker, for example, from intercepting and stealing data. But invalid or "rogue certificates" can manipulate the entire encryption process, and as a result, "millions of users have been given a false sense of security," Jenkinson said.

Layers of False Trust

Michael Duren, executive vice president of cybersecurity firm Global Cyber Risk LLC, said that digital certificates are typically issued by trusted CAs, and equal levels of trust are then passed on to intermediate providers. However, there are opportunities for a communist entity, a bad actor, or another untrustworthy entity to issue certificates to other "nefarious folks" that would appear to be trustworthy but aren't, he said.

"When a certificate is issued from a trusted entity, it's going to be trusted," Duren said. "But what the issuer could actually be doing is passing that trust down to someone that shouldn't be trusted."

Duren said he would never trust a Chinese certificate authority for this reason, stating that he's aware of a number of companies that have banned Chinese certificates because they've been issued to entities that can't be trusted.

Jenkinson said that Chinese certificate authorities make up a small proportion of the overall sector, and the certificates they issue are typically confined to Chinese entities and products.

In 2015, certificates issued by the China Internet Network Information Center (CNNIC), the state-run agency that oversees China's domain name registry, were called into question. Google and Mozilla banned CNNIC certificates upon learning of unauthorized digital certificates connected to several domains. Both internet firms objected to the CNNIC delegating its authority to issue certificates to an Egyptian company, which issued the unauthorized certificates.

> A back door means [the Chinese certificate authority] could literally take over administration access and send data back to the mothership.
>
> Andrew Jenkinson, CEO, Cybersec Innovation Partners

According to Jenkinson, the CNNIC certificates were banned because "they had back doors in them."

"A back door means [the Chinese certificate authority] could literally take over administration access and send data back to the mothership," he said.

Since 2016, Mozilla, Google, Apple, and Microsoft have also banned Chinese Certificate Authorities WoSign and its subsidiary StartCom over unacceptable security practices.

> Since 2016, Mozilla, Google, Apple, and Microsoft have also banned Chinese Certificate Authorities WoSign and its subsidiary StartCom over unacceptable security practices.

Security Flaw

Despite these bans on Chinese digital certificates in recent years, the CCP hasn't been deterred and is playing the long game, Jenkinson said.

He pointed to an alarming discovery made by his cybersecurity firm two years ago, affecting a multinational consulting company.

Typically, digital certificates are valid for a couple of years, depending on the certification authority, and renewal is required to keep them valid and the data they're supposed to protect secure, he said.

"But in 2019, CIP Chinese discovered certificates that were in place for 999 years," Jenkinson said.

His firm made this discovery when examining the laptops of a prominent global consulting company.

Jenkinson brought this security flaw to the firm's attention and offered services to secure its computer and customer networks. But the company declined.

"Either they are incredibly complacent, or they are complicit," he said, noting that the company's clients include U.S. government entities.

This multi-billion-dollar company's failure to remedy this issue means that hundreds of thousands of people could be exposed to Chinese infiltration via this firm's lax security, Jenkinson said.

The firm is compromising its customers every time someone uses one of their laptops, he said. For example, companies or clients using the company's services could be held to ransom, have their intellectual property stolen, or be the recipient of malicious codes planted for later use.

This company is "in breach of every regulation of privacy known to man—and they just want to dismiss it," the cybersecurity professional said, particularly pointing to the EU's strict data protection laws.

And if this information were made public, the repercussions would be extensive, Jenkinson said.

"Imagine a waterhole attack or a drive-by attack, one where a cybercriminal can just sit there and easily gain access to capture data without even thinking about it or having to decrypt it—because it's all in plain text [due to a rogue certificate or configuration error]," he said.

For such a large reputable company to choose to not protect their clients is "madness," Jenkinson said.

A 'Slippery Slope'

Economic losses from cybercrimes are far from trending in the right direction, according to Jenkinson.

Global losses from cybercrime exceeded $1 trillion in 2020, according to a report from computer security company McAfee. In 2021, losses are expected to escalate to more than $6 trillion, research firm Cybersecurity Ventures said.

Jenkinson predicts that economic losses will exceed $10 trillion by 2025.

"This will impact every man, woman, and child," he said. "The slippery slope we're on, well, we're greasing it ourselves."

As a start to reversing this trend, "people should not be using CNNIC digital certificates," Jenkinson said.

