WEEK 15, 2019

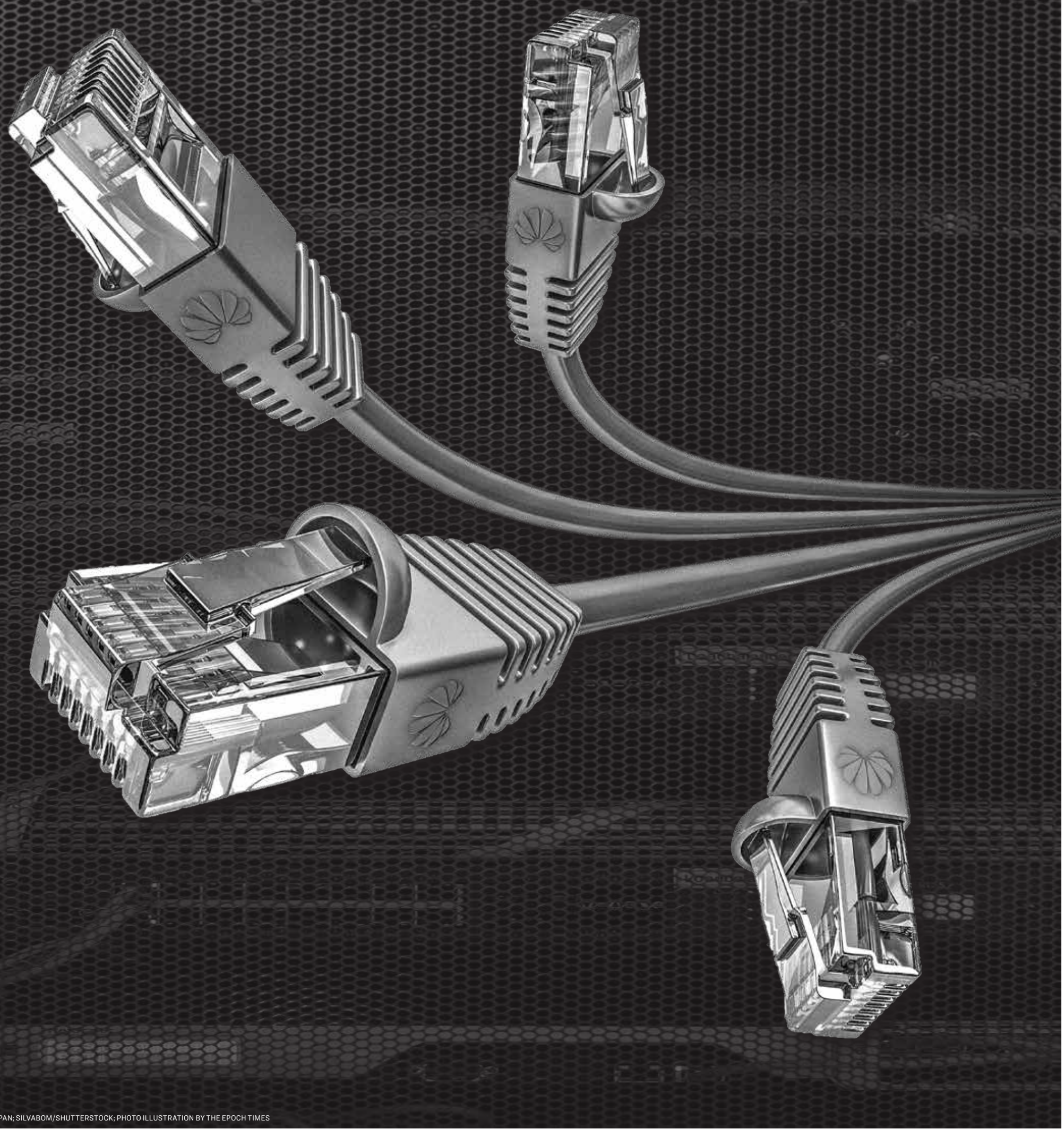
THE EPOCH TIMES

CHINA WEEKLY

HUAWEI

A FORMIDABLE THREAT TO US TELECOM INFRASTRUCTURE

See Page 4



PHOTOS BY MIPAN; SILVABOM/SHUTTERSTOCK; PHOTO ILLUSTRATION BY THE EPOCH TIMES

CHINESE INFLUENCE

FOREIGN INFLUENCE: CHINA'S ATTEMPTS TO INTERFERE WITH CANADIAN UNIVERSITIES

LIMIN ZHOU

The attempt last week by a Chinese diplomat to prevent an exiled Uyghur activist from talking at a Canadian university is the latest in a string of cases in which the Chinese communist regime tried to exert influence in Canadian universities.

It is yet one more incident in a long-trend of Chinese interference in Canadian educational institutions.

A precedent-setting court case from the late 1990s shows how Canadian laws were used by immigration officials in a case involving Chinese espionage and subversion activities on a university campus.

3 Recent Cases

According to the National Post, last week consul Wang Wenzhang from the Chinese consulate in Montreal sent an email to Kyle Matthews, the executive director of the Montreal Institute for Genocide and Human Rights at Concordia University, demanding that exiled Uyghur leader Dolkun Isa refrain from talking to students at an upcoming event at the university.

In another recent case, a University of Toronto Scarborough student was the victim of a slew of online abuse after being elected president of the student union because she had spoken out against the Chinese regime's abuses in Tibet. Toronto police have opened an investigation into the case.

> The government of China has been penetrating and infiltrating the entire societies of both Canada and Australia for many, many years.
>
> *Clive Ansley, China expert*

In yet another incident, this time at McMaster University, a human rights event related to Uyghur Muslims persecuted in China was disrupted by a man shouting a profanity at the speaker. Online discussions later revealed that someone had made a recording of the event and passed it on to the Chinese consulate.

Students and Scholars Association

According to the online discussions in the McMaster incident, consulate officials had asked the students to report their observations to the consulate and to get in touch with the university's Chinese Students and Scholars Association (CSSA). The association later issued a statement condemning the human rights event, saying it had reported the event to the Chinese consulate and that it would make an objection about it to the university.

CSSAs and numerous other Chinese student associations are known to be closely linked with Chinese consulates, with the websites of many of the associations saying they were founded by the consulate. CSSAs have even been linked with espionage, as was the case with the association at a Belgian university that acted as a front for industrial espionage in the mid-2000s.

In another case in the 1990s and early 2000s, Canadian immigration officials accused Yong Jie Qu, a Chinese student association leader at Concordia University in Montreal, of engaging "in acts of espionage and subversion." Authorities said he identified pro-democracy students and reported information about them to the Chinese Embassy.

Winnipeg-based lawyer David Matas says permanent residents or those on student visas who engage in acts considered espionage or subversion against Canada can be rendered inadmissible to the country.

CSSA Student Involved in Espionage

Matas points to the precedent-setting case of Qu, whose permanent residency request was denied by a visa officer due to his activities as a leader in a Chinese student association in Montreal.

Qu came to Montreal from mainland China in 1991 to pursue graduate studies at Concordia. Three years later he applied for permanent residency status at the Canadian consulate in Buffalo, New York.

After reviewing Qu's case, the visa officer rejected his application due to what he said was Qu's involvement in espionage and subversion of a democratic institution.

