(https://msadvisory.com)

Category	Locations
State-Level New Areas	Changsha City, Hunan Province Zhoushan City, Zhejiang Province Changchun City, Jilin Province Lanzhou City, Gansu Province Shanghai City Baoding City, Hebei Province Nanjing City, Jiangsu Province Jiujiang City and Nanchang City, Jiangxi Province Chengdu City and Meishan City, Sichuan Province Guizhou City and Anshun City, Guizhou Province Dalian City, Liaoning Province Tsingtao (Qingdao) City, Shandong Province Fuzhou City, Fujian Province Chongqing City Xi'an City and Xianyang (Hsienyang) City, Shaanxi Province Tianjin City Guangzhou City, Guangdong Province Kunming City, Yunnan Province Harbin City, Heilongjiang Province
Special Economic Zones	Shenzhen Hainan Kashgar Zhuhai Xiamen Khorgas Swatow (or Shantou)

(https://msadvisory.com)

Category	Locations
Pilot Free Trade Zones	Chongqing Tianjin Sichuan Liaoning Shanghai Zhejiang Fujian Guangdong Henan Hubei
Coastal Open Cities	Qinhuangdao Weihai Yingkou City Lianyungang Guangzhou Tianjin Shanghai Zhanjiang Qingdao Fuzhou Wenzhou Yantai Ningbo Dalian North Sea Nantong

Foreign Direct Investments (FDIs) and Their Role in SEZ Growth

Foreign Direct Investment (FDI) plays a vital part in the prosperity of SEZs. Aside from attracting capital, FDIs bring new technologies and management skills that promote learning in the local vicinity.

(https://msadvisory.com)

Manufacturing capacities also expand due to the influx of FDIs, generating more jobs for local Chinese employees.

What makes SEZs continuously attractive to FDIs are the cheap labor and good infrastructure available in the special zones. The open-door policies and generous incentives allowed money and labor to flow into China from the diaspora.

Factors Attracting FDI to Chinese SEZs

Reduced Duties on Imports: Lower import tariffs make it easier and cheaper for companies to bring necessary goods and materials.

Streamlined Administrative Control: Simplified bureaucratic processes help businesses operate more efficiently.

Greater Flexibility in Employment Policies: SEZs offer more adaptable labor regulations, making it easier for companies to hire and manage employees.

Preferential Fees for Land or Facility Use: Businesses benefit from lower costs for land and facilities within SEZs.

Concessionary Tax Breaks, Rates, and Exemptions: Companies enjoy various tax incentives that reduce operational costs.

Free or Low-Rent Business Accommodation: Affordable office and industrial

Advance Your Business in China

spaces enhance the attractiveness of SEZs.

Favorable Arrangements on Project Ownership, Size, Location, and Duration: SEZs provide advantageous project development and operation terms.

Overall, the policies' attractiveness makes China's SEZs highly viable for businesses that want to tap into the local market and take advantage of the numerous benefits available to them. (https://msadvisory.com)

Final Thoughts

Over the past few years, China has continued to enjoy the benefits that its SEZs supply to the local market. They are still encouraging more businesses to enter into and participate in SEZs. The tax breaks, low rents, reduced import duties, and employment flexibility businesses in the economic zones can benefit from are commensurate with the country's strong economic growth and stability. SEZs continue attracting foreign investors, increasing job creation and employment opportunities.

To establish a business in China's SEZ, you must navigate the complex requirements that the local and national governments enforce. Hiring local employees can also be challenging (https://msadvisory.com/hire-foreign-employees-china/) since different regions in China implement differing policies. As such, you will need the help of a partner who is well acquainted with the governing employment laws in China.

As a high-quality service provider, MSA has over a decade of experience supporting foreign enterprises in China. We are here to help you in this area and ensure your business complies with local and national employment regulations. Contact us (/contact/) for more information on our services in accounting, financial advisory, and corporate services.

Learn how we can help you **start**, **manage**, and **grow** your business in China.

First Name *

Last Name *

Business Email *

Phone Number

▾ (201) 555-0123

Company Name *

Contact Language *

English ▾

What business challenges can MSA help you address? *

Submit

Receive expert tips and local insights

By subscribing, you agree to MSA Privacy Policy (https://msadvisory.com/privacy-policy/).

First Name

Last Name

We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies.

EXHIBIT 112

The Select Committee on the CCP
Testimony by Donald H. Im
April 2024

Good morning Chaiman Gallagher, Ranking Member Krishnamoorthi and distinguished members.

Thank you for the opportunity to testify in regards to the economic impact of China's supply of synthetic chemicals leading to the deadly crisis killing tens of thousands of Americans every month. I'd like to caveat my testimony with the fact that this is my opinion and mine alone, based on my 31-years of experience, adjudicated investigations, open-source affidavits, and open-source academic studies.

As it is known, Mexican Cartels are the producers and traffickers of narcotics laced with synthetically produced fentanyl. These deadly poisons could not be produced without precursor chemicals manufactured in laboratories in China. But Mexican Cartels also produce methamphetamine, heroin and traffic cocaine into the United States generating billions of dollars in profit annually. The piles of cash are hidden in discreet houses or apartments in cities and towns where drugs are sold. Drug trafficking organizations need to launder these proceeds to safely integrate their profits into the legitimate economy.

In my 31 years with the Drug Enforcement Administration, I initiated, conducted, supervised, and supported hundreds of money laundering investigations and operations involving Colombian, Venezuelan, Panamanian, Mexican, Lebanese, and Chinese criminal organizations and networks throughout the world. We were able to penetrate these criminal entities with our drug money investigations that identified the sources of the illicit drugs, the chemists, the transporters, the distributors, terrorists, and, the money brokers. We also identified the key facilitators such as business entrepreneurs, bankers, lawyers, accountants and corrupt officials.

In the 1990's when I investigated Chinese Triads and heroin networks from Southeast Asia to the United States, or Colombian Medellin and Cali Cartels, a nexus to China began to appear, but leads sent to the DEA office in Beijing met with negative responses. And again, when I initiated the HSBC Bank investigation in 2007, we encountered Mexican, Chinese, Russian, Venezuelan, East and South African criminal networks as well as Middle East terrorist organizations, funneling and transferring funds through HSBC's global banking network. And again, leads into China-based state-owned banks, companies and manufacturers met with limited responses.

Limited Cooperation

Throughout the years, DEA made continuous efforts to provide leads, information, evidence and even training to People's Republic of China (PRC) law enforcement officials regarding various forms of money laundering. DEA also presented and produced information to Chinese government officials at the highest levels during the Bi-Lateral Counternarcotic Working Group meetings.

Outside of a handful of successful cooperative results, thousands of leads were met with silence or responses that, "a crime was not committed according to China's laws." Regardless of proven drug funds transferred into Chinese banks directly linked to a specified unlawful activity, even under Chinese law, they would reply that there were no crimes committed on Chinese soil. When we passed leads regarding a China-based company involved in drug or precursor chemical trafficking, Ministry of Public Security officials would ask for additional details of the company in question and the scope of our investigation. We subsequently determined and realized through sources, the targeted company, if owned or was linked to a Chinese Communist Party (CCP) member, would be notified and warned that US law enforcement authorities were either investigating or monitoring them. The DEA Fujing Zheng investigation being one of them.

Drug Money & Global Commerce

Early in my DEA career, I noticed the significant underlying symbiotic relationship between drug trafficking, banking and commerce. Primarily, because illicit drugs are a commodity in demand for money: Hundreds of billions of dollars' worth, throughout the world annually.

A 2017 Global Financial Integrity Report estimates that the value of global drug trafficking for the year 2014 alone, was between US $426 and US $652 Billion, with the United States as the leading drug consuming nation in the world. Now, I would estimate it even closer to US $1 trillion dollars annually.

What DEA uncovered in the 1980's during the period of unregulated money laundering, were the paths and conduits for illicit drug proceeds to become integrated in the legitimate economy. And since then, China's massive export economy has helped create the world's largest money laundering system, fueled by the multi-billion-dollar illicit drug industry. This global money laundering system is intertwined with the legitimate economy, expanding its reach in every alley, road, neighborhood, town, city, country, and more now than ever, over the world wide web in cryptocurrencies.

The myriad of tangible and intangible assets and value are purchased or bartered from the cash generated from the global drug trafficking industry and integrated as prepaid value and credit cards tethered to a slush fund, commodities, assets and values such as electronics, condominiums, properties, luxury items, expensive art, casino chips, favors, services, school tuitions, scholarships, job positions, vacations, political donations, home mortgage payoffs, and even as collateral on large bank loans with the borrower subsequently defaulting.

In the 2000's, China's economic expansion, coupled with their rapidly burgeoning economy, allowed Colombian and Mexican Cartels, a secure avenue to launder and conceal their illicit profits, all the while, helping fuel China's export economy. Since then, the need by drug cartels to repatriate their ill-gotten profits in US and European cities are being fulfilled by Chinese criminal networks and underground banks, operating cash businesses in North and Latin America and Europe.

The "Contract"

Chinese criminal money brokers charge Colombian or Mexican Cartels a "contract" fee of zero to 3% on the front end, to launder the piles of drug cash in US and European cities. On the back end, the Chinese brokers would then auction the amount on China's WeChat social media app, and under the eyes of PRC monitors, and charge commission fees of up to 20% over the base amount. Their associate networks structure the illicit cash into thousands of bank accounts in North America and Europe, and then layer and integrate the funds into assets or into other financial instruments.