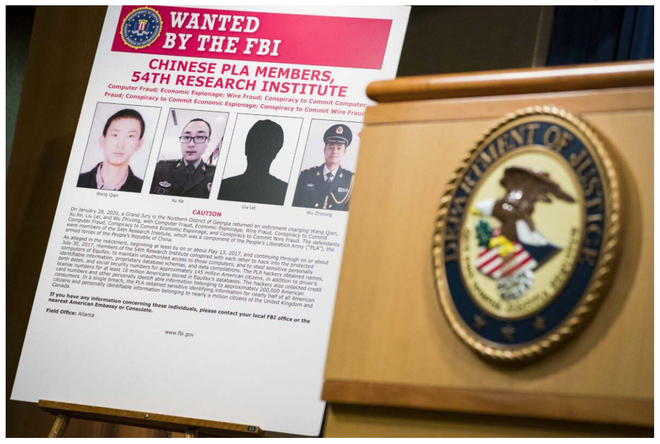
Duren of Global Cyber Risk agreed, saying, "Anything coming out of a state-controlled entity like communist China acting as a certificate authority should not be trusted."

CAs need better controls and oversight, Jenkinson said. "Without this, nobody has any chance of knowing what digital certificates are being used, considering that a standard laptop contains hundreds of thousands of digital certificate instances."

Jenkinson noted that Chinese computer products will predominately use Chinese digital certificates. Therefore, users of such products should be aware that their security could be compromised as a result.

J.M. Phelps is a writer and researcher of both Islamist and Chinese threats.

SARAH SILBIGER/GETTY IMAGES



A sign shows four members of China's military indicted on charges of hacking into Equifax Inc. and stealing data from millions of Americans, at the Department of Justice in Washington on Feb. 10, 2020.

PANDEMIC ORIGINS

COVID-19 Originated From a Chinese Laboratory, Investigative Reporter Says

FRANK FANG & JAN JEKIELEK

JOHANNES EISELE/AFP VIA GETTY IMAGES

A worker is seen inside the P4 laboratory in Wuhan, Hubei Province, China, on Feb. 23, 2017.

Award-winning Australian investigative reporter Sharri Markson says there are convincing pieces of evidence to show that the virus causing the COVID-19 pandemic originated from a Chinese lab with ties to the communist regime's military.

Markson's findings are published in her new book, "What Really Happened in Wuhan," and evidence suggests that Beijing knew about the virus months before the onset of the pandemic.

"I think the evidence quite clearly points to a leak at the Wuhan Institute of Virology, either in mid-September or at least that's when the Wuhan Institute of Virology became aware of it ... and then after that, there was a deliberate decision by Chinese authorities to cover this up," she said in a recent interview with EpochTV's "American Thought Leaders."

The Chinese regime has vehemently denied that the CCP (Chinese Communist Party) virus, the pathogen that causes COVID-19, escaped from the Wuhan Institute of Virology (WIV), despite evidence pointing to it. The institute has been doing research on bat coronaviruses for more than a decade, and it's located a short drive from a local market in Wuhan, Hubei province, where the first cluster of infection cases emerged.

More importantly, a fact sheet released by the U.S. State Department in January stated that several researchers at the WIV fell ill with COVID-19-like symptoms in autumn 2019.

Markson said she presented more evidence implicating the WIV in her book, including how a database containing 22,000 viruses at the institute was "taken offline mysteriously" for the first time on Sept. 12, 2019—three months before China warned that the virus was contagious.

On the same day, the WIV issued a tender to upgrade its security, Markson said. During the ensuing weeks, the institute went on a spending spree, paying $500,000 to boost its security, including the purchase of new CCTV systems and the hiring of new guards.

Eventually, the purchases also included a new air ventilation system, a medical air incinerator, and a coronavirus testing PCR (polymerase chain reaction) machine, according to Markson.

It turned out that China was buying significantly more PCR equipment in Hubei province in 2019 compared to years earlier, according to a recent report by Australia-based cybersecurity company Internet 2.0. About 67.4 million yuan (about $10.5 million) was spent on PCR equipment in 2019, an increase of about 83 percent compared to the total in 2018.

"We assess with high confidence that the pandemic began much earlier than China informed the WHO [World Health Organization] about COVID-19," the report reads.

> We were given this false impression that there was a scientific consensus that this was a natural virus.
>
> Sharri Markson, author of "What Really Happened in Wuhan"

"And then there's the evidence that followed about Gen. Chen Wei," Markson said. "She was the leading army official who went in and took over the Wuhan Institute of Virology, the gag order, and the fact that [Chinese leader] Xi Jinping then issued a new bio-security law. So, there's a lot of other evidence that points to a laboratory leak as well."

The bio-security law was fast-tracked—the legislation was adopted in October 2020, eight months after it was proposed by Xi. The law went into effect in April.

Narrative on Virus Origins

Markson said people were very much misled in 2020 about the origins of the virus. China's narrative—that the virus had a natural origin—took hold "at the expense of finding out the truth."

"We were given this false impression that there was a scientific consensus that this was a natural virus," she said. "We were told in that Lancet letter that it was a conspiracy to suggest this was a lab leak. As it turned out, many of the scientists behind that letter were incredibly conflicted."

On Feb. 19, 2020—less than a month after the United States reported its first local COVID-19 case in the state of Washington—27 scientists issued a joint statement published in the medical journal The Lancet.