Qu was also interviewed by officials from the Canadian Security Intelligence Service (CSIS), showing that CSIS was paying attention to CSSA leaders at least as far back as in the 1990s.

After the rejection of his residency request, Qu applied for a judicial review of the case. Documents from the court, which sided with the visa officer's findings, show that Qu regularly reported pro-democracy students who were members of the Chinese student association and their activities to the Chinese Embassy in Ottawa. Qu also sought to change the direction of the student association, using funds provided by the Embassy to support activities condoned by the Embassy, to make the association "sensitive to the Chinese government and Chinese officials," and to conform to the policies and objectives of the Beijing regime.

The court ruled that Qu did, in fact, engage in espionage and subversion at the Concordia Chinese student association, but the court agreed with Qu that the "democratic institution" referred to in the immigration act applies narrowly to "governmental institutions or processes" only and not a student body such as the association, and ordered a review of the case.

Ottawa appealed the judgment, and as a result, the appeal court overturned the lower court's decision by giving a broader explanation to "democratic institution" referred to in the Immigration Act to encompass institutions and processes that are non-governmental but are part and parcel of the democratic fabric of Canada.

The court sent the case back to visa officers to make the final decision based on whether the CSSA falls into the definition of a democratic organization according to the appeal court decision. Due to privacy laws, it is not clear what the visa officers ultimately decided in Qu's case.

Matas says when it comes to the Immigration Act, student groups such as Chinese student associations should be considered democratic institutions since that is what their constitutions—based on university student union requirements—calls for.

"In my view, the federal court left it open, but judging from the English text of some CSSA branches posted on the web, they should be a democratic institution as understood in the legislation," says Matas.

With this classification, Matas says those who are found to be in violation of the laws can be deported.

"The democratic nature of that organization has been subverted. Anybody who goes about continuing to subvert it and is not a citizen can be deported."

Subverting Student Groups

The Epoch Times spoke to J. Li, a former Chinese student association president at the California Institute of Technology. According to Li, who didn't want his full first name used, CSSAs started to be more established on North American campuses in the early to mid-1980s.

Although the constitutions of most CSSAs follow the norms of typical student organizations to hold elections and follow democratic processes as required by universities, Li says the associations have now become directly controlled by Chinese missions. Many CSSA pamphlets, and even their websites, state that their association was founded by the Chinese consulate or that they are supported by the Chinese consulate or embassy.

However, following the Tiananmen Square Massacre on June 4, 1989, the control of the Chinese officials over CSSAs slipped for a period of time, as many students became sympathetic to the persecuted pro-democracy students back home. In addition, since they had been overseas for some time and some of them had obtained permanent residency, they were less scared of the Chinese Communist Party (CCP) retaliating against them.

Li says this period lasted for about one or two years, and by the early 1990s the CSSAs were back to being fully controlled by the CCP.

A former executive member of the CSSA in Ottawa in the year of 1992/1993, who asked for anonymity, says that after the group held elections, the elected members were invited to the Chinese Embassy for a social event. Later that year when the student association was going to make an announcement about a June 4 memorial in front of the Chinese consulate, the association got a call from the Chinese Embassy telling them not to do so. She says the association has since slipped further under the full control of the Chinese Embassy.

According to U.S. Vice President Mike Pence, CSSAs are part of China's efforts to exert influence in academia. These organizations "alert Chinese consulates and embassies when Chinese students, and American schools, stray from the Communist Party line," he said in an October 2018 speech.

A 2018 report by Foreign Policy says that many CSSAs officially describe themselves as being under the "guidance" or "leadership" of the Chinese Embassy or consulate. The report, based on interviews with CSSA heads and internal documents, says some CSSAs even vet their membership to ensure only those whose views are aligned with the CCP are included. In the case of universities in the Southwestern United States, the report adds, an umbrella group overseeing CSSAs in these universities requires all CSSA presidential candidates to have approval from the Chinese consulate before elections take place.

Following Australia's Example

Clive Ansley, a China expert based on Vancouver Island who used to practice law in China, says Beijing has been attempting to infiltrate and exert influence in countries like Canada and Australia for decades.

"The government of China has been penetrating and infiltrating the entire societies of both Canada and Australia for many, many years and the Canadian public has no perception of it at all," he says.

Ansley says Canada should follow the example of Australia, which has recently enacted anti-interference legislation after revelations of the extent of China's infiltration of political circles in the country.

The new laws require anyone acting on behalf of foreign powers to influence the Australian political process to publicly register their names and provide details of their relationship and activities with the foreign agent.

"Canada should be doing something along the same lines, because Canada and Australia have a similar problem," Ansley says.

MEUNIERD/SHUTTERSTOCK

FACEBOOK

Concordia University's downtown campus in Montreal. The Montreal Institute for Genocide and Human Rights Studies at Concordia held a talk by Uyghur leader Dolkun Isa on March 26, 2019.

Chemi Lhamo, a student at the University of Toronto Scarborough, who was recently elected as the president of the student union at the university.

> A precedent-setting court case from the late 1990s shows how Canadian laws were used by immigration officials in a case involving Chinese espionage and subversion activities on a university campus.

NATIONAL SECURITY

CHINA IS ADVANCING ARTIFICIAL INTELLIGENCE TECHNOLOGY TO FOOL US SATELLITES

FRANK FANG

China is advancing a type of artificial intelligence that can fool U.S. satellites into seeing things that aren't there.

The emerging technique is known as generative adversarial networks (GANs), which involves a computer network creating fake images to trick analytical computers into believing that the images are real.

This has military repercussions since the U.S. military relies on automated image analysis to screen large volumes of satellite images. The analysis systems could be fooled by intentionally doctored images generated by Chinese computer networks, according to a U.S. intelligence official.

"The Chinese have already designed; they're already doing it right now, using GANs–which are generative adversarial networks–to manipulate scenes and pixels to create things for nefarious reasons," said Todd Myers, automation lead and chief information officer at the Pentagon's National Geospatial-Intelligence Agency, at the Genius Machines summit on artificial intelligence, held on March 28.

As an example, Myers stated that an image analysis might wrongly conclude from a doctored image that there is a bridge across a river, when there isn't one in real life.

> You train your forces to go a certain route, toward a bridge, but it's not there. Then there's a big surprise waiting for you.
>
> *Todd Myers, chief information officer, National Geospatial-Intelligence Agency*

"So, from a tactical perspective or mission planning, you train your forces to go a certain route, toward a bridge, but it's not there. Then there's a big surprise waiting for you," Myers said, according to defense news website Defense One.

He added that China is currently the leader in GANs, and the process to defeat GANs is time-consuming and costly.

Beijing has laid out a detailed plan to become the world leader in artificial intelligence (AI).

In 2015, China announced its industrial plan of "Made in China 2025," with the goal of transforming China into a high-tech manufacturing powerhouse by 2025, including in sectors such as artificial intelligence and big data.

Two years later, in July 2017, China's State Council published the "Next-Generation Artificial Intelligence Development Plan" in July 2017.

The plan envisions a three-step process for China: to keep pace with AI technology and applications by 2020, become a world leader in AI tech by 2025, and the center of AI innovation by 2030.

The plan also explains that China must be able to develop indigenous AI industries, including smart robots, smart delivery tools, and smart software and hardware–including graphics processing, pattern recognition, and machine translations –all of which are key areas to advancing GANs.