For example, US $1 million in fentanyl and methamphetamine proceeds in New York City, will be auctioned on various WeChat rooms and Chinese citizens will bid to purchase the US $1 million for up to US $1.2 million. The citizen will not exchange US $1.2 million in Renminbi into US dollars and transfer it abroad, but the US $1.2 million in Renminbi will be transferred to Chinese manufacturing companies in China for various merchandise and commodities worth US $1.2 million and have it exported to those Chinese money brokers and/or businesses in Colombia, Mexico or Panama.

The products will be sold into the legitimate Colombian or Mexican economy, generating profits for those Chinese brokers, simultaneously, servicing as an ad hoc bank for Colombian and Mexican Cartels, who safely receive their ill-gotten wealth in their home currency. The US $1 million in the United States, is secured in bank accounts, in real estate, or other assets and even escrow accounts for college tuition, and are now owned by the Chinese citizen who purchased the US $1.2 million worth of exported merchandise. This is called: Trade Based Money Laundering (TBML).

While there are many other variations to this money laundering method, currently, it is the most optimal and effective way. This indirect, asymmetric processes of commercial and banking cycles are like separate wheels in a traditional wrist watch, triggered by illicit cash that churns other wheels simultaneously in other parts of the world, without a direct linear nexus between the illicit drugs and the billions converted into various forms of assets and value. This takes place daily between drug source countries, drug consuming countries and China.

China's strict capital flight restrictions implemented in 2016, limit Chinese citizens from transferring large sums of cash abroad. The TBML system has allowed many wealthy Chinese citizens and government officials a way to bypass these regulations and transfer billions in wealth to more stable economies. Those Chinese citizens know the proceeds are from drug trafficking or other criminal activities but will look the other way, or deny any knowledge of its source.

While Chinese criminal organizations launder Mexican and Colombian Cartel drug proceeds, the same Chinese criminal organizations and networks have been cultivating tens of thousands of marijuana farms and grows houses throughout the United States and Europe, namely, in states that legalized marijuana. With billions of dollars and Euros in profit generated, and with limited chances of being prosecuted and imprisoned, this lucrative cash cow has become a source of cheap capital, directly, or indirectly, for China's wealthy, provincial BRI projects, various debt, and for failing state-owned enterprises (SOE's) on the verge of bankruptcy. Furthermore, the expansion of marijuana cultivation sites combined with China's rising unemployment rate, continue to lure thousands of Chinese migrants into the United States to work in these sites generating massive profits that help create liquid capital for China-based entities.

Colombian and Mexican Drug Cartel profits generated in the United States and Europe, trigger hundreds of billion dollars' worth of Chinese merchandise and commodities exported to third party countries via TBML. This system is the most lucrative and elusive method of concealing the original sources of funds, and likely, causing skewed trade balance data between nations importing Chinese-manufactured products, all the while, allowing Chinese citizens to transfer vast amounts of capital out of China.

China's BRI – Drug Money & Corruption

When China began its global economic expansion strategy, the One Belt One Road Initiative (BRI) in 2013, the lynchpin to cooperative agreements with over 150 nations have always been capital. Funds to develop, design, and construct thousands of infrastructure projects creating a network of rail, road, shipping, air, and cyber connections. Chinese state-owned banks from various provinces in China provided cheap loans for capital to other Chinese SOE's to construct those key projects that support and sustain the BRI. Key industries and manufacturers from throughout China's provinces had been providing capital, goods and commodities, equipment, raw minerals and resources, and manpower, generating employment and profit, for China's growing capital market-economy.

These provincial governors and other CCP leaders compete with one another for higher positions based on economic performance in their province. Hence, the pursuit of economic growth and competition, created an atmosphere of reduced oversight, regulations, accountability and enforcement, leading to significant corruption throughout China's provincial governments, and even up to high level military and CCP party members.

Chinese Customs and Trade Ministry Officials in certain provinces either participated or and encouraged capital investment with incentives such as subsidies or reduced taxes and tariffs for exporting companies, or reduced inspections and laxed regulations. Many China-based chemical companies that supplied fentanyl precursors and illicit drugs benefited from these incentives for many years. Hundreds of billions of dollars of illicit drug proceeds have been laundered through the thousands of manufacturing companies exporting finished commodities and chemicals to Mexico, North, South and Central America, Africa, Europe and Middle East.

Chinese Companies Shift into Mexico

In the past 4 years, Mexico has taken over China as the largest exporter into the United States. Mostly due to the tariff war between the US and China, and the impact of COVID. China's exports to the United States have decreased since 2018 while Mexico's volume of exports into the United States have increased.

However, this direct reduction of trade between the United States and China does not necessarily result in a total loss for Chinese companies and SOEs, as more than 100 Chinese manufacturing companies are helping create approximately 18 industrial manufacturing parks throughout Mexico, all the while, allowing Chinese manufacturing companies to bypass US tariffs, and scrutiny.

Combining the lack of regulatory oversight, accountability, and enforcement, the creation of these industrial parks in Mexico with Chinese SOE's and manufacturing companies, potentially, will become susceptible, if not already, to Chinese criminal organizations and drug cartels.

A critical gap exists regarding the sources of capital generated and invested in industrial parks by both Mexican and Chinese companies. Previous DEA and HSI money laundering investigations have revealed hundreds of millions of dollars identified and traced into small and large businesses and even corporations for the purchase of construction materials, machinery, tools, industrial chemicals, vehicles, appliances, tires, and other necessary items.

Coordinated & Synchronized Measures

The threat from China can be resolved with the understanding that this deadly opioid crisis is not just about drug addiction; it's about crime; terrorism; national security; global commerce and banking; corruption; and greed.

Our inability to tackle this deadly crisis is underpinned by the lack of an integrated and coordinated effort between the sectors of government. In addition, there is a sense of indifference by US private sector corporations and banks, which, if reversed, could help mitigate this deadly crisis. Hundreds of billions of dollars in trade and services are exchanged by US corporations and banks, which can be leveraged to influence key Chinese provincial governors and industries in China and Mexico.

Conclusion

Mr. Chairman, Ranking Member, Honorable Committee. My fear is not China launching nuclear missiles or a military invasion against the United States, it's the degradation and destruction of our country by the allure of money exploiting society with deadly addictive poisons, cheap merchandise and tailored-made information and entertainment. Our country is undergoing an unrelentless attack of unrestrictive and asymmetric warfare, tactics for which our national security structure is currently ill suited to deter. And it’s all written and planned out.

I ask you and our leaders this one question: If Russia, not China, were manufacturing fentanyl precursor chemicals and selling them to ISIS terrorists instead of Mexican cartels, to traffic fentanyl-laced pills killing tens of thousands of Americans monthly, would we respond differently or continue with our current policies and funding?

EXHIBIT 113

U.S. DEPARTMENT OF THE TREASURY

U.S. Sanctions Suppliers of Precursor Chemicals for Fentanyl Production

April 14, 2023

WASHINGTON – Today, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) designated two entities in the People’s Republic of China (PRC) and five individuals, based in the PRC and Guatemala, for supplying precursor chemicals to drug cartels in Mexico for the production of illicit fentanyl intended for U.S. markets.

“Illicit fentanyl is responsible for the deaths of tens of thousands of Americans each year,” said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. “Treasury, as part of the whole-of-government effort to respond to this crisis, will continue to vigorously apply our tools to prevent the transfer of precursor chemicals and machinery necessary to produce this drug.”

This action was carried out in partnership and close coordination with the Drug Enforcement Administration and the Department of Justice.

DISRUPTING THE FLOW OF FENTANYL PRECURSOR CHEMICALS

Today, OFAC designated **Wuhan Shuokang Biological Technology Co., Ltd** (武汉硕康生物科技有限公司) (**WSBT**) and **Yao Huatao** (姚华涛) (**Yao**) pursuant to Executive Order (E.O.) 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production. Yao, a PRC national, is the sole owner of PRC-based chemical company WSBT—an entity responsible for the sale of fentanyl precursor chemicals—and, as its Executive Director, oversees the company’s operations. OFAC additionally designated WSBT for being owned, controlled, or directed by, or having acted or purported to act for or on behalf of, directly or indirectly, Yao.

OFAC also sanctioned three additional PRC nationals for their association with WSBT. **Wu Yaqin** (吴雅琴) (**Wu**) and **Wu Yonghao** (吴永昊) (**Yonghao**), sales representatives of Yao’s company

WSBT, not only negotiated and facilitated the sale of fentanyl precursor chemicals on the behalf of WSBT, but Wu also provided information on efficient preparation methods for synthesizing illicit fentanyl. **Wang Hongfei** (王洪飞) (**Wang**), a WSBT collaborator, is the owner of a cryptocurrency wallet that has been used to receive bitcoin payments for illicit drug transactions on behalf of WSBT.

On April 4, 2023, a federal grand jury in the U.S. District Court for the Southern District of New York (SDNY) indicted Yao, Wu, and Yonghao for various conspiracy charges including fentanyl importation and money laundering.

OFAC designated Wu and Yonghao pursuant to E.O. 14059 for being owned, controlled, or directed by, or having acted or purported to act for or on behalf of, directly or indirectly, Yao. OFAC additionally designated Wu and Yonghao pursuant to E.O. 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production.

OFAC designated Wang pursuant to E.O. 14059 for having provided or attempted to provide, financial, material, or technological support for, or goods or services in support of WSBT and Yao.