"We stand together to strongly condemn conspiracy theories suggesting that COVID-19 does not have a natural origin," the letter reads.

However, it emerged that one of the 27 scientists had a conflict of interest. In June, The Lancet updated the letter, naming Peter Daszak for failing to disclose "competing interests," a requirement under the International Committee of Medical Journal Editors.

Daszak's organization, EcoHealth Alliance, a New York-based nonprofit research foundation, received millions of dollars in grants from the National Institute of Allergy and Infectious Diseases (NIAID), with some of that money being sent to the WIV.

> When I was writing the book, there had been this unbelievable censorship of science.
>
> Sharri Markson, author of "What Really Happened in Wuhan"

Before The Lancet made the update, it came to light that EcoHealth had been working with Chinese scientists for more than 15 years, and the nonprofit received Chinese funding.

In contrast, scientific research that went against China's narrative on the virus's origins was being rejected, Markson said, pointing to how Australian immunologist Nikolai Petrovsky had trouble getting his work published.

"When he couldn't get his paper published, even preprint servers were knocking it back, Markson said. "Preprint servers are designed to get science out into the world while it's being peer-reviewed. Even they were knocking it back.

"For me at the time, when I was writing the book, there had been this unbelievable censorship of science."

Petrovsky, a professor at Australia's Flinders University, eventually published his work on the ArXiv preprint server. The research has since been peer-reviewed and published in the Nature journal Scientific Reports. Using computer modeling, his research found that the spike protein in the CCP virus can bind more tightly to a protein called ACE2 on human cells than on the same protein on other tested species, including bats and pangolins.

"This argues against the virus being transmitted directly from bats to humans. Hence, if the virus has a natural source, it could only have come to humans via an intermediary species which has yet to be found," Petrovsky said in a statement.

Moving forward, Markson suggested that there should be a credible body other than the World Health Organization to probe the origins of the virus. She recommended either a presidential commission or a bipartisan congressional inquiry.

"There are very clear avenues to pursue here, even if China refuses to cooperate, and there's no sign that the Communist Party regime is going to suddenly become transparent," she said.

Frank Fang is a Taiwan-based journalist. He covers news in China and Taiwan. He holds a master's degree in materials science from Tsinghua University in Taiwan.

Jan Jekielek is a senior editor with The Epoch Times and host of the show, "American Thought Leaders." His career has spanned academia, media, and international human rights work. In 2009 he joined The Epoch Times full time and has served in a variety of roles, including as website chief editor. He is the producer of the award-winning Holocaust documentary film "Finding Manny."

HECTOR RETAMAL/AFP VIA GETTY IMAGES

Passengers wearing masks arrive at Shanghai Pudong International Airport in Shanghai on March 19, 2020.

KEVIN FRAYER/GETTY IMAGES

A display for facial recognition and artificial intelligence is seen on monitors at Huawei's Bantian campus in Shenzhen, China, on April 26, 2019.

TECH WAR

CCP Poses 'Insider Threat' to American Companies: Former Pentagon Official

ANDREW THORNEBROOKE & JAN JEKIELEK

A former Pentagon official has warned that the Chinese Communist Party is sending people to infiltrate American businesses. In addition, the Department of Defense needs to do a better job of working with the tech industry to prevent China from achieving dominance in the field of artificial intelligence, the former official said.

"The fact is, the Chinese Communist Party is really sending a lot of people to our universities and to our most innovative companies," said Nicolas Chaillan, the former chief software officer for the U.S. Air Force and Space Force. "And there is a very big risk of exfiltration of data from within."

"Insider threat is probably the most underestimated threat of all these top organizations on the commercial side," he added.

The comments were made during an appearance on EpochTV's "American Thought Leaders" program, following Chaillan's highly publicized resignation as the Pentagon's first chief software officer.

Chaillan said that a key issue in mitigating insider threat in the future would be striking a balance between an appropriate amount of caution regarding those with ties to the Chinese regime, while still maintaining America's democratic values.

"It's a real issue, and there's not many solutions," Chaillan said. "You don't want to start saying 'we're not going to allow these people to contribute to society.' We need those talents."

To that end, Chaillan said that a key factor in securing American industry would be working to effectively sever U.S.-based workers' dependency on and ties to the Chinese Communist Party (CCP). Current U.S. policy prohibits the immigration of CCP members to the United States.

"If they're willing to come and make a difference, they can actually be great assets to by providing more insights about their countries," Chaillan said. "So, I think the solution would have to deal with how do we help them bring their families and try to remove these dependencies or these kind of side effects and risks that could be spreading rapidly. You have to be proactive."

"At some point it's a gamble, but there is more risk not doing it sometimes than doing it."

'We're Losing This Battle'

Chaillan also said that the CCP's ability to control China-based companies and leverage their technologies was a key factor in his decision to resign from the DoD.