"China is by far the United States' most ambitious competitor in the international AI market," stated a U.S. Congressional Research Service (CRS) report published in January this year.

Yet, some American AI technology is being funneled to China. According to the CRS report, China invested an estimated total of $1.3 billion in American AI companies between 2010 and 2017, "potentially granting [Beijing] lawful access to U.S. technology and intellectual property."

The report also pointed out that, in 2017, Beijing created a Military-Civil Fusion Development Commission to speed up the transfer of AI technology from commercial companies and research institutes to the Chinese military.

Myers also warned of another danger: open-source images that are easily accessed by the public can be corrupted. For example, mapping on the Google Maps app is susceptible to infiltration by GANs.

Defense One's report warned that the compromise of open-source data and images could "erode the public credibility of the national security community and the functioning of democratic institutions."

Meanwhile, Andrew Hallman, head of the Central Intelligence Agency's Digital Directorate, said at the same summit: "We are in an existential battle for truth in the digital domain," according to the Defense One report.

NEWS ANALYSIS

SECRET CHINESE ANTI-SATELLITE, EMP BASES DISCOVERED, EVEN AS CHINA TALKS PEACE IN SPACE

JOSHUA PHILIPP

Satellite imagery has revealed a secret anti-satellite weapons base in China, as well as electromagnetic pulse (EMP) weapons testing facilities. This news is making the rounds online even as the Chinese regime is criticizing India for its space weapons programs, and is calling for peace in space.

The discovery was made by retired Indian Army Col. Vinayak Bhat, who specializes in satellite image analysis focused on China. He noted in India's The Print news website that the Chinese Communist Party (CCP) now has several of these facilities, including in Tibet and Xinjiang.

Bhat wrote that the facilities have tracking equipment, and it is believed the anti-satellite laser weapons stationed in buildings with sliding roofs can be used for varying purposes that include blinding or destroying satellites.

The EMP weapons facilities, meanwhile, appear to be for testing. They include some simulated electrical infrastructure and nearby facilities housing the weapons. Included in one image is what appears to be a mobile EMP generator.

These images are being circulated just after India tested an anti-satellite missile and destroyed a satellite March 27. The test sent debris hurtling through orbit.

After the recent test, the CCP came out playing the peacekeeper. According to The Times of India, Chinese Foreign Ministry spokesman Hong Lei said at a press conference, "Outer space is shared by the entire mankind. Every country has the right to make peaceful exploration and use of outer space."

In reality, the CCP has been highly aggressive with its military space programs. It tested its first anti-satellite weapon in May 2005, and shocked the space community in 2007 when it used a missile to destroy its Feng Yun 1-C weather satellite, and sent over 3,000 pieces of debris into low-earth orbit.

The CCP has continued testing its anti-satellite weapons since then, and the secret laser weapons facilities revealed by satellite imagery are just small pieces of the bigger picture.

In its 2015 Annual Report to the Congress, the U.S.-China Economic and Security Review Commission warned that "China's recent space activities indicate that it is developing co-orbital anti-satellite systems to target U.S. space assets."

Militarily, space is regarded as the "ultimate high ground." Weapons placed in orbit could allegedly target missiles on earth as they launch, nuclear weapons could be detonated in orbit for destructive EMP without the need for launch, and satellites crucial for military communications and targeting can be destroyed.

Under the CCP's unconventional warfare programs designed to destroy the weakest links of the U.S. military, weapons of these types are regarded as highly valuable. CCP military doctrine such as its Assassin's Mace or "Trump Card" program describe such weapons directly.

In 2014, Chinese Ret. Lt. Gen. Wang Hongguang threatened the United States with these weapons systems in the CCP's state-run Global Times news outlet. Wang said that the CCP would use these weapons suddenly, and warned Americans in their "pride and arrogance" to "not get trampled beneath us."

Public information on the CCP's Assassin's Mace weapons are thin, but a 2011 report from the National Ground Intelligence Center said, "These modern Trump Card and Assassin's Mace weapons will permit China's low-technology forces to prevail over U.S. high-technology forces in a localized conflict."

> The secret laser weapons facilities revealed by satellite imagery are just small pieces of the bigger picture.

According to a recent Government Accountability Office report, on April 3, little has changed. It says, "China and Russia in particular are developing a variety of means to exploit perceived U.S. reliance on space-based systems and challenge the U.S. position in space."

It's in this context that President Donald Trump signed an executive order on March 26 to harden U.S. critical infrastructure to protect against EMP attacks. It's also in this context that Trump is pushing for a Space Force military branch that would consolidate U.S. military space programs.

OPINION

HUAWEI: A FORMIDABLE THREAT TO US TELECOM INFRASTRUCTURE

JAMES GORRIE

The arrest of Huawei executive Meng Wanzhou in Vancouver last December for allegedly violating U.S. sanctions against Iran confirmed what experts in the telecom industry, some members of Congress, and the U.S. defense establishment have long suspected: Huawei and its subsidiaries represent a tangible threat to the United States.

The Chinese tech giant also has been accused of intellectual property theft involving phone-testing robot technology owned by T-Mobile. And in January, a Huawei employee was arrested in Poland on espionage charges.

But these incidents—though serious—haven't disrupted Huawei's business relationships with Europe and Asia. Today, Huawei operates in more than 170 countries, supporting more than 500 telecom providers. What's more, Huawei technology and infrastructure will play a key role in deploying the next generation of mobile communications, the 5G network, for much of the world. But the Huawei story is much more complex than sanctions violations and spying employees.

Huawei's Biggest Espionage Coup?

Yet even as U.S. President Donald Trump attempts to limit Huawei's expansion into the global 5G market, some experts fear that it may already too late. Defense and telecom authorities assert that Huawei may have already accomplished its biggest espionage coup of eavesdropping on America's strategic nuclear forces and other major defense installations located in the Western states.

According to telecom expert Gary Frost, in the early 2000s, smaller, rural customers in states such as Nebraska, Wyoming, Montana, South Dakota, and Colorado were overlooked by equipment giant Cisco and others. These underserved states created an opportunity for a low-cost, good-quality infrastructure provider to step in.

Huawei was happy for the opportunity to install its own cheaper versions of Cisco-type equipment—routers, switches, and other telephone and internet infrastructure—and gain customers in these rural communities.

Today, not all of the states in question are entirely dependent on Huawei, but up to 25 percent of rural wireless carriers use the company's equipment, with Montana highly dependent upon it and Wyoming almost not at all. But Frost points out that although there's no Huawei fiber to his knowledge, Huawei equipment sits adjacent to fiber carrying nuclear and highly sensitive defense data to launch command sites and defense facilities located throughout the states mentioned.

Have there been compromises? It's unknown for sure, and it's not clear there has been any investigation.

CALEA Makes Spying Easier for Everyone

A key enabling factor in creating these vulnerabilities was the establishment of the Communications Assistance for Law Enforcement Act (CALEA), which was passed in 1994 and became effective on Jan. 1, 1995. CALEA mandated that for national security reasons, both telecom companies and manufacturers of telecom equipment must add built-in access for lawful surveillance to eavesdrop on suspicious communications. This can be done remotely.