In 2021, PRC-based chemical company **Suzhou Xiaoli Pharmatech Co., Ltd** (苏州小栗医药科技有限公司) (**SXPC**) shipped 25 kilograms of N-BOC-4-Piperidone (CAS No.: 79099-07-3), a fentanyl precursor chemical to Guadalajara, Mexico with an ultimate destination in Sinaloa, Mexico. At the time of the N-BOC-4-Piperidone sale, the SXPC sales representative was aware that it would be used for the purpose of aiding in the manufacturing of illicit fentanyl and/or fentanyl pills. The SXPC sales representative additionally noted that SXPC was a supplier of fentanyl precursor chemicals for Mexico-based narcotics traffickers.

OFAC designated SXPC pursuant to E.O. 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production.

ILLICIT FENTANYL PRECURSOR BROKER IN GUATEMALA

Ana Gabriela Rubio Zea (**Rubio Zea**) is a Guatemala-based broker of fentanyl precursor chemicals who buys fentanyl precursor on behalf of Mexico-based drug traffickers. Rubio was the broker for the 25 kilograms of N-BOC-4-Piperidone, which was purchased from SXPC on behalf of the Sinaloa Cartel in Mexico. Rubio Zea has used her connections to PRC-based suppliers and chemical manufacturers to procure fentanyl precursor chemicals for the Sinaloa Cartel and to put Sinaloa Cartel traffickers in touch directly with those PRC-based suppliers, knowing that these chemicals would be used to manufacture fentanyl for ultimate distribution in the United States and elsewhere. Rubio Zea's primary fentanyl precursor chemicals suppliers include sales representatives at PRC-based chemical companies WSBT and SXPC.

In addition, Rubio Zea uses her expertise and contacts to ensure the safe delivery of precursors without detection by customs officials in Mexico or other countries. For example, Rubio Zea arranged for chemicals to be disguised in food containers or packaged alongside legal chemicals to avoid detection.

OFAC designated Rubio Zea pursuant to E.O. 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production.

On April 4, 2023, a federal grand jury in the U.S. District Court for SDNY indicted Rubio Zea for various conspiracy charges including fentanyl importation and money laundering. According to the indictment, Rubio Zea is directly connected to "Los Chapitos," a reference to four sons of notorious Mexican drug lord, Joaquin "El Chapo" Guzman Loera. Los Chapitos includes brothers Ivan Archivaldo Guzman Salazar and Jesus Alfredo Guzman Salazar, as well as their stepbrothers, Ovidio Guzman Lopez and Joaquin Guzman Lopez, the first three of whom were indicted by SDNY.

As high-ranking members of the Sinaloa Cartel—one of the largest and most powerful drug trafficking organizations in the world—Los Chapitos are involved in drug trafficking, money laundering, and violence. OFAC previously designated the Guzman Salazar brothers, as well as Ovidio Guzman Lopez, in 2012 pursuant to the Foreign Narcotics Kingpin Designation Act. The trio were designated again in 2021 pursuant to E.O. 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production.

The U.S. Department of State's Narcotics Reward Program announced reward offers from up to $1 million to up to $10 million for information leading to the arrest and/or conviction of several targets indicted today, including Yao, Wu, Yonghao, and Zea. For Yao, Wu, Yonghao, submit tips via email to ChapitosTips@dea.gov via Whatsapp at 1-202-743-1066. For Zea, tips may be submitted via email to ChapitosTips@dea.gov.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated individuals and entities that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked. OFAC's regulations generally prohibit all dealings by U.S. persons or within the United States (including transactions transiting the United States) that involve any property or interests in property of designated or otherwise blocked persons.

Today's action is part of a whole-of-government effort to counter the global threat posed by the trafficking of illicit drugs into the United States that is causing the deaths of tens of thousands of Americans annually, as well as countless more non-fatal overdoses. This action demonstrates the Administration's strengthened approach to saving lives by disrupting the trafficking of illicit fentanyl and its precursors into American communities. OFAC, in coordination OFAC, in coordination with its U.S. Government partners and foreign counterparts, will continue to target and pursue accountability for foreign illicit drug actors.

In addition, persons that engage in certain transactions with the individuals and entities designated today may themselves be exposed to sanctions or subject to an enforcement action.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the Specially Designated Nationals and Blocked Persons List (SDN List), but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC's Frequently Asked Question 897. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please click here.

Click here for identifying information on the individuals and entities designated today.

###

EXHIBIT 114

OFAC

Office of Foreign Assets Control

Sanctions List Search

Specially Designated Nationals and Blocked Persons list ("SDN List") and all other sanctions lists administered by OFAC, including the Foreign Sanctions Evaders List, the Non-SDN Iran Sanctions Act List, the Sectoral Sanctions Identifications List, the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions and the Non-SDN Palestinian Legislative Council List. Given the number of lists that now reside in the Sanctions List Search tool, it is strongly recommended that users pay close attention to the program codes associated with each returned record. These program codes indicate how a true hit on a returned value should be treated. The Sanctions List Search tool uses approximate string matching to identify possible matches between word or character strings as entered into Sanctions List Search, and any name or name component as it appears on the SDN List and/or the various other sanctions lists. Sanctions List Search has a slider-bar that may be used to set a threshold (i.e., a confidence rating) for the closeness of any potential match returned as a result of a user's search. Sanctions List Search will detect certain misspellings or other incorrectly entered text, and will return near, or proximate, matches, based on the confidence rating set by the user via the slider-bar. OFAC does not provide recommendations with regard to the appropriateness of any specific confidence rating. Sanctions List Search is one tool offered to assist users in utilizing the SDN List and/or the various other sanctions lists; use of Sanctions List Search is not a substitute for undertaking appropriate due diligence. The use of Sanctions List Search does not limit any criminal or civil liability for any act undertaken as a result of, or in reliance on, such use.

Download the SDN List | Sanctions List Search: Rules for use | Visit The OFAC Website

Download the Consolidated Non-SDN List | Program Code Key

Details:

Type:	Entity	**List:**	SDN
Entity Name:	WUHAN SHUOKANG BIOLOGICAL TECHNOLOGY CO., LTD	**Program:**	ILLICIT-DRUGS-EO14059
		Remarks:	(Linked To: YAO, Huatao)

Identifications:

Type	ID#	Country	Issue Date	Expire Date
Unified Social Credit Code (USCC)	91420100MA49RQRJ87	China		
Registration Number	420100001731665	China		
Organization Established Date	25 May 2021			
Organization Type:	Retail sale of pharmaceutical and medical goods, cosmetic and toilet articles in specialized stores			

Addresses:

Address	City	State/Province	Postal Code	Country
H05106, Building 1, No. 58, Guangxi Avenue, East Lake New Technology Development Zone	Wuhan	Hubei		China

Back

SDN List last updated on: 10/8/2024 10:03:42 AM
Non-SDN List last updated on: 9/30/2024 11:33:53 AM

EXHIBIT 115

Wed, September 11, 2024

Wuhan East Lake High-tech Development Zone
中国光谷
OPTICS VALLEY OF CHINA
National Innovation Demonstration Zone
China (Hubei) Pilot Free Trade Zone Wuhan Area

Search

Home Overview Media Center Industrial Parks Doing Business Communities Enterprises Conta

Home > Wuhan East Lake Free Trade Zone

Overview

Updated: 2024-03-04 (chinaopticsvalley.com)

Located in central East Lake High-tech Development Zone, Wuhan East Lake Free Trade Zone is a special customs supervision area functioning as a bonded logistics area and an export processing zone. It has a planned area of five square kilometers, 1.82 square kilometers of which went into operation in 2013.

[Photo/wehdz.gov.cn]

Proposed by the State Council, the free trade zone will build nine key platforms for bonded processing and manufacturing, international biomedicine, cross-border business services, bulk commodity trading, bonded stock exhibition, comprehensive services in foreign trade, international examination and maintenance, cross-border financial services and researches and design of bonded zones, respectively.

The zone will strengthen its role as a domestic and international hub of openness, innovation and ecology.

People can enjoy a series of services, including duty-free imports of equipment, bonded goods, tax rebates, and VAT and consumption tax-free transactions done within the territory.

It is free from the import and export quota license system, the bonded warehousing storage period, the bank deposit account system for processing enterprises, and foreign exchange offset procedures for imports and exports so taxes and transactions can be settled in a foreign currency or RMB.

Since the first phase of Wuhan East Lake Free Trade Zone started operations in June 2013, its export volume has increased from $343 million in 2013 to $6.714 billion in 2017.

As of April 2018, its total export volume had reached $18.2 billion, accounting for more than one-third of annual export volumes in the city of Wuhan, capital of central China's Hubei province.

Videos

Nicaraguan journalists visit Wuhan

Specials

Following the Belt and Roa Chinese chimes

In 2017, the trading volume of the zone's commodities trading platform topped 55 billion yuan ($7.91 billion), achieving tax revenue of 81 million yuan. Officials said Hubei's cross border e-commerce public service platform in the zone has attracted about 80 enterprises to complete filings and carry out business. Three business models for general imports, general exports and bonded imports have been developed in the zone.

The Wuhan East Lake Free Trade Zone is:

the first comprehensive bonded zone in the National Independent Innovation Demonstration Zone;

the first comprehensive bonded zone in Central China to carry out bonded exhibitions and trade;

first pilot reform and innovative comprehensive free trade zone in Hubei Province;

first comprehensive bonded zone included in provincial legislative protection;

first comprehensive bonded area in Hubei to realize tax rebates for water and electricity;

first comprehensive free trade zone in Hubei to provide comprehensive foreign trade services;

Hubei's first comprehensive bonded zone to launch cross-border e-commerce public service platforms;

first comprehensive bonded zone in the Wuhan Customs area to achieve seven days a week, 24-hour customs clearances of goods.