"China is taking off, leading the pace, by mandating their companies to partner with them," Chaillan said. "That's been a tremendous challenge and, at some point, I had no choice but to raise the alarm because we are seeing that we're losing this battle."

"China is leading right now, they're already leading in many of those fields because of the adoption of the technology from their companies. That's the difference."

Chaillan explained that a lack of transparency between the Pentagon and the private technology sector was driving down the industry's desire to work with government, and that an inability to leverage private sector tech was hamstringing U.S. efforts to compete with China.

"At the end of the day, the U.S. companies are all leading against China, but we [the DoD] do not have access to that technology," Chaillan said. "So that puts us behind because, effectively, we're left not being able to partner and competing at the same time with a massive country with 1.5 billion people that are not waiting for us to wake up."

> Insider threat is probably the most underestimated threat of all these top organizations on the commercial side.
>
> Nicolas Chaillan, former chief software officer, U.S. Air Force and Space Force

US Tech Collaboration With China

That lack of communication and the at times hostile culture towards the military in big tech firms have become something of a problem in recent years.

Perhaps the most notable example of such was when Google opted not to continue a government contract that would have improved the accuracy of drones by leveraging AI and big data, but continued to develop AI resources that were known to benefit the CCP.

The move, and others like it, were roundly criticized as an effective collaboration between the CCP and its military wing, the People's Liberation Army.

Numerous companies including Apple, Google, IBM, and Microsoft all still maintain AI research laboratories in mainland China, where the CCP can leverage national security laws to compel those companies to hand over trade secrets at any time.

JARED CUMMINGS/CONSERVATIVE PARTNERSHIP INSTITUTE

Nicolas Chaillan, former Air Force chief software officer, in Washington on Oct. 13, 2021.

DoD and asking the department to invest more money writing reports."

"We need actions. We need outcomes. We need tangible value to the warfighter."

To that end, Chaillan's time at the Pentagon included developing and deploying a working model for the Joint All-Domain Command and Control (JADC2), an inter-service network that would combine sensors from across the Air Force, Army, Marines, Navy, and Space Force.

The unexpected cancellation of funding for JADC2, which was described as "best of breed" by Air Force officials just months ago, was a key factor in Chaillan's departure from the DoD.

Seizing the Opportunity

Still, though Chaillan believes that the window of opportunity is quickly closing for the United States to avoid losing the AI war with China, he maintained that not all hope was lost.

"I don't believe that we have lost," Chaillan said. "What I said is that if we don't act now, and don't wake up right away, and not in five to 10 years from now like some of the Pentagon reports are saying, but if we don't take a stand now and take action, we have no fighting chance in succeeding 10 to 15 years from now."

"The velocity of adoption of AI compounds over time so, effectively, you're going to be at a situation at some point where you pass the point of no return. You will not be able to catch up."

Accordingly, Chaillan said that the DoD must do more to encourage innovative thinking and risk-taking among its ranks, as well as to increase transparency with its private-sector contractors.

"Well, you know, I think that the issue is there is no reward for taking risks," Chaillan said. "On the commercial side, if you do good you get bonuses, you get credit, right? In the government, it's actually safer not to take [risks], because you have more chance of rising up if you don't make noise, even if you end up having a large program that fails."

"There's no one held accountable when something goes wrong," Chaillan added. "Effectively, when something is going to go wrong, it's going to be most likely classified, and we can't talk about it."

When asked to comment on Chaillan's remarks, the DoD referred The Epoch Times to comments made by press secretary John Kirby during a press conference on Oct. 12.

"[Secretary of Defense Lloyd Austin] was very clear about our concerns about China's desires to advance in this field and he's focused and we still remain focused on advancing AI capabilities in a responsible way, in close partnership with industry and academia and building a digitally talented and capable workforce here for the Department," Kirby said.

"What I can tell you is that we recognize the importance of AI as a technology and as a capability and the Secretary has spoken about this and we have invested quite a bit of effort and energy into making sure that we can advance AI technology in a responsible way."

> China is leading right now, they're already leading in many of those fields because of the adoption of the technology from their companies. That's the difference.
>
> Nicolas Chaillan, former chief software officer, U.S. Air Force and Space Force

Andrew Thornebrooke is a freelance reporter covering China-related issues with a focus on defense and security. He holds a master's in military history from Norwich University and authors the newsletter Quixote Hyperdrive.

Jan Jekielek is a senior editor with The Epoch Times and host of the show, "American Thought Leaders." His career has spanned academia, media, and international human rights work. In 2009 he joined The Epoch Times full time and has served in a variety of roles, including as website chief editor. He is the producer of the award-winning Holocaust documentary film "Finding Manny."