When CALEA was established, it was likely assumed that all relevant infrastructure and access points to be used by CALEA were specific and identified. If that was true, it wasn't for very long. Quick expansion of both CALEA and infrastructure demands meant that packaging of switches became hybrids of various technologies—creating multiple vulnerabilities. Today, all telecom manufacturers have remote access monitoring and update capabilities. These also have been targeted by Huawei since they are embedded into the telecommunications architecture.

> A key enabling factor in creating these vulnerabilities was the establishment of the Communications Assistance for Law Enforcement Act.

Network cable panel, switch and internet cables in data center. Many rural communities have telephone and internet infrastructure supplied by Huawei, exposing the networks to spying by China.

China's Involvement

Some of those vulnerabilities were exploited and the evidence points to China as the culprit. It's a bit technically complex to explain in detail here, but essentially, when access points are used to steal data, that data is sent to a determined destination for it to be received and analyzed. In other words, a hacking or eavesdropping event on switches and other infrastructure leaves a trail and reveals where data was sent.

In the hacks that Frost references, both the data flows hitting interfaces to CALEA equipment and the IP addresses where the data went, were Chinese. They were so-called "brute force" attacks, which, in layman's terms, means overwhelming the security of a program or piece of equipment with multiple interactions or instructions all at once or over a period of time. It's not a particularly clever technique, but the attacks worked.

Thus, Huawei leveraged the opportunity to bring rural America into the digital age, and Rural Telephone Associations and Rural Wireless Associations (RTAs and RWAs) in those sparsely populated states were more than grateful. Over the years, Huawei has become embedded in the telephone and wireless associations.

Huawei officials have sat on RTA boards for years and have helped steer additional infrastructure build-outs as needed. But in the process, Huawei—and, according to Frost and other experts, the Chinese regime—have been eavesdropping via built-in access points in America's telephone and internet infrastructure in rural areas.

To be clear, it's not likely that there is Huawei fiber in sensitive installations. So-called "last mile" communication lines serving those areas are protected by "armored fiber pairs." This hardened equipment is then installed by vetted telecom contractors. But at some point, some distance away, those installations are connected to vulnerable equipment manufactured and installed by Huawei. And it's not simply listening in on conversations. As Frost explains it, Huawei may potentially be able to even remotely change or block data and communication transmissions to strategic U.S. sites.

How could such oversights occur time after time over the years?

A Series of Errors

For one, not all relevant federal agencies were looking for espionage vulnerabilities. The main interest of the U.S. Department of Commerce and the Federal Communications Commission was to certify that new equipment won't harm the existing system and would perform as advertised. And the main interests of rural telecoms, at least at first, was to enter the digital age with the low cost and high functionality of Huawei's equipment.

Preventing spying wasn't a major concern at the time.

But the way in which cable and fiber pairs are laid out opens up the possibility for access that shouldn't be allowed. There may be several fiber pairs existing side-by-side within the same cable, with the defense pairs adjacent to Huawei equipment—where its technicians could potentially "tap" into the defense infrastructure. This could mean that Huawei and the Chinese regime have been able to hack and track data transmissions of America's most sensitive installations for decades.

That's why it would appear to be no coincidence that Huawei focused its first efforts in the state of Nebraska. Nebraska is where Offutt Air Force Base is situated, and, more to the point, where the U.S. Strategic Air Command headquarters is located.

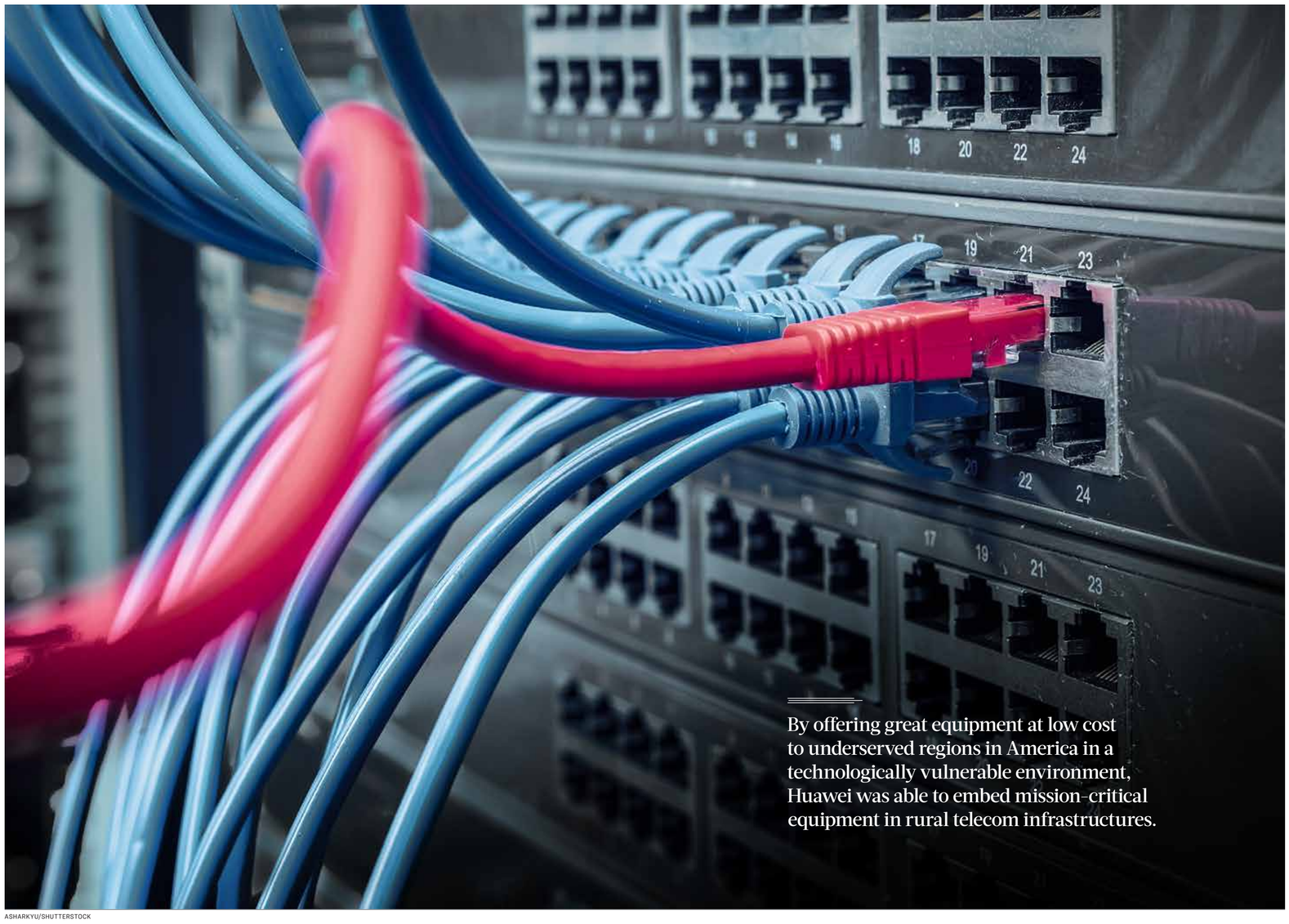
Huawei's strategy to gain access to the crown jewels of U.S. defense installations was as simple as it is brilliant. By offering great equipment at low cost to underserved regions in America in a technologically vulnerable environment, it was able to embed mission-critical equipment in rural telecom infrastructures. That positioned it to exploit the vulnerabilities that surround the United States' most strategic defense operations.