Overview
Profile
Policy Advantage
Capital Advantage
Talent Advantage
Innovation

Media Center
Updates
Specials
Videos

Parks
Biolake
Wuhan Future City
Wuhan East Lake Free Trade Zone
The Optoelectronic Information Industrial Park
Optics Valley Modern Service Industrial Park
Optics Valley Smart Manufacturing Industrial Park
Optics Valley Chinese Sci-tech City
Optics Valley Central City

Doing Business
Investment Environment
Investment Policies
Procedures
Approval Standards
Major Industries

Communities
Hotels
Dining
Tourism
Transportation
Education
Entertainment
Events
Shopping

Enterp
Overview
Compani
Quotes

Contac

Links: Beijing, China | International Services Shanghai | Wuhan Municipal People's Government | Zhongguancun Science Park

Presented by China Daily

EXHIBIT 116

An official website of the United States government Here’s how you know

U.S. DEPARTMENT OF THE TREASURY

Treasury Targets Large Chinese Network of Illicit Drug Producers

October 3, 2023

Action highlights U.S. whole-of-government approach to address fentanyl crisis

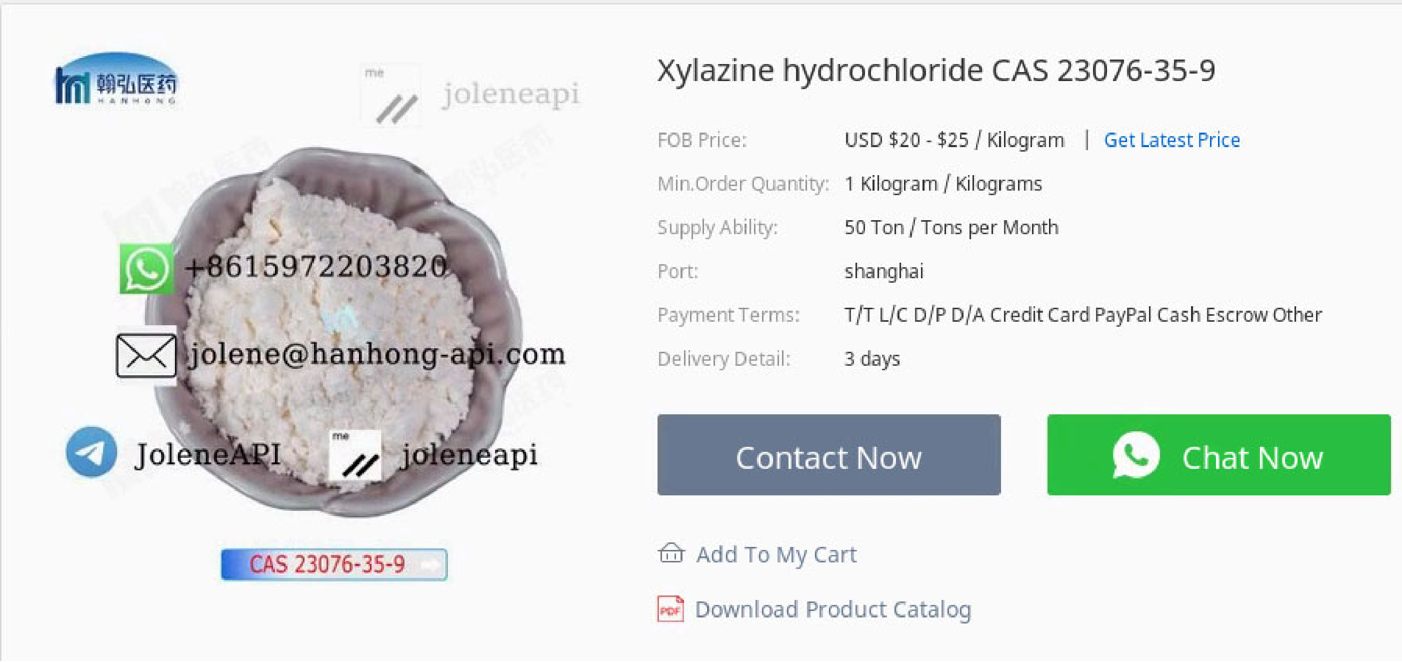
WASHINGTON — Today, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) designated 28 individuals and entities involved with the international proliferation of illicit drugs, including a China-based network responsible for the manufacturing and distribution of ton quantities of fentanyl, methamphetamine, and MDMA precursors. Those designated by OFAC today are also involved in the global trafficking of xylazine and “nitazenes,” which are highly potent and often mixed with illicit fentanyl or other drugs.

“Treasury is taking sweeping action with our colleagues in law enforcement to expose and disrupt a network responsible for manufacturing and distributing illicit drugs, including fentanyl and other substances that take thousands of American lives each year,” said Deputy Secretary of the Treasury Wally Adeyemo. “Today’s action from OFAC and IRS-CI reflects how we will swiftly use all of our tools to counter the global threat posed by the illicit drug trade.”

Treasury’s sanctions complement indictments issued today by the U.S. Attorneys Offices for the Southern District of Florida and the Middle District of Florida. For information on actions taken by the U.S. Department of Justice, please see this link.

These designations, which target 12 entities and 13 individuals based in China and two entities and one individual based in Canada pursuant to Executive Order (E.O.) 14059, would not have been possible without the cooperation, support, and ongoing collaboration between Treasury’s OFAC, Internal Revenue Service, Criminal Investigations, and Financial Crimes Enforcement Network, the Drug Enforcement Administration (DEA), and the Department of Homeland Security’s U.S. Customs and Border Protection agency. These partnerships highlight the Biden-Harris Administration’s strengthened whole-of-government offensive to save lives by disrupting illicit fentanyl supply chains around the globe.

This action follows a rapid increase in Treasury financial sanctions targeting the illicit fentanyl supply chain, including a recent action against China- and Mexico-based enablers of counterfeit pill production. Furthermore, this action demonstrates the importance of coordination amongst authorities in investigating precursor supply chains and disrupting financial flows of illicit drugs proceeds, as identified in the Financial Action Task Force's 2022 report on Money Laundering from Fentanyl and Synthetic Opioids.



Xylazine hydrochloride CAS 23076-35-9

FOB Price:	USD $20 - $25 / Kilogram | Get Latest Price
Min.Order Quantity:	1 Kilogram / Kilograms
Supply Ability:	50 Ton / Tons per Month
Port:	shanghai
Payment Terms:	T/T L/C D/P D/A Credit Card PayPal Cash Escrow Other
Delivery Detail:	3 days

***Hanhong Pharmaceutical Technology Co., LTD** posted this listing to an online chemical marketplace selling the veterinary sedative xylazine, also known by the street name "tranq."*

The networks targeted today have been involved in the trafficking of xylazine and "nitazenes" into the United States.

Xylazine, or "tranq," is a powerful sedative for veterinary use that is increasingly misused by narcotics traffickers who mix it with illicit fentanyl to produce a deadly mixture. According to a DEA public safety alert, fentanyl and xylazine mixtures are more potent than either drug alone, placing users at a higher risk of suffering a fatal drug overdose. Xylazine has also been coined the "zombie drug" because it can cause severe wounds in users, including necrosis — the rotting of human tissue — which may lead to amputation.

Nitazenes are also increasingly found mixed with illicit fentanyl or other drugs in the United States. Nitazenes are synthetic, non-fentanyl opioids. Metonitazene, butonitazene, isotonitazene, and protonitazene are examples of nitazenes gaining prevalence in the United States. Nitazenes vary in potency with some being considerably more potent than fentanyl, which is already approximately 100 times more potent than morphine and 50 times more potent than heroin. Known for their lethality, nitazenes are not approved for medical use in the United States.