HONG KONG

Hong Kong's Press Freedom Is Under Siege: Former Apple Daily Director

FRANK FANG

Mark Clifford, one of the former independent non-executive directors at Next Digital, told a congressional hearing on Oct. 14 how press freedom is under attack in Hong Kong, as evident by how the Chinese regime has driven Apple Daily to its deathbed.

Apple Daily, which is published by Next Digital, is a Hong Kong newspaper known for publishing voices critical of the Chinese Communist Party (CCP) and voices supportive of the Hong Kong protesters. The paper printed its last edition on June 24, after printing its first edition in 1995.

Clifford said Beijing has broken its promises written in Hong Kong's mini-constitution, known as the Basic Law, and the paper's founder Jimmy Lai has been in prison for "exercising the freedoms that are promised" in that document.

"This has the seal of the People's Republic of China on it, and yet, it's not even really worth the paper that's printed on," Clifford said while holding a copy of the Basic Law in his hand. The hearing, which focused on the current state of civil and political rights in Hong Kong, was co-hosted by Reps. Chris Smith (R-N.J.) and James McGovern (D-Mass.).

The Basic Law protects Hongkongers rights such as freedom of speech and freedom of the press, neither of which is available to Chinese people in mainland China. The rights are guaranteed for at least 50 years under a governance framework called "one country, two systems," which Beijing agreed to implement when it signed the 1984 Sino-British Joint Declaration, a legally binding international treaty.

"What we've seen is that these promises that the Chinese government solemnly made cannot be trusted," Clifford added.

Clifford is currently the president of the advocacy group Committee for Freedom in Hong Kong. He and three other directors resigned from their Next Digital positions in early September, citing a "climate of fear" caused by Hong Kong's draconian national security law.

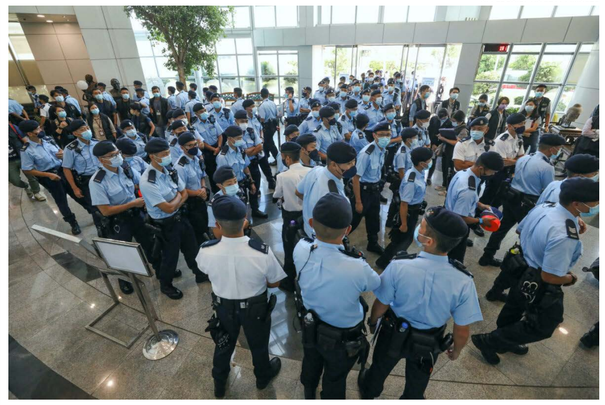
Hong Kong's autonomy and freedoms have been drastically eroded after Beijing imposed the national security law on the city in late June last year. The law criminalizes vaguely defined crimes such as subversion and collusion with foreign forces with a maximum penalty of life imprisonment.

Less than two months later, on Aug. 10, 2020, Lai was arrested and the Apple Daily newsroom was raided by about 200 police officers, drawing international condemnation.

The newsroom was raided again on June 17, when about 500 police officers stormed the paper's headquarters. On the same day, five executives of the paper, including editor-in-chief Ryan Law and chief executive officer Cheung Kim-hung, were arrested. At that time, Lai was already in prison for taking part in unauthorized assemblies in 2019.

> What we've seen is that these promises that the Chinese government solemnly made cannot be trusted.
>
> Mark Clifford, former independent non-executive director, Next Digital

APPLE DAILY VIA GETTY IMAGES



Police officers conduct a raid at the Apple Daily office in Hong Kong on June 17, 2021.

Continued Attack

Clifford told the two congressmen what the Hong Kong police did inside the newsroom during the second raid.

"They ended up pretty much stripping the shelves bare. They questioned journalists about more than 100 different articles that have been written—who wrote it, who edited it, who [was] involved," he said.

As of now, Clifford said there are seven Next Digital employees in jail, awaiting trial on national security charges. Among them is Lai, who is accused of "colluding with foreign forces."

"These trials are in some cases a year or two off; they're just presumed guilty," he added.

Though Apple Daily is not printing papers anymore and its website is down, the Hong Kong government is still investigating the company and its senior staff, according to Clifford.

"We now have four different investigations going against the company and against directors," Clifford said, "trying to blame us for the fact that the company is out of business, when they [Hong Kong government] put us out of business by freezing assets and essentially throwing the senior leadership in jail."

One of the investigations is being carried out by a special inspector appointed by Hong Kong's Financial Secretary. According to Hong Kong media, the inspector raided Next Digital's office on Sept. 28, in an effort to obtain the company's financial records.

Clifford said the Hong Kong authorities went to the banks to freeze Lai's assets and his bank accounts.

The Hong Kong government "told the bankers, including bankers at Citibank, that if anybody touched those accounts, the bankers and anybody did the touching would be subject to seven years in prison. This is pretty heavy-duty stuff."

The sanctions the U.S. government has placed on Hong Kong and Chinese officials for suppressing the city's democracy "have certainly gotten people's attention," Clifford said, but the U.S. government could "cut deeper."