This apparent sloppiness of U.S. defense officials regarding our strategic communication infrastructure is more than troubling. As of yet, there's no serious evidence that the Huawei vulnerability is being reviewed at the granular level necessary by the Department of Defense.

They seem to be much more focused on the potential threats of the as-of-yet non-existent 5G network deployment, instead of dealing with the current threats—which should be removed and replaced immediately.

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

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



By offering great equipment at low cost to underserved regions in America in a technologically vulnerable environment, Huawei was able to embed mission-critical equipment in rural telecom infrastructures.

ASHARKYU/SHUTTERSTOCK

COURTESY OF RUI PEDRO OLIVEIRA

Portuguese entrepreneur Rui Pedro Oliveira.

INTELLECTUAL PROPERTY

PORTUGUESE ENTREPRENEUR CLAIMS HUAWEI STOLE HIS CAMERA INVENTION

CATHY HE

A Portuguese entrepreneur claims that Chinese tech giant Huawei stole his 360-degree smartphone-attachable camera invention after he pitched the patent-pending product to the company for licensing five years ago.

The offending product, according to Rui Pedro Oliveira, CEO of multimedia company Imaginew, is Huawei's smartphone-attachable camera called EnVizion 360 Camera, announced in 2017.

The 45-year-old entrepreneur from Porto said that during the past year, he had been negotiating with Huawei's U.S. lawyers to resolve the dispute and believed that they were approaching a settlement—only to find that the company had sued him at a Texas court on March 25.

The lawsuit, filed by Huawei's U.S. subsidiaries, Huawei Technologies USA Inc. and Huawei Device USA Inc., seeks a declaration that the companies didn't infringe upon Oliveira's patent.

The inventor's claims add to a growing pile of accusations against Huawei, from allegations of technology theft to governments warning of security risks that its products could be used by Beijing for spying.

At the same time, many countries are finalizing their decisions on whether to include the company's technology in their emerging 5G networks. The United States, Australia, New Zealand, and several mobile operators in Europe and Asia have already shut out Huawei from their 5G plans.

Meeting

In an extensive interview with The Epoch Times, Oliveira explained how he visited the United States in 2014 to pitch his camera to various technology companies in hopes that they would license, manufacture, and sell his invention.

With the help of a U.S. businessman who set up the meetings, Oliveira secured a meeting with Huawei on May 28, 2014. The two were invited to discuss the licensing opportunity at Huawei's U.S. headquarters in Plano, Texas.

At the time, Oliveira's invention, a 360-degree camera attachable to smartphones called SmatCam, was patent pending with the U.S. Patent and Trademark Office. The two patents relating to the camera have since been approved.

Prior to the meeting, Oliveira entered into a non-disclosure agreement with one of Huawei's representatives, a copy of which The Epoch Times has obtained.

Oliveira said he met with four representatives from the company's business and sales divisions, and gave a presentation, which included the results of focus group tests that surveyed how people reacted to the product, priced at $99.95.

During the meeting, he also presented a 3D model of his invention and showed them the design drawings attached to his patent applications.

The entrepreneur said the Huawei representatives expressed interest and asked him to return the next day to give the same presentation to some technicians. This, Oliveira said, seemed to be a good sign, as most other companies he pitched to didn't ask for a second meeting.

After the second meeting, Oliveira was told that the company would consider his offer and get back to him soon.

The entrepreneur never heard back from Huawei.

Dealings With Huawei

Oliveira didn't think back to those meetings for three years, until one day, a friend who knew about his invention messaged him, telling him to check out a website link to Huawei's new smartphone-attachable camera, the EnVizion 360 Camera.

"I thought it was crazy. How could they dare to do something so ... similar?" Oliveira said.

The camera was sold at $99.95, the same price suggested during Oliveira's presentation.

He immediately emailed the Huawei representatives he met with in 2014, as he had kept their business cards, alleging that Huawei's EnVizion Camera violated his intellectual property. He was eventually referred to the company's U.S. legal department.

Through his Portuguese lawyer, Oliveira said he started communicating with two of Huawei's U.S. attorneys from about April 2018, after he sent a letter to Huawei charging that the company had infringed upon his patents and seeking compensation.

After a few months of back and forth communication, Huawei's lawyers told him they couldn't proceed with discussions until Oliveira hired a U.S. attorney.

So Oliveira and his wife decided to sell his house in Portugal to fund a U.S. lawyer. The couple sold the house in September 2018 and hired a Boston-based intellectual property attorney.

Oliveira says that he, his wife, and their 10-year-old daughter now rent a house in his hometown of Porto.

His U.S. lawyer resumed negotiations with Huawei's attorneys, but during the next five months, Oliveira said, there was always something to delay the discussions, such as a missing signature or someone from Huawei would be away on a business trip.

Oliveira believes these tactics were employed "just to pass time until I am hit with severe financial limitations and can no longer pursue the case."

Surprise Counterattack

In late March, however, the negotiations appeared to be making headway. Earlier, Oliveira had told Huawei's lawyer that if they didn't negotiate a settlement by April 1, he would start legal action against the company for patent infringement.

> "I thought it was crazy. How could they dare to do something so ... similar?
>
> *Rui Pedro Oliveira*

According to Oliveira, on March 25, Huawei's attorney asked him to offer an amount to settle the matter. Oliveira made an offer, and was told the next day that the attorney was going to inform Huawei superiors in China of the offer and get back to him.

Days passed without a reply from Huawei.

Now Oliveira knows why. That same day, the company had filed a lawsuit against him at the federal court in the eastern district of Texas, seeking a declaration that its EnVizion 360 Camera did not infringe upon his patents.

"I'm speechless. I didn't know ... how low [they] could go," he said.

Oliveira said he was completely blindsided by Huawei's actions, as he was carrying out negotiations in good faith and expected the other party to act the same.

At no point during the negotiations did Huawei mention a lawsuit, he said.

In its court documents, Huawei acknowledged the meeting "on or about 28-29 May 2014" wherein Oliveira met with company representatives in Plano to "discuss his patents and business plan and offer a license to Huawei USA."

The company later rejected Oliveira's offer, court documents state.

Huawei USA's affiliate in China, Huawei Device Co. Ltd., designed the EnVizion 360 Camera, the document said, adding that the product was first publicly announced in September 2017.

In addition to a judgment that Huawei did not infringe upon Oliveira's intellectual property, the company also seeks an order that Oliveira pay Huawei's attorney fees on the basis that "this case is exceptional ... due to ... Oliveira's actions, including but not limited to express or implied threats to harm Huawei USA's reputation in the press unless Huawei USA pays money to settle the dispute."

Huawei did not respond to The Epoch Times' requests for comment.

In a response to Portuguese technology website Pplware, which published a story about Oliveira's dispute with Huawei on March 16, Huawei said the EnVizion 360 was developed entirely by its research and development team in China, and thus denied Oliveira's allegations of intellectual property theft, adding that the company "reserved the right to take legal action in response to false charges."

The company is no stranger to legal controversy. Huawei and its affiliates currently face two U.S. federal prosecutions.

In a 13-count indictment, the company, as well as its chief financial officer (CFO), were charged with bank fraud and violating U.S. sanctions against Iran. Prosecutors allege Huawei lied to banks about its relationship with an unofficial subsidiary that did business with Iran, thus causing the banks to unknowingly breach U.S sanctions.