DISRUPTION OF CHINA-BASED ILLICIT DRUGS SYNDICATE

Du Changgen

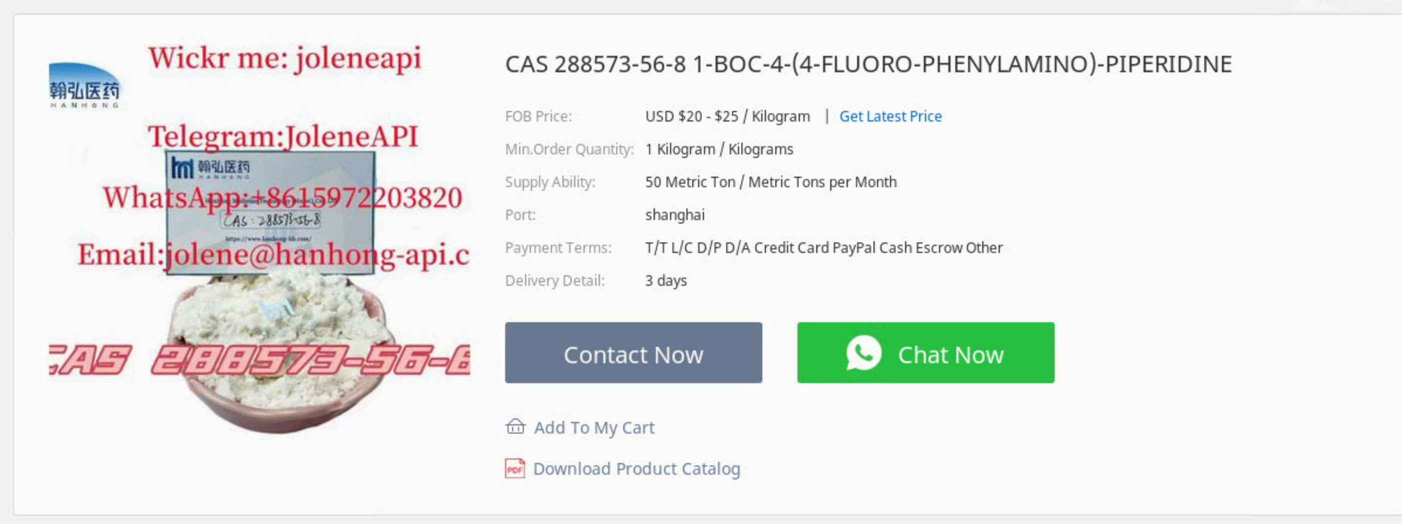
The actors designated today comprise, or are otherwise affiliated with, a Chinese illicit drugs syndicate (hereafter, the “Syndicate”). From at least 2016 on, **Wang Shucheng** (王树程) directed members of the Syndicate to establish companies that would be used for cover to move pharmaceutical products internationally. A member of the Syndicate previously under Wang Shucheng, **Du Changgen** (杜长根) has risen to prominence and currently maintains the greatest influence over the organization in its current state. Under Du Changgen’s leadership, the Syndicate is responsible for the manufacturing and distribution of ton quantities of nitazenes, fentanyl, methamphetamine, and MDMA precursors and various other illicit chemicals utilized to synthesize finished fentanyl, methamphetamine, and MDMA. The network is capable of synthesizing multi-thousand-kilogram quantities of the aforementioned substances, and Du Changgen and persons operating under him have been responsible for approximately 900 kilograms of seized fentanyl and methamphetamine precursors shipped to the United States and Mexico.

As the leader of the Syndicate, Du Changgen oversees a large group of sales teams based in China who communicate with their co-conspirators via encrypted messaging. These groups of individuals send and receive funds through virtual currency, bank-wire transfers, and other financial transactions. Du Changgen himself has personally received virtual currency in exchange for shipments of fentanyl precursors. The Syndicate is the source of supply for dozens of narcotics traffickers in the United States, dark web vendors, virtual currency money launderers, and Mexico-based criminal organizations such as the Sinaloa Cartel and the Jalisco New Generation Cartel (CJNG). The Sinaloa Cartel and CJNG have been designated by OFAC pursuant to the Foreign Narcotics Designation Kingpin Act and E.O. 14059.

Du Changgen is the owner of Hong Kong-based **Hubei Vast Chemical Co., Limited** (湖北翰弘化工有限公司) (Hubei Vast), Hong Kong-based **Hebei Guanlang Biotechnology Co., Limited** (河北冠朗生物科技有限公司) (Hebei Biotechnology Limited), China-based **Hebei Xiuna Trading Co., LTD.** (河北休纳商贸有限公司) (Hebei Xiuna), and China-based **Shanghai Jarred Industrial Co., LTD.** (上海嘉瑞德实业有限公司) (Shanghai Jarred). Highlighting the interrelated nature of the persons designated today, Wang Shucheng is the legal supervisor of Shanghai Jarred.

Du Changgen was designated today pursuant to E.O. 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production. Hubei Vast, Hebei Biotechnology Limited, Hebei Xiuna, and Shanghai Jarred were designated today pursuant to E.O. 14059 for being owned, controlled, or directed by, or for having acted or purported to act for or on behalf of, directly or indirectly, Du Changgen. Wang Shucheng was designated today pursuant to E.O. 14059 for being or having been a leader or official of Shanghai Jarred.

Hanhong Pharmaceutical Technology Co., LTD and its Representatives



CAS 288573-56-8 1-BOC-4-(4-FLUORO-PHENYLAMINO)-PIPERIDINE

FOB Price:	USD $20 - $25 / Kilogram | Get Latest Price
Min.Order Quantity:	1 Kilogram / Kilograms
Supply Ability:	50 Metric Ton / Metric Tons per Month
Port:	shanghai
Payment Terms:	T/T L/C D/P D/A Credit Card PayPal Cash Escrow Other
Delivery Detail:	3 days

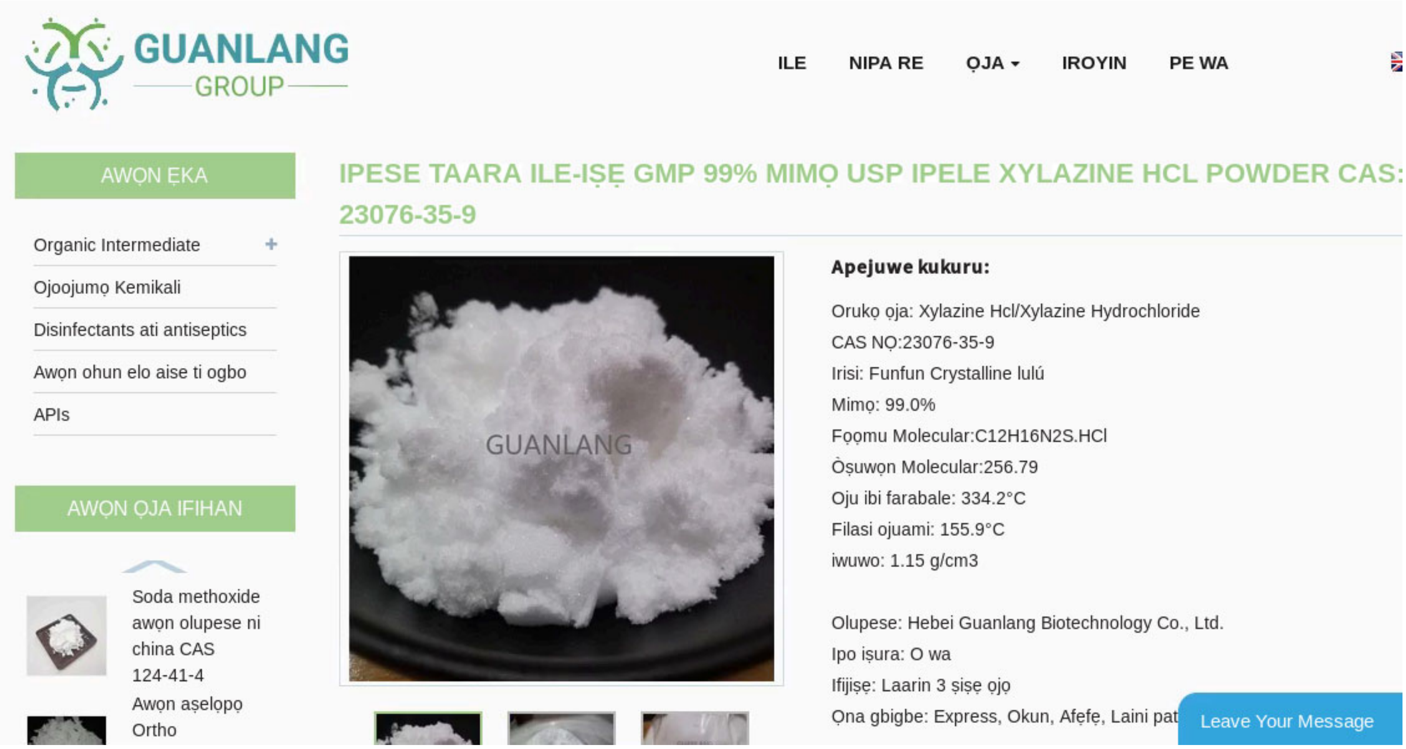
Hanhong Pharmaceutical posted this listing to an online chemical marketplace selling 288573-56-8, a fentanyl precursor with no known legitimate use.

In addition to the aforementioned entities, Du Changgen owns **Hanhong Pharmaceutical Technology Co., LTD** (湖北翰弘化工有限公司) (Hanhong Pharmaceutical), which is directly and indirectly linked to multiple Syndicate members. Hanhong Pharmaceutical has advertised the sale of fentanyl precursors to Mexican customers and its sales representatives have communicated with Mexico-based persons linked to the Sinaloa Cartel and to illicit fentanyl trafficking.

Gan Xuebi (甘雪碧) a.k.a Bella Chen, **Song Xueqin** (宋雪琴) a.k.a. Shelly Song, and **Yang Qi** a.k.a. Daisy Yang are sales representatives for Hanhong Pharmaceutical and have been points of contact for Hanhong Pharmaceutical's sale of fentanyl precursors and protonitazene. Each of them have been involved in illicit drugs-related activity in these positions: Gan Xuebi has communicated with multiple persons linked to illicit fentanyl trafficking, including those linked to the Sinaloa Cartel; Song Xueqin has illicitly distributed chemicals to a Mexico-based drug trafficking organization; and Yang Qi has been involved in negotiations for the purchase of chemicals with a U.S.-based narcotics distributor, who later received illicit chemicals from Hanhong Pharmaceutical itself.

Hanhong Pharmaceutical, Gan Xuebi, Song Xueqin, and Yang Qi were designated today pursuant to E.O. 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production.