Clifford explained the United States could further stand up for Hong Kong by targeting business interactions, since some work for private companies "under the veneer for the Hong Kong government."

One example named by Clifford was the special inspector investigating Next Digital. The inspector, Clement Chan Kam-wing, is the managing director for assurance of the accounting firm BDO, one of the biggest accounting firms in the world.

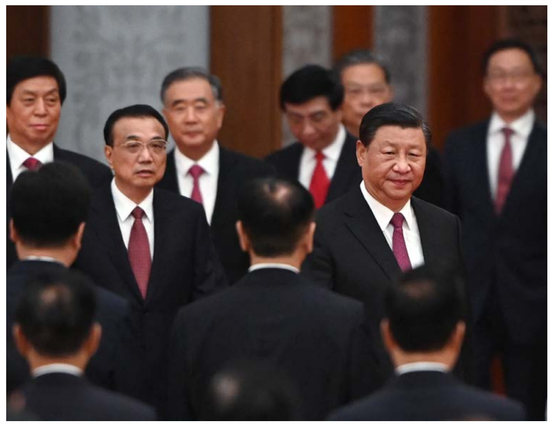
"Do we want to look back, do any of us want to look back later on in our lives and say that we didn't do what we could to stop this, we just let companies pursue short term profit when we could have stopped it as a government," Clifford said.

Frank Fang is a Taiwan-based journalist. He covers news in China and Taiwan. He holds a master's degree in materials science from Tsinghua University in Taiwan.

ANTHONY KWAN/GETTY IMAGES

Supporters hold up placards outside of the Apple Daily newspaper offices in Hong Kong on June 24, 2021.

GREG BAKER/AFP



Chinese leader Xi Jinping (R) arrives with Premier Li Keqiang (L) and members of the Politburo Standing Committee for a reception at the Great Hall of the People in Beijing on the eve of China's National Day on Sept. 30, 2021.

OPINION

What's Behind Beijing's Latest Round of Bank Regulations

FAN YU

Beijing is tightening governance around banks and insurance companies to bar large shareholders from having excessive influence and engaging in unfair dealings.

China wants to rein in financial sector risk and corporate governance. Many of these affiliated deals generated losses or bad debts for banks. But there are other layers to this new round of regulations—a new phase of the anti-corruption campaign waged by CCP regime boss Xi Jinping to root out political dissent.

The new regulations went into effect as of Sept. 30 following an initial draft published in June.

The problem, as explained by the China Banking and Insurance Regulatory Commission (CBIRC) in a FAQ, is that "a small number of major shareholders have abused shareholder rights, improperly interfered with company operations, sought control in violation of regulations, and used affiliated transactions to transfer interests and transfer assets."

In other words, certain powerful individuals affiliated with these institutions have obtained loans or transferred assets illegally, often using non-standard terms and concealing from regulators true beneficiaries behind those transactions.

These are serious issues. Major shareholders should not be able to obtain loans without underwriting, must be engaged in an arms-length manner, and these relationships should be disclosed properly.

This is part of a renewed effort to inspect the country's financial regulators, banks, insurance companies, and asset managers to root out corruption and illicit behavior. Beginning October, the Central Commission for Discipline Inspection, the Party's top anti-graft body, will begin to inspect the CBIRC, China's main banking regulator.

Xi appears to be embarking on another phase of anti-graft, anti-corruption campaign that initially began as soon as his ascension to the top position within the CCP. The years-long campaign has ensnared more than a million CCP cadres, and most recently included the execution of Lai Xiaomin, ex-chairman of China Huarong Asset Management, one of the country's biggest "bad debt" managers.

So what drove this latest round of inspections?

The flip side of recent headlines surrounding property developer Evergrande and other highly indebted companies is the plight facing China's banks and financial institutions who lent to these over-levered companies. If property developers can't sink China's economy, bank failures surely would. Most of these debt transactions were arms-length, albeit ill-advised from a risk perspective. But a small portion of loans was made to entities affiliated with bank insiders and political heavyweights who never intended to repay such loans. The new regulation is looking to combat this dark corner of lending.

It appears that there are still some "bad actors" remaining within China's powerful financial sector, clinging onto corrupt positions and potentially using political power to push back against Xi's policy shift away from the crony pseudo-capitalism policies of the last three decades. That previous policy began with CCP boss Deng Xiaoping and was continued by his successors Jiang Zemin and Hu Jintao, which allowed Party cadres to get rich by any means necessary as long as they follow the CCP boss's orders.

And that is no longer the modus operandi of Xi's regime.

In an expose explaining the CBIRC's moves to limit shareholder power, the mainland Chinese financial magazine Caixin cited a few egregious examples of scandals that could suggest exactly who the rules will target. Caixin is believed to be aligned with Xi and its editorials tend to advocate for and expound upon his economic policies.