Meanwhile, its CFO Meng Wanzhou, who is also the daughter of Huawei's founder, is fighting extradition proceedings in Canada in relation to this case.

In a separate 10-count indictment, prosecutors accuse Huawei of stealing trade secrets, committing wire fraud, and obstructing justice for allegedly stealing information from mobile carrier T-Mobile about its robot nicknamed "Tappy," which was designed to test smartphones' durability.

In that case, prosecutors also allege the company established a bonus program to reward employees who would steal confidential information from competitors.

In early March, Huawei announced it is suing the U.S. government over section 889 of the National Defense Authorization Act passed last August, which bans federal agencies and their contractors from purchasing Huawei equipment. Lawmakers had added that provision due to national security risks associated with Huawei products.

Outside of the courts, Bloomberg reported in February that the FBI was investigating Huawei for suspected theft of diamond-coated smartphone glass technology made by Illinois-based tech company AKHAN Semiconductor.

AKHAN, the report said, had sent samples of the diamond glass to Huawei for standard testing after the Chinese smartphone maker expressed interest in licensing the technology. The glass, however, was returned to AKHAN in pieces—raising the company's suspicions that Huawei had tampered with the glass to figure out how it was engineered, Bloomberg reported.

A February report by The Information, citing unnamed sources, said Huawei had approached Apple suppliers, former Apple employees, and Foxconn assembly line workers for information on components used in Apple products, including the Apple Watch's heart-rate monitor and a connecter for the MacBook Pro. Huawei denied the allegations.

At the time of publication, Oliveira has yet to be served with the lawsuit.

The entrepreneur said he will now have to tap into proceeds from the sale of his house to hire another U.S. attorney to defend this new action.

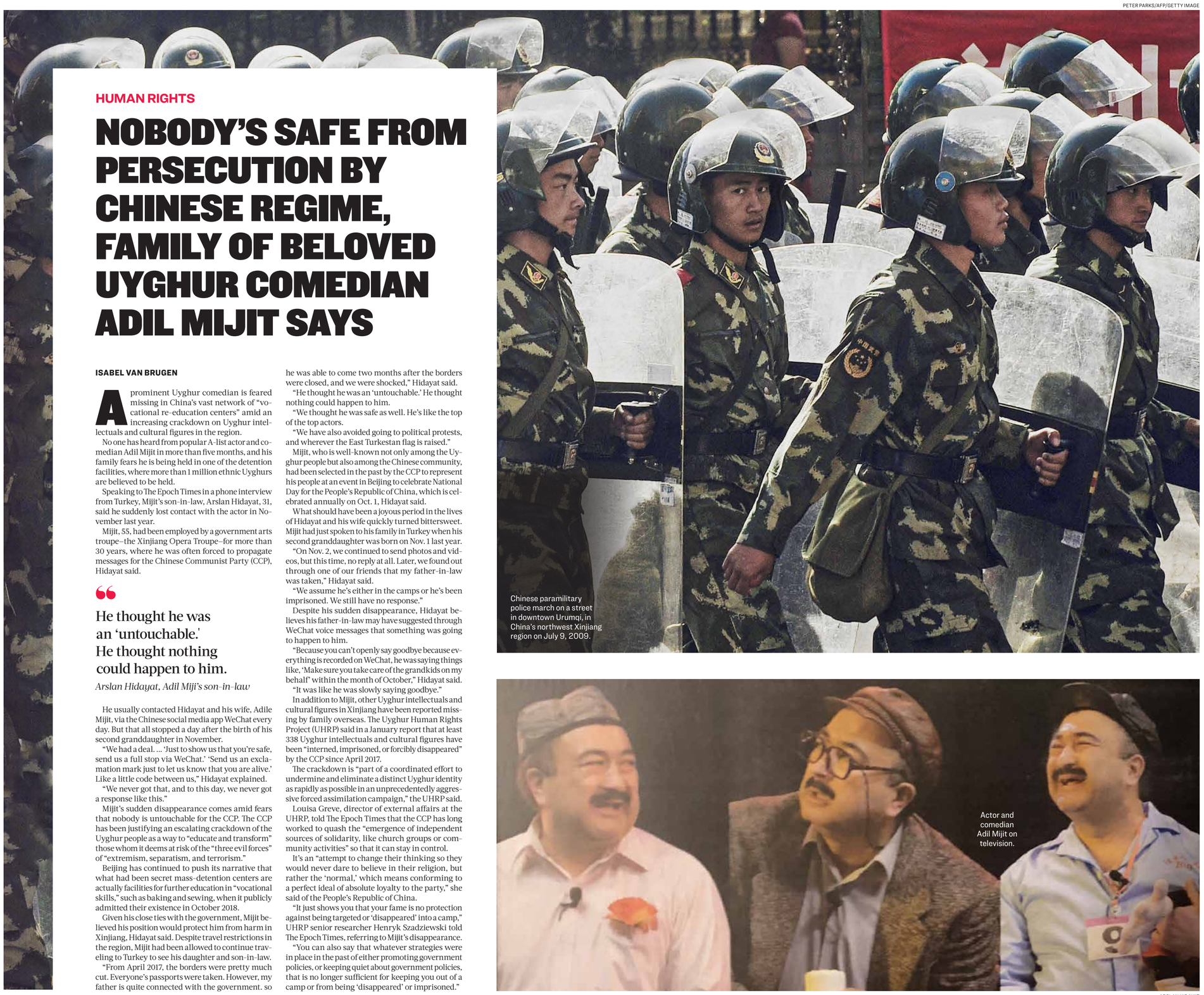
Apart from setting aside some money for his young daughter's education, Oliveira is prepared to use all the money to see this case through.

He believes the lawsuit is an attempt to scare him into backing down.

"They need much more to make me sweat," he said.

"I won't give up."

PETER PARKS/AFP/GETTY IMAGE



Chinese paramilitary police march on a street in downtown Urumqi, in China's northwest Xinjiang region on July 9, 2009.

HUMAN RIGHTS

NOBODY'S SAFE FROM PERSECUTION BY CHINESE REGIME, FAMILY OF BELOVED UYGHUR COMEDIAN ADIL MIJIT SAYS

ISABEL VAN BRUGEN

A prominent Uyghur comedian is feared missing in China's vast network of "vocational re-education centers" amid an increasing crackdown on Uyghur intellectuals and cultural figures in the region.

No one has heard from popular A-list actor and comedian Adil Mijit in more than five months, and his family fears he is being held in one of the detention facilities, where more than 1 million ethnic Uyghurs are believed to be held.

Speaking to The Epoch Times in a phone interview from Turkey, Mijit's son-in-law, Arslan Hidayat, 31, said he suddenly lost contact with the actor in November last year.

Mijit, 55, had been employed by a government arts troupe—the Xinjiang Opera Troupe—for more than 30 years, where he was often forced to propagate messages for the Chinese Communist Party (CCP), Hidayat said.

> He thought he was an 'untouchable.' He thought nothing could happen to him.
>
> *Arslan Hidayat, Adil Miji's son-in-law*

He usually contacted Hidayat and his wife, Adile Mijit, via the Chinese social media app WeChat every day. But that all stopped a day after the birth of his second granddaughter in November.