Additional Syndicate Members and Entities



IPESE TAARA ILE-IṢẸ GMP 99% MIMỌ USP IPELE XYLAZINE HCL POWDER CAS: 23076-35-9

Apejuwe kukuru:

Orukọ ọja: Xylazine Hcl/Xylazine Hydrochloride
CAS NỌ:23076-35-9
Irisi: Funfun Crystalline lulú
Mimọ: 99.0%
Fọọmu Molecular:C12H16N2S.HCl
Ọ̀ṣuwọn Molecular:256.79
Oju ibi farabale: 334.2°C
Filasi ojuami: 155.9°C
iwuwo: 1.15 g/cm3

Olupese: Hebei Guanlang Biotechnology Co., Ltd.
Ipo iṣura: O wa
Ifijiṣẹ: Laarin 3 ṣiṣẹ ọjọ
Ọna gbigbe: Express, Okun, Afẹfẹ, Laini pat

*Screenshot from **Hebei Guanlang Biotechnology Co., LTD.**'s website selling xylazine.*

Hebei Guanlang Biotechnology Co., LTD. (河北冠朗生物科技有限公司) (Hebei Guanlang) is an entity that publicly advertises the sale of fentanyl and methamphetamine precursors. In one example of its illicit drugs-related activity, a Hebei Guanlang sales representative provided a virtual currency address in exchange for methylamine hydrochloride, a methamphetamine precursor. **Gao Lanfang** (高兰芳) is the owner and an official of Hebei Guanlang. **Wang Mingming (**王明明) is also an official of Hebei Guanlang. Wang Mingming's virtual currency addresses have received payments in exchange for fentanyl and methamphetamine precursor chemicals.

Gao Lanfang, **Wang Mingjing** (王明镜), previously designated Wang Hongfei (王洪飞), and others transacted with a U.S.-based illicit drugs distributor who later pled guilty to felony narcotics charges following the death of a teenager. Wang Mingjing is an official of Hebei Xiuna and the founder of **Hebei Crovell Biotech Co., LTD.** (河北克拉维尔生物科技有限公司) (Hebei Crovell), a vendor of fentanyl-analogs whose employees market and export drugs, as well as manufacture them. Hebei Crovell has also publicly advertised the sale of 4-anilinopiperidene, a fentanyl precursor, as well as precursor chemicals of other illicit drugs.

The chief executive of Hebei Crovell is **Zhang Wei** (张伟). Zhang Wei has received virtual currency payments in exchange for illicit drugs-related transactions, including for methylamine hydrochloride. Further demonstrating how the Syndicate operates, Hebei Crovell shares over a dozen phone numbers and overlapping contacts with **Qingdao Cemo Technology Develop Co., LTD** (青岛盛茂科技发展有限公司) (Qingdao Cemo). Qingdao Cemo sales representatives offer various substances used to make illicit drugs such as fentanyl and methamphetamine. Wang Tianmin (王天民) is an owner and official of Qingdao Cemo, as well as a registered owner of **Hebei Yaxin Restaurant Management Co., LTD.** (河北雅新餐饮管理有限公司) (Hebei Yaxin).

Hebei Guanlang, Hebei Crovell, and Qingdao Cemo were designated today pursuant to E.O. 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production. Gao Lanfang was designated today pursuant to E.O. 14059 for being or having been a leader or official of Hebei Guanlang. Zhang Wei was designated today pursuant to E.O. 14059 for being or having been a leader or official of Hebei Crovell. Wang Mingjing was designated today pursuant to E.O. 14059 for being or having been a leader or official of Hebei Xiuna. Wang Tianmin was designated today pursuant to E.O. 14059 for being or having been a leader or official of Qingdao Cemo. Hebei Yaxin was designated today pursuant to E.O. 14059 for being owned, controlled, or directed by, or for having acted or purported to act for or on behalf of, directly or indirectly, Wang Tianmin. Wang Mingming was designated today pursuant to E.O. 14059 for being or having been a leader or official of Hebei Guanlang.

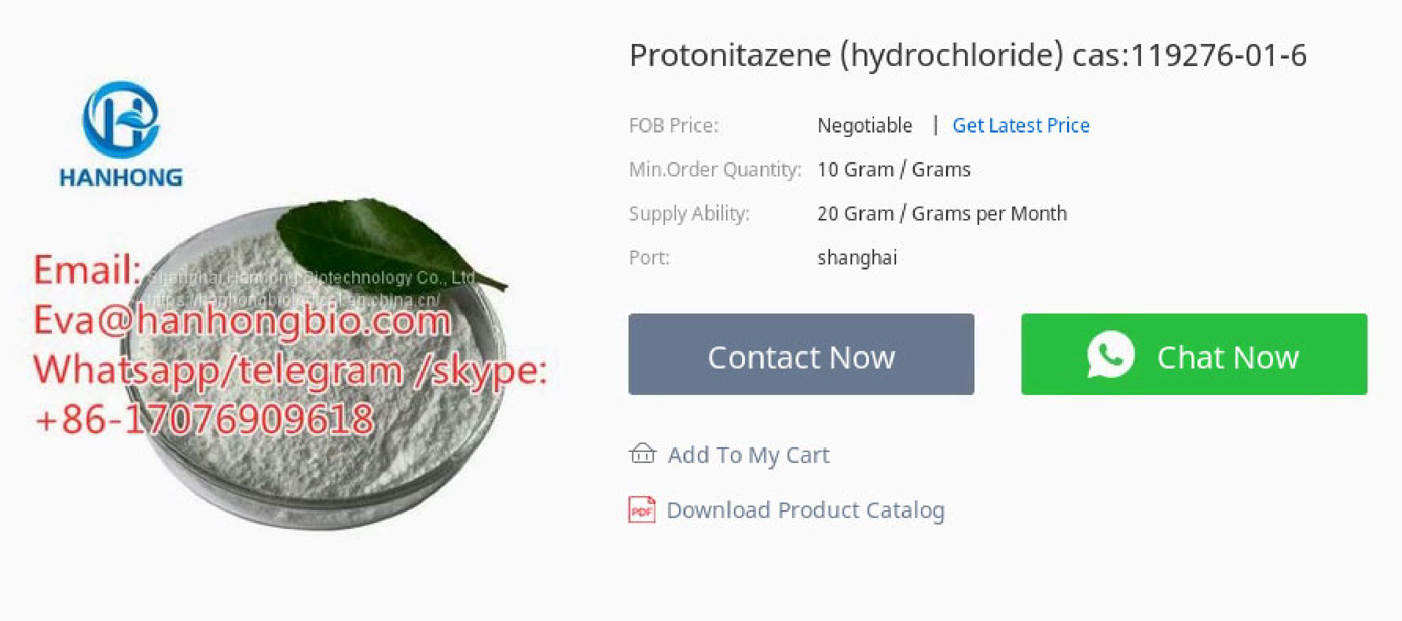
TARGETING ADDITIONAL ILLICIT DRUGS ACTIVITY

Punch and Die Manufacturer

Jinhu Minsheng Pharmaceutical Machinery Co. LTD. (金湖明生制药机械有限公司) (Jinhu Minsheng) is a China-based entity that advertises punches and dies for tablet presses with pharmaceutical imprints on e-commerce platforms and has provided pill dies for counterfeit oxycodone M30 tablets. **Shen Xingbiao** (沈兴标) is an official and part-owner of Jinhu Minsheng. On behalf of Jinhu Minsheng, Shen Xingbiao has made efforts to sell pill press machines and a pill die in exchange for funds in virtual currency.

Jinhu Minsheng and Shen Xingbiao were designated today pursuant to E.O. 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production.

Illicit Drugs Distributors



Protonitazene (hydrochloride) cas:119276-01-6

FOB Price:	Negotiable | Get Latest Price
Min.Order Quantity:	10 Gram / Grams
Supply Ability:	20 Gram / Grams per Month
Port:	shanghai

Hanhong Pharmaceutical posted this listing to an online chemical marketplace in which it offered protonitazene for sale.

A major customer of Jinhu Minsheng's is Western Canada-based **Valerian Labs, Inc.,** which is led by Canadian national **Bahman Djebelibak** (Djebelibak) a.k.a. Bobby Shah. Valerian Labs, Inc. shares its British Columbia address with **Valerian Labs Distribution Corp**., which is owned by Djebelibak. Djebelibak is a distributor of illicit precursor chemicals and equipment used to produce an array of synthetic drugs.

Valerian Labs, Inc. has received shipments of methylamine hydrochloride, which is a precursor chemical used to produce methamphetamine and MDMA. Valerian Labs Distribution Corp. has attempted to procure 2,000 liters of chloroform, 800 liters of dichloromethane, and 200 kg of iodine, substances used in the production of fentanyl, heroin, and methamphetamine.

Notably, Valerian Labs Distribution Corp. has imported chemicals from Hebei Guanlang, which as previously mentioned, is a member of the Syndicate targeted today.

Valerian Labs, Inc., Bahman Djebelibak, and Valerian Labs Distribution Corp. were designated today pursuant to E.O. 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production.

Today's designations of **Jiangsu Bangdeya New Material Technology Co., LTD.** (江苏邦得雅新材料科技有限公司) (Jiangsu Bangdeya) and several of its enablers further highlights the multi-layered role of drug trafficking organizations. Jiangsu Bangdeya has offered illicit substances for sale, including chemicals associated with fentanyl and methamphetamine production, as well as protonitazene and xylazine. Jiangsu Bangdeya and its sales representative and part-owner, **Wang Jiantong** (王建通), have sent protonitazene to the United States in exchange for funds in virtual currency. **Xia Fengbing** (夏凤兵) is the owner of a virtual currency address used to receive payment for Jiangsu Bangdeya's sales of illicit drugs-related substances. This virtual currency address was specifically used to receive payment from a U.S.-based individual. In addition, **Xingtai Dong Chuang New Material Technology Co., LTD.** (邢台东创新材料科技有限公司) (Xingtai Dong Chuang) has accepted wire payments on behalf of Jiangsu Bangdeya. Xingtai Dong Chuang is affiliated with Yip Chuen Fat (Ye Chuanfa), who was previously designated pursuant to E.O. 14059 on December 15, 2021.