The Caixin report specifically states two examples—the failures of Baoshang Bank Ltd. and Anbang Insurance Group—that the new law will target.

Before its bankruptcy last year, Baoshang was the financial war chest of disgraced Chinese oligarch Xiao Jianhua and his investment firm Tomorrow Group, which owned 89 percent of Baoshang. At the time, Baoshang held billions in bad debts and non-performing loans, mostly from affiliated entities within Xiao's financial empire.

Xiao, through a network of companies he controlled, was believed to be a "white glove" for high-ranking CCP cadres and assisted in laundering their corrupt gains abroad. The Epoch Times reported in 2017 that Xiao was being investigated for his close ties to the political faction of former CCP regime boss Jiang Zemin and his close ally Zeng Qinghong, which had dissented against Xi's rule.

The other company named, Anbang Insurance, was also recently disbanded by Beijing after several scandals. Its former chairman and CEO, Wu Xiaohui, was sentenced in 2018 to 18 years in prison on embezzlement and graft charges. Wu was also believed to be a "white glove" in transacting on behalf of CCP officials loyal to Jiang. Beginning in 2014, Anbang had made several high-profile offshore acquisitions including the Waldorf Astoria hotel and Dutch insurer VIVAT.

Tomorrow Group and Anbang are both old news, but the fact that they are dug up as justification for the current slate of regulation is telling. It appears the latest slate of financial regulations is both economically and politically motivated.

Fan Yu is an expert in finance and economics and has contributed analyses on China's economy since 2015.

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

CCP

China's Escalating Military Pressure on Taiwan Poses Challenge to Democracies Everywhere: Experts

ANDREW THORNEBROOKE

JIN DANHUA/XINHUA VIA AP

Two Chinese SU-30 fighter jets take off from an unspecified location to fly a patrol over the South China Sea, in this file photo.

What began earlier this month as a routine display of cross-strait harassment resulted in a record-breaking 149 Chinese warplanes transgressing into Taiwan's air defense identification zone (ADIZ) over the course of four consecutive days, sparking international alarm and outrage.

The incursions, including one incident in which 56 aircraft entered the ADIZ in a single day, were derided by the White House as "destabilizing" and "provocative."

The Chinese Communist Party (CCP), meanwhile, said that the incursions were "necessary" to preserve its sovereignty and territorial integrity over the island, which Beijing claims as its own.

The events marked a new low in cross-strait relations. Experts, however, believe that the show of force is not a signal of imminent attack, but a complex display meant to simultaneously intimidate Taiwan, undermine the island's international relationships, and solidify Xi Jinping's standing within the Chinese Communist Party and its military, the People's Liberation Army (PLA).

Intimidation or Weakness?

John Dotson, deputy director of Washington-based non profit Global Taiwan Institute, told The Epoch Times that the incursions were an intimidation tactic and part of a grander strategy by Beijing to coerce the international community away from the defense of Taiwan.

"The flights into Taiwan's ADIZ are part of a larger intimidation campaign that is also being conducted in the realms of diplomacy and propaganda," Dotson said in an email, "as seen in Xi Jinping's Oct. 9th speech, which condemned Taiwan's government and reasserted the inevitability of Taiwan's 'unification' with China."

Shortly after the incursions, the People's Liberation Army (PLA) also conducted amphibious assault drills across the Taiwan Strait, and CCP General Secretary Xi Jinping delivered a speech calling for the "reunification" of Taiwan with mainland China.

The PLA Daily, China's official military newspaper, followed up with an article that said that the PLA would "crush" any attempts to separate Taiwan from the mainland, though Taiwan has been self-governed since 1949.

Former U.S. Under Secretary of State Keith Krach told The Epoch Times in an email that the rapid escalation of air incursions was designed to simultaneously intimidate the people of Taiwan into abandoning democratic forms of governance and to undermine the island's relationship with the United States following the fall of Afghanistan to the Taliban.

"As the highest-ranking U.S. diplomat to visit Taiwan in four decades, I know what it's like to be greeted by 40 Chinese fighters and bombers," Krach said, referring to his three-day visit to the island last September, during which the regime sent aircraft over the ADIZ on two of those days.

"The escalation of these intrusions is meant to [firstly] intimidate the Taiwanese people, who cherish their democracy, into giving up the will to stand their ground. [And secondly], test the will of the U.S. and free world after Chinese state media openly mocked Taiwan for relying on the US for its defense after the Afghanistan crisis."

Dotson and Krach also said that the incursions belied the current weakness of Xi's position in Beijing, following months of attempts to tighten his personal control over the CCP and PLA, a floundering real estate market, and growing energy crisis.

"Intimidation tactics against Taiwan also serve Xi Jinping's purposes for shoring up his own position within the Communist Party," Dotson said. "Ultimately, that's a more important factor than any of the justifications cited by Beijing."