"We had a deal. ... 'Just to show us that you're safe, send us a full stop via WeChat.' 'Send us an exclamation mark just to let us know that you are alive.' Like a little code between us," Hidayat explained.

"We never got that, and to this day, we never got a response like this."

Mijit's sudden disappearance comes amid fears that nobody is untouchable for the CCP. The CCP has been justifying an escalating crackdown of the Uyghur people as a way to "educate and transform" those whom it deems at risk of the "three evil forces" of "extremism, separatism, and terrorism."

Beijing has continued to push its narrative that what had been secret mass-detention centers are actually facilities for further education in "vocational skills," such as baking and sewing, when it publicly admitted their existence in October 2018.

Given his close ties with the government, Mijit believed his position would protect him from harm in Xinjiang, Hidayat said. Despite travel restrictions in the region, Mijit had been allowed to continue traveling to Turkey to see his daughter and son-in-law.

"From April 2017, the borders were pretty much cut. Everyone's passports were taken. However, my father is quite connected with the government. so he was able to come two months after the borders were closed, and we were shocked," Hidayat said.

"He thought he was an 'untouchable.' He thought nothing could happen to him.

"We thought he was safe as well. He's like the top of the top actors.

"We have also avoided going to political protests, and wherever the East Turkestan flag is raised."

Mijit, who is well-known not only among the Uyghur people but also among the Chinese community, had been selected in the past by the CCP to represent his people at an event in Beijing to celebrate National Day for the People's Republic of China, which is celebrated annually on Oct. 1, Hidayat said.

What should have been a joyous period in the lives of Hidayat and his wife quickly turned bittersweet. Mijit had just spoken to his family in Turkey when his second granddaughter was born on Nov. 1 last year.

"On Nov. 2, we continued to send photos and videos, but this time, no reply at all. Later, we found out through one of our friends that my father-in-law was taken," Hidayat said.

"We assume he's either in the camps or he's been imprisoned. We still have no response."

Despite his sudden disappearance, Hidayat believes his father-in-law may have suggested through WeChat voice messages that something was going to happen to him.

"Because you can't openly say goodbye because everything is recorded on WeChat, he was saying things like, 'Make sure you take care of the grandkids on my behalf' within the month of October," Hidayat said.

"It was like he was slowly saying goodbye."

In addition to Mijit, other Uyghur intellectuals and cultural figures in Xinjiang have been reported missing by family overseas. The Uyghur Human Rights Project (UHRP) said in a January report that at least 338 Uyghur intellectuals and cultural figures have been "interned, imprisoned, or forcibly disappeared" by the CCP since April 2017.

The crackdown is "part of a coordinated effort to undermine and eliminate a distinct Uyghur identity as rapidly as possible in an unprecedentedly aggressive forced assimilation campaign," the UHRP said.

Louisa Greve, director of external affairs at the UHRP, told The Epoch Times that the CCP has long worked to quash the "emergence of independent sources of solidarity, like church groups or community activities" so that it can stay in control.

It's an "attempt to change their thinking so they would never dare to believe in their religion, but rather the 'normal,' which means conforming to a perfect ideal of absolute loyalty to the party," she said of the People's Republic of China.

"It just shows you that your fame is no protection against being targeted or 'disappeared' into a camp," UHRP senior researcher Henryk Szadziewski told The Epoch Times, referring to Mijit's disappearance.

"You can also say that whatever strategies were in place in the past of either promoting government policies, or keeping quiet about government policies, that is no longer sufficient for keeping you out of a camp or from being 'disappeared' or imprisoned."

Actor and comedian Adil Mijit on television.

ARSLAN HIDAYAT

ORGAN HARVESTING

TRIBUNAL HEARS EVIDENCE ON FORCED ORGAN HARVESTING IN CHINA

CATHY HE

An independent people's tribunal in London has heard evidence concerning the mass killing of prisoners of conscience for their organs in China.

From April 6 to 7, two dozen witnesses, including researchers, medical professionals, journalists, and survivors from around the world, gave testimonies before the tribunal on allegations of state-sanctioned organ harvesting targeting persecuted groups in China, including practitioners of the spiritual practice Falun Gong and the Uyghur ethnic minority.

The tribunal follows a three-day hearing that took place last December, when tribunal members passed a draft interim judgment concluding that forced organ harvesting from prisoners of conscience has taken place in China "on a substantial scale."

Chaired by Sir Geoffrey Nice, QC, who previously led the prosecution of former Yugoslavian President Slobodan Milosevic at the International Criminal Tribunal, the panel consists of seven experts tasked with conducting the world's first ever independent analysis of forced organ extraction in China.

According to legal counsel Hamid Sabim, the tribunal invited representatives from the Chinese regime, including top health officials and Chinese embassy officials in London, to participate in the hearings, but did not receive a response.

Widespread Blood Testing

Refugees who have escaped persecution in China gave evidence at the tribunal, recounting that they had received blood and medical testing during their detention.

> I knew that they took blood from my arm twice, but I don't know how much blood was drawn.
>
> *Mihrigul Tursun, Uyghur survivor*

Mihrigul Tursun, a Uyghur who last year testified before a U.S. congressional committee about being tortured and abused at an internment camp in the northwestern region of Xinjiang, told the tribunal via video on April 7 that camp detainees underwent detailed health checks, including blood tests and ultrasounds.

The U.S. Department of State and other international experts estimate that the communist regime is holding more than 1 million Uyghurs, ethnic Kazakhs, and other Muslim minorities in a vast network of internment camps in Xinjiang, as part of a purported campaign to combat "extremist threats."

Tursun said she was tortured under interrogation for three days in April 2017, after which she was transported—while hooded, cuffed, and shackled—to an exam room in a hospital.

"I knew that they took blood from my arm twice, but I don't know how much blood was drawn," Tursun said through an interpreter.

She said she also received blood pressure tests and medical tests to check her heart condition.

Tursun said she was then led to a dark room in what she suspected was the basement of the hospital. In that room, the handlers removed her hood and restraints, and then all her clothes. They then attached equipment onto her chest area and used a machine to examine her body.

Her handlers then put liquid on Tursun's forehead, shoulders, just below her heart, and both legs, and placed her into a glass machine, where she was made to circle inside while shouting numbers from one to 10.

Tursun could not hear anything while inside the machine.

"I became terrified after I was placed into that machine. I thought they may be taking my internal organs and that I might die that day," she said through the interpreter.

Ethan Gutmann, China analyst and investigator, testified on April 7 about the Xinjiang crisis.

"You have maybe a million and a half people who have all been blood tested and they're in detention, and their families have lost sight of them," Gutmann said.

He said that recent evidence indicates the Chinese regime is targeting this group for organ extracting, including accounts of DNA testing being conducted at the homes of Uyghurs in Xinjiang and the known construction of regional crematoriums and a dedicated lane for transferring organs for transplant surgery at a local airport.

Organs Mainly Sourced From Falun Gong Practitioners

In 2016, Gutmann co-authored, with Canadian human rights lawyer David Matas and former Canadian Secretary of State (Asia-Pacific) David Kilgour, an in-depth report that found a huge discrepancy between China's official transplantation figures and the number of transplants performed in hospitals

By analyzing the public records of 712 Chinese hospitals that carry out liver and kidney transplants, the report showed that roughly 60,000 to 100,000 transplants are being conducted each year, far outstripping the officially reported number of 10,000 to 20,000 per year.