Jiangsu Bangdeya, Wang Jiantong, and Xia Fengbing were designated today pursuant to E.O. 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production. Xingtai Dong Chuang was designated today pursuant to E.O. 14059 for being owned, controlled, or directed by, or for having acted or purported to act for or on behalf of, directly or indirectly, Jiangsu Bangdeya.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated individuals and entities that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons. U.S. persons may face civil or criminal penalties for violations of E.O. 14059.

Today's action is part of a whole-of-government effort to counter the global threat posed by the trafficking of illicit drugs into the United States that is causing the deaths of tens of thousands of Americans annually, as well as countless more non-fatal overdoses. This action demonstrates the Administration's strengthened approach to saving lives by disrupting the trafficking of illicit fentanyl and its precursors into American communities. These efforts are part of the Biden-Harris Administration's comprehensive, whole-of-government strategy to tackle the nation's overdose epidemic, which goes after two key drivers of this crisis: untreated addiction and the drug trafficking profits that fuel it. Today's action will help strengthen public safety by disrupting the illicit drug production and trafficking pipeline that profits by harming Americans. As a key part of the President's Unity Agenda, the Administration has also made historic investments in critical public health interventions including research, prevention, treatment, and recovery support services.

OFAC, in coordination with its U.S. Government partners and foreign counterparts, will continue to target and pursue accountability for foreign illicit drug actors. In addition, persons that engage in certain transactions with the individuals and entities designated today may themselves be exposed to sanctions or subject to an enforcement action.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the Specially Designated Nationals and Blocked Persons List (SDN List), but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC's Frequently Asked Question 897. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please click here.

View more information, including virtual currency wallet addresses, on the individuals and entities designated today.

###

EXHIBIT 117

Office of Foreign Assets Control

Sanctions List Search

Specially Designated Nationals and Blocked Persons list ("SDN List") and all other sanctions lists administered by OFAC, including the Foreign Sanctions Evaders List, the Non-SDN Iran Sanctions Act List, the Sectoral Sanctions Identifications List, the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions and the Non-SDN Palestinian Legislative Council List. Given the number of lists that now reside in the Sanctions List Search tool, it is strongly recommended that users pay close attention to the program codes associated with each returned record. These program codes indicate how a true hit on a returned value should be treated. The Sanctions List Search tool uses approximate string matching to identify possible matches between word or character strings as entered into Sanctions List Search, and any name or name component as it appears on the SDN List and/or the various other sanctions lists. Sanctions List Search has a slider-bar that may be used to set a threshold (i.e., a confidence rating) for the closeness of any potential match returned as a result of a user's search. Sanctions List Search will detect certain misspellings or other incorrectly entered text, and will return near, or proximate, matches, based on the confidence rating set by the user via the slider-bar. OFAC does not provide recommendations with regard to the appropriateness of any specific confidence rating. Sanctions List Search is one tool offered to assist users in utilizing the SDN List and/or the various other sanctions lists; use of Sanctions List Search is not a substitute for undertaking appropriate due diligence. The use of Sanctions List Search does not limit any criminal or civil liability for any act undertaken as a result of, or in reliance on, such use.

Download the SDN List | Sanctions List Search: Rules for use | Visit The OFAC Website

Download the Consolidated Non-SDN List | Program Code Key

Details:

Type:	Entity	**List:**	SDN
Entity Name:	HANHONG PHARMACEUTICAL TECHNOLOGY CO., LTD.	**Program:**	ILLICIT-DRUGS-EO14059
		Remarks:	

Identifications:

Type	ID#	Country	Issue Date	Expire Date
Unified Social Credit Code (USCC)	91420111MA4KP9GA7L	China		
Organization Established Date	03 Nov 2016			
Phone Number	862786832068			
Website	www.hanhong-med.com			

Aliases:

Type	Category	Name
f.k.a.	strong	HANHONG MEDICINE TECHNOLOGY HUBEI CO., LTD.

Addresses:

Address	City	State/Province	Postal Code	Country
H0781, Bldg. 1, No. 58 Guanggu Road East Lake New Technology Development Zone	Wuhan	Hubei Province	430000	China

Back

SDN List last updated on: 10/8/2024 10:03:42 AM
Non-SDN List last updated on: 9/30/2024 11:33:53 AM

EXHIBIT 118

OFAC
Office of Foreign Assets Control

Sanctions List Search

Download the SDN List · Sanctions List Search: Rules for use · Visit The OFAC Website

Download the Consolidated Non-SDN List · Program Code Key

Details:

Type:	Entity	**List:**	SDN
Entity Name:	YASON GENERAL MACHINERY CO., LTD.	**Program:**	ILLICIT-DRUGS-EO14059
		Remarks:	

Identifications:

Type	ID#	Country	Issue Date	Expire Date
Unified Social Credit Code (USCC)	91440300586742510R	China		
Phone Number	8675536528786			
Phone Number	8618170079734			
Organization Established Date	30 Nov 2011			
Website	www.ytkmachine.com			
Website	www.ytkpack.com			
Website	www.medpacking.com			
Email Address	worldyason@live.com			
Email Address	jelly-yason@outlook.com			

Aliases:

Type	Category	Name
a.k.a.	strong	SHENZHEN YASON GENERAL MACHINERY CO., LTD.
a.k.a.	strong	YASON GENERAL MACHINERY MANUFACTURING CO., LTD.

Addresses:

Address	City	State/Province	Postal Code	Country
301A, Fl. 3, No. 17 III of Xinxiang Industrial Park Xinhe Street New and Emerging Industrial Area (A) Fuhai Street, Baoan District	Shenzhen	Guangdong Province	518000	China
Floor 3, Bldg 1, (Zone A) Zone 3 Xinhe Xinxing Ind. Zone Fuyong Street, Baoan Dist.	Shenzhen	Guangdong		China
No 188-23, Xiangming RD, Fengcheng Town, Anxi County	Quanzhou	Fujian		China

Back

SDN List last updated on: 10/8/2024 10:03:42 AM
Non-SDN List last updated on: 9/30/2024 11:33:53 AM

EXHIBIT 119

An official website of the United States government Here’s how you know

U.S. DEPARTMENT OF THE TREASURY

Treasury Sanctions China- and Mexico-Based Enablers of Counterfeit, Fentanyl-Laced Pill Production

May 30, 2023

Action Taken in Coordination with U.S. Law Enforcement and the Government of Mexico

WASHINGTON — Today, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) sanctioned 17 individuals and entities involved in the international proliferation of equipment used to produce illicit drugs. These targets are directly or indirectly involved in the sale of pill press machines, die molds, and other equipment used to impress counterfeit trade markings of legitimate pharmaceuticals onto illicitly produced pills, often laced with fentanyl, frequently destined for U.S. markets.

“Treasury’s sanctions target every stage of the deadly supply chain fueling the surge in fentanyl poisonings and deaths across the country,” said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. “Counterfeit pills laced with fentanyl constitute a leading cause of these deaths, devastating thousands of American families each year. We remain committed to using all authorities against enablers of illicit drug production to disrupt this deadly global production and counter the threat posed by these drugs.”

These designations, which target seven entities and six individuals based in China and one entity and three individuals based in Mexico, would not have been possible without the cooperation, support and ongoing collaboration among OFAC; the Drug Enforcement Administration (DEA), including the Special Operations Division; Homeland Security Investigations (HSI), and its El Paso Field Office; and the Department of Homeland Security’s U.S. Customs and Border Protection (CBP) agency. These partnerships highlight the Biden-Harris Administration’s strengthened whole-of-government offensive to save lives by disrupting illicit fentanyl supply chains around the globe. Pertaining to Mexico-based persons sanctioned today, this action was also coordinated closely with the Government of Mexico, including the Unidad de Inteligencia Financiera (Mexico’s Financial Intelligence Unit).

PILL PRESS AND COUNTERFEIT PILL TYPOLOGY

Examples of pill presses used in the production of illcit drugs laced with fentanyl.

A pill press — also called a tablet press or a tableting machine — is a mechanical device that compresses powdered substances into tablets of uniform size and weight. The U.S. government regulates pill press machine importation. These machines vary in size and capacity, each of which can produce thousands of pills daily. The lack of controls and safeguards in illicit pill production often results in inconsistent and lethal dosages.

Illicit drugs in pill form, including those laced with fentanyl, may be blank or bear custom impressions. They may also be counterfeits of scheduled drugs, bearing trademarked wordmarks without authorization, such as “M30” for schedule II oxycodone products or “Xanax” for schedule IV alprazolam products.

Manufacturing illicit drugs in pill form requires a pill press machine, a controlled substance, and die molds — metallic pill press components bearing impressions that are punched onto pills. A die is fixed to a pill press machine in order to punch repeated impressions during pill mass-production. If the impressions on a die and on the pills it punches mimic trademarked pharmaceuticals, the die and impressed pills are counterfeit.

Facilitation of equipment importation by bad actors is sometimes attempted in a manner designed to evade law enforcement scrutiny, which can include the mislabeling of shipments, the use of circuitous shipment routes, and the shipment of equipment parts in piecemeal fashion.

DISRUPTING FACILITATORS OF COUNTERFEIT PILL PRODUCTION

Today, OFAC designated Chinese pill press supplier **Youli Technology Development Co., Ltd**. (尤里科技发展有限公司) (**Youli**) along with three Youli-affiliated Chinese nationals, **Guo Chunyan** (郭春艳), **Guo Yunnian** (郭运年), and **Guo Ruiguang** (郭瑞光), all located in Huizhou, China. Youli has shipped pill press machinery to individuals in the United States involved in the manufacture of counterfeit pills. Youli ships the machinery using techniques intended to evade law enforcement scrutiny. In addition, Youli has shipped scheduled pharmaceuticals to the United States for counterfeit pill manufacturing. Guo Chunyan and Guo Yunnian have supplied pill presses and dies to drug traffickers operating in the United States, including those involved with fentanyl-laced pills production.

OFAC designated Youli, Guo Chunyan, and Guo Yunnian pursuant to Executive Order (E.O.) 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production. OFAC designated Guo Ruiguang pursuant to E.O. 14059 for having acted or purported to act for or on behalf of, directly or indirectly, Youli.

OFAC also designated Shenzhen, China-located **Yason General Machinery Co., Ltd.** (亚新通用机械有限公司) (**Yason**), Hong Kong-registered but Shenzhen, China-based **Yason Electronics Technology Co., Limited** (亞新電子科技有限公司) (**Yason Electronics**), and Nanchang, China-located **Shenzhen Yason General Machinery Co., Ltd. Nanchang Branch** (深圳市亚新通用机械有限公司南昌分公司) (**Yason Nanchang**), interrelated Chinese companies implicated in the supply of press equipment internationally. OFAC additionally designated Yason and Yason Electronics company official **Fei Yiren** (费亿人) (**Fei**), a Chinese national.

Yason sells pill press-related equipment and has worked with a Mexico-based pill equipment supplier and contact who previously provided equipment to a Sinaloa Cartel-linked individual. This individual used the machines to create superlabs in Mexico with the capacity to produce millions of fentanyl-laced pills weekly. In 2017, Yason Electronics sent a pill press machine — in multiple packages and via the United States — to the contact in Mexico, the intended buyer of the equipment.

OFAC designated Yason and Yason Electronics pursuant to E.O. 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production. OFAC designated Fei pursuant to E.O. 14059 for being or having been a leader or official of Yason and of Yason Electronics. OFAC designated Yason Nanchang pursuant to E.O. 14059 for being owned, controlled, or directed by, or having acted or purported to act for or on behalf of, directly or indirectly, Fei.

Today's designations also include **Mexpacking Solutions** (**Mexpacking**), a Chihuahua, Mexico-based business that sells pill presses and other equipment and is controlled by a Sinaloa Cartel pill press supplier. The business has been used as cover for an individual involved with making fentanyl-laced pills and with assisting Mexico-based cartel members with pill press operations. Goods from Mexpacking were shipped to another pill press equipment supplier involved with coordinating shipments of pill press machines and parts to drug trafficking organizations, including the Sinaloa Cartel.

Along with Mexpacking, OFAC designated three related individuals, all Mexican nationals: **Mario Ernesto Martinez Trevizo** (**Martinez**), **Cinthia Adriana Rodriguez Almeida** (**Rodriguez**), and **Ernesto Alonso Macias Trevizo** (**Macias**). Martinez, a sales representative with Mexpacking, as of late 2022, was responsible for managing activities of a pill press supply network in Mexico, the head of which supplied pill press equipment the Sinaloa Cartel used. In this role, Martinez maintained business communications with China-based supplier Yason Electronics, which between 2019 and 2022 provided the network with numerous pill press machines and "M30" die molds. Rodriguez, as of late 2022, had a senior role in the pill press equipment supply network, which likewise necessitates coordination with Chinese supplier Yason Electronics. Between 2015 and 2021 Rodriguez also assisted with illicit drug production, including illicit drugs in pill form. Macias is a sales associate for Mexpacking.

OFAC designated Mexpacking, Martinez, and Rodriguez pursuant to E.O. 14059 for having engaged in, or attempting to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production. OFAC designated Macias pursuant to E.O. 14059 for having acted or purported to act for or on behalf of, directly or indirectly, Mexpacking.

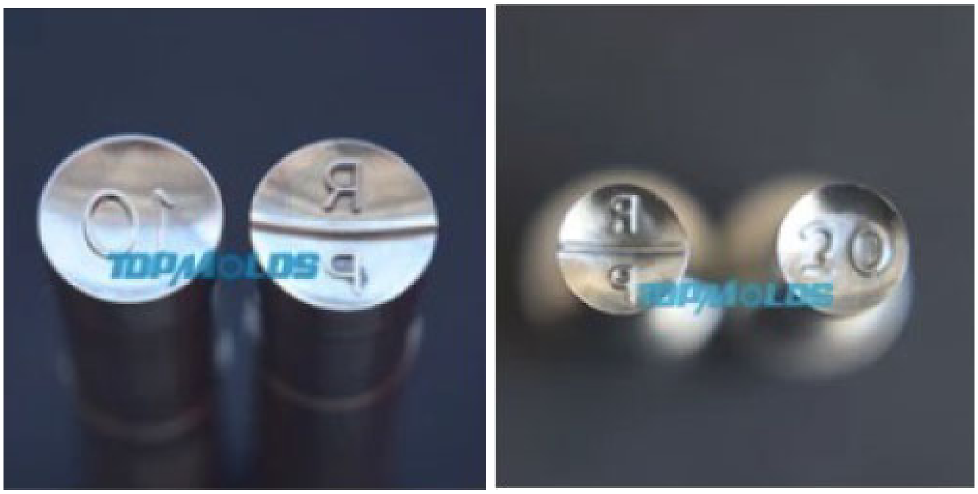
Lastly, OFAC designated online business **Tdpmolds**, an entity established and controlled by **Zhao Dongdong** (赵冬冬) (**Zhao**), a Chinese national located in Yantai, China. In addition to Tdpmolds, OFAC designated Chinese nationals and entities Zhao, **Pan Hao** (潘昊) (**Pan**), **Yantai**

Yixun International Trade Co., Ltd. (烟台易迅国际贸易有限公司) (**Yantai Yixun**), and **Yantai Mei Xun Trade Co., Ltd.** (烟台美讯商贸有限公司) (**Yantai Mei Xun**).

Counterfeit “Xanax” dies for schedule IV alprazolam products, sold online by Tdpmolds.

Tdpmolds offers a range of pill press machines and dies for sale, and as recently as 2020, Tdpmolds shipped to the United States several pill press die molds, including ones used to produce counterfeit schedule II oxycodone and amphetamine pill products. As of 2019, “Xanax” dies used in support of U.S.-based pill press operations and sourced from Tdpmolds were seized by U.S. authorities. In that same year, Tdpmolds was also the source of other dies, including a counterfeit “M30” die, also used in U.S.-based criminal pill press operations. In 2019 and 2020, Zhao sold pill presses and die sets to individuals in the United States who used the equipment to produce pills with scheduled substances, including counterfeit pills marked with “M30” and “Xanax.” In 2019 and 2020, Pan facilitated the sale from Tdpmolds to the United States of dies used to manufacture counterfeit pills. As of 2019, Yantai Yixun was the source of equipment used by a U.S.-based drug trafficker involved with an illicit pill manufacturing business using dies to counterfeit scheduled drugs.

OFAC designated Tdpmolds, Zhao, Pan, and Yantai Yixun pursuant to E.O. 14059 for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production. OFAC additionally designated Yantai Yixun for being owned, controlled, or directed by, or having acted or purported to act for or on behalf of, directly or indirectly, Zhao. OFAC designated Yantai Mei Xun pursuant to E.O. 14059 for being owned, controlled, or directed by, or having acted or purported to act for or on behalf of, directly or indirectly, Pan.



RP 10 & RP 30 Oxycodone Hydrochloride (schedule II) Dies Sold online by Tdpmolds.

COUNTERFEIT PILL-RELATED RESOURCES

In 2021, the DEA issued a Public Safety Alert to warn the American public about the dangers of fake prescription pills containing fentanyl. DEA updated its “One Pill Can Kill” media campaign information in 2022 to indicate a dramatic increase in the potency and lethality of fentanyl pills. Laboratory testing revealed that six out of ten fentanyl-laced counterfeit pills analyzed in 2022 contained lethal doses of the drug, which represented an increase from 2021 figures. The announcement, which links to an accompanying DEA “One Pill Can Kill” social media campaign, and urges all Americans to take only medications prescribed by medical professionals and dispensed by licensed pharmacists, can be found here.

SANCTIONS IMPLICATIONS

As a result of today’s action, all property and interests in property of the designated persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC’s regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons. U.S. persons may face civil or criminal penalties for violations of E.O. 14059.

Today's action is part of a whole-of-government effort to counter the global threat posed by the trafficking of illicit drugs into the United States that is causing the deaths of tens of thousands of Americans annually, as well as countless more non-fatal overdoses. OFAC, in coordination with its U.S. Government and foreign partners, will continue to target and pursue accountability for foreign illicit drug actors.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the Specially Designated Nationals and Blocked Persons List (SDN List), but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC's Frequently Asked Question 897 here. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please click here.

For more information on the individuals and entities designated today, click here.

###

EXHIBIT 120

OFAC
Office of Foreign Assets Control

Sanctions List Search

Specially Designated Nationals and Blocked Persons list ("SDN List") and all other sanctions lists administered by OFAC, including the Foreign Sanctions