Krach said, "With the brewing domestic real estate and energy crisis, Xi is weaker than he wants the world to believe and he's overplaying his hand."

> Intimidation tactics against Taiwan also serve Xi Jinping's purposes for shoring up his own position within the Communist Party.
>
> John Dotson, deputy director, Global Taiwan Institute

> If the free world stands with Taiwan, in both the diplomatic and economic realms, Xi and the CCP leadership will get the message that a military invasion will bring about their political demise.
>
> Keith Krach, former U.S. Under Secretary of State

"Tyrants can't persuade, so they bully, especially when their own deck of cards is weaker than they want others to think," he added.

Fatigue is the Real Threat

Despite PLA saber-rattling, Dotson and Krach believed that an invasion of Taiwan was not imminent, though an attempted assault could be likely in the coming years.

"I believe that the leaders of the Chinese Communist Party see that trends in Taiwan are not running their way, and are losing patience with hopes that Taiwan will submit to voluntary annexation," Dotson said. "It is plausible, and a growing danger, that the PRC [People's Republic of China] might undertake an amphibious invasion against Taiwan within the coming decade."

"But, I think it more likely that we will see an escalating campaign of 'gray zone' intimidation tactics, perhaps ultimately leading to efforts to block shipping in and out of Taiwan ports, and flights in or out of Taiwan's airports."

For his part, Krach believed that China could still be deterred from all-out conflict provided the United States and its allies remained steadfast in their commitment to a free and open Indo-Pacific.

"General Secretary Xi sees the annexation of Taiwan as a crowning jewel in his legacy," Krach said. "That certainly makes the China-Taiwan tensions more combustible."

"If the free world stands with Taiwan, in both the diplomatic and economic realms, Xi and the CCP leadership will get the message that a military invasion will bring about their political demise."

Continued PLA incursions into Taiwan's ADIZ nevertheless present a real threat to the people and military of Taiwan. Each such incursion requires the Taiwan military to scramble fighters and respond in kind, and this constant strain on material and psychological resources has led to something of a crisis fatigue on the island.

"The need to constantly launch air patrols to escort PLA aircraft will produce multiple forms of strain on Taiwan's air force: to include pilot fatigue, increased wear on airframes, and increased fuel and maintenance budgets," Dotson said. "It will also cut into training time."

"There is the risk of psychological fatigue over time," Krach said, "as these provocative PRC military flights become routine. This presents an increased risk of tactical surprise if one of these sorties were to turn into an actual attack, or direct flight over the island."

Indeed, such strain has already proven fatal at times. There were at least four aircraft crashes in Taiwan last year, including one that killed Taiwan's top military officer.

Still, Krach expressed a belief that the people of Taiwan would continue to express resiliency in the face of adversity.

"I have unwavering belief in the strength of the Taiwanese people and confidence that Taiwan's leaders and citizens will stand their ground and know they'll have support from plenty of friends," Krach said.

The Future of Freedom at Stake

Following the incursions earlier this month, Taiwan President Tsai Ing-wen swore that the self-governed island would defend itself and its "free and democratic way of life" from CCP aggression.

That appeal to the continued dominance of democratic values was not a simple talking point. To hear Dotson tell it, it is a statement of what is truly at stake in the current standoff between Taiwan and the CCP.

"These growing tensions surrounding Taiwan are genuinely very dangerous," Dotson said. "As has been accurately pointed out in recent statements by President Tsai Ing-wen and other senior Taiwan officials, the growing stand-off over Taiwan is a struggle between expansive authoritarianism and democracy, and the outcome will have tremendous repercussions for the decades ahead."

"Taiwan is critically important," Dotson added. "If the United States were to stand back while a democratic state was annexed by force, it would present an enormous blow to both U.S. moral authority and the cohesion of the U.S.-led alliance systems in Asia and Europe."

In addition to wearing down the hearts and minds of the people of Taiwan, Krach noted that the recent uptick in ADIZ incursions is also an effort to champion the CCP's sovereignty-based authoritarianism and to erode the influence of the United States' democratic and international multilateralism abroad.

The reasons for this, according to Krach, go beyond mere jockeying for influence, and extend to a deep-seated fear among the CCP's elite concerning the influence that free peoples in democratic states can wield. Taiwan specifically, he said, represents a vision of a future that is wholly incompatible with communist repression.

"What I have come to know in my 40-year career as a businessman and later as a diplomat, is that Taiwan is an indispensable partner in advancing freedom, and shows the power of free markets and democracy as a counterweight to authoritarian states," Krach said.

"Taiwan is a testament to the Chinese mainland that democracy and human rights are possible for them too."

Andrew Thornebrooke is a freelance reporter covering China-related issues with a focus on defense and security. He holds a master's in military history from Norwich University and authors the newsletter Quixote Hyperdrive.