> Chaired by Sir Geoffrey Nice, the panel consists of seven experts tasked with conducting the world's first ever independent analysis of forced organ extraction in China.

The shortfall, the report concluded, is made up by organs forcibly harvested from prisoners of conscience in China, primarily from practitioners of Falun Gong (also known as Falun Dafa), while Uyghurs, Tibetan Buddhists, and some house Christians also have been targeted.

Several Falun Gong practitioners gave evidence during the December and April hearings, speaking of their experiences of being detained for their faith in China.

Aside from personal accounts of torture they experienced inside China's labor camps and prisons, all spoke of undergoing physical examinations during detention.

Feng Hollis, who was arrested in 2005, said in her December testimony that at the time, she wondered why she was given a medical test despite being frequently tortured in prison.

The tribunal is due to release its final judgment on June 17.

NTD reporter Jane Werrell contributed to this report.

NATIONAL SECURITY

US EXPERTS, LAWMAKERS HIGHLIGHT CHINA'S THREAT TO US RAIL SECURITY

FRANK FANG

China's ambitions to become a top leader in the railway industry is threatening U.S. national security, according to industry experts and lawmakers.

Chinese rail manufacturers have been able to expand quickly across the globe because of Beijing's government policies and heavy subsidies.

One company in particular, the state-owned rail car manufacturer China Railway Rolling Stock Corp. (CRRC), has racked up several contracts in major U.S. cities in recent years.

Concerned that the partnerships could pose security threats, a bipartisan group of U.S. senators recently sought to address the issue with new legislation.

The Transit Infrastructure Vehicle Security Act was introduced by U.S. Sens. John Cornyn (R-Texas) and Tammy Baldwin (D-Wisc.) on March 15, which would prohibit federal money from being used to award a procurement contract or subcontract for passenger rail cars and transit buses to Chinese state-owned, controlled, or subsidized enterprises, according to a press release from the office of Sen. Sherrod Brown (D-Ohio). Brown and his colleague Mike Crapo (R-Idaho) are co-sponsors of the legislation.

"China poses a clear and present danger to our national security and has already infiltrated our rail and bus manufacturing industries," Cornyn said in the press release, arguing that the new legislation would help safeguard the U.S. transportation and infrastructure sectors.

Recent Deals

China's CRRC succeeded in winning contracts in several major U.S. cities to supply rail cars. According to local news site Boston.com, CRRC was awarded an $843 million contract by the Massachusetts Bay Transportation Authority to assemble 404 subway cars in 2014.

Then, in March 2016, the Chicago transport authority contracted CRRC to build 846 rail cars for $1.3 billion, according to Reuters.

A year later, the Los Angeles County Metropolitan Transportation Authority awarded CRRC with a $647 million contract to supply 282 subway cars, according to Reuters.

Winning mass transit contracts is just the first step in China's agenda to take over the U.S. freight rail sector, retired U.S. Brigadier General John Adams warned in a report he wrote for the U.S. industry group Rail Security Alliance in October last year.

"The Chinese government is banking on the fact that once CRRC secures sufficient U.S. municipal transit contracts, it can pivot quickly and inexpensively toward the more strategically important [U.S.] freight rail sector," Adams wrote.

Freight railroads play a key role in U.S. military operations, such as transporting military equipment to their destinations. The report warned that Chinese-made rail cars would provide Beijing knowledge of "early and reliable warning of U.S. military mobilization," based on information such as GPS train locations.

State Support for Overseas Growth

CRRC's aggressive push into the American market is tied to China's state industrial policies.

Sen. Baldwin explained in the press release about the new bill: "China has made clear its intent to dismantle U.S. railcar manufacturing in its 'Made in China 2025' plan—our economic and national security demands that we address Chinese attempts to dominate industries that build our nation's critical infrastructure."

Beijing rolled out "Made in China 2025" in May 2015, an industrial blueprint that envisions turning China into a manufacturing powerhouse in 10 tech sectors, including robotics, advanced information technology, advanced rail equipment, and aerospace.

The U.S. administration under President Donald Trump has criticized Made in China 2025 for abetting Chinese entities' theft of intellectual property, targeting primarily the United States and Europe, in pursuit of policy goals.

CRRC is also a key feature of Beijing's flagship foreign policy initiative, "One Belt, One Road." According to the company's website, Liu Hualong, who is both the firm's chairman and the Communist Party secretary, has publicly stated his support for the initiative on several occasions.

"One Belt, One Road" (OBOR, also known as "Belt and Road") is an investment initiative announced by Beijing in 2013, which aims to build up trade routes in Asia, Europe, and Africa through Chinese-financed infrastructure projects.

Under OBOR, CRRC signed a contract to provide rail cars for Pakistan's 27-kilometer (16.7 miles) metro line, according to CRRC's website. 27 trains were delivered in May 2017, according to Pakistani media reports.

According to a December 2018 article by Chinese state-run media China Daily, CRRC had 83 subsidiaries in 26 countries as of the end of 2017. 58 of the 83 were established after 2013, when OBOR was officially launched.

Domestic State Support

In recent years, CRRC also has been the beneficiary of many government subsidies. According to the company's website, it received a total of 1.298 trillion yuan ($193 billion) in subsidies in 2014 and 1.802 trillion yuan ($268 billion) in 2015.

While there are no public figures for how much CRRC received in the years since, the company also has received government research subsidies. For instance, in 2017, CRRC Zhuzhou Locomotive, a subsidiary of CRRC, received 10 million yuan ($1.5 million) in subsidies from the central government for digitizing its rail traction system. A year later, the company received 9 million yuan ($1.3 million) in subsidies for developing underwater robotics and selfless driving system projects.

CRRC's Liu is also a high-level Party official. He is a member of the Central Commission for Discipline Inspection, the Communist Party's internal anti-corruption watchdog.

Cybersecurity Concerns

Cybersecurity risks in U.S. public transportation systems were the topic of a Congressional hearing in February 2019, where vice president of the Rail Security Alliance, Erik Olson, spoke of the potential threats.

Olson pointed to the case of a procurement proposal issued by the Washington Metropolitan Transit Authority (WMATA) in September last year, which sought the acquisition of new subway cars, video surveillance, monitoring and diagnostics, data interface with WMATA, and automatic train control systems—all of which are vulnerable to cyber attacks, according to Olson.

Given China's history of cyber espionage and hacking, particularly targeting American businesses and government agencies, Olson stated that "We cannot trust a Chinese state-owned enterprise to build, own, or operate in U.S. critical infrastructure."

An example would be the June 2015 cyber attack against the U.S. Office of Personnel Management, which breached the personal records of roughly 4.2 million current and former federal employees. The attack has been attributed to Chinese entities.

There are more than 140,000 miles of track running through every major American city, according to U.S. statistics.

"Without action, America's industrial, military, and other government interests could be forced to rely significantly or wholly on rail cars made by the Chinese Government, thus creating massive cyber vulnerabilities that threaten our military and industrial security," Olson warned.

KAREN BLEIER/AFP/GETTY IMAGES

Patrons crowd the platform at the Washington Metropolitan Area Transit Authority's Metro Center Station in Washington, on Dec. 20, 2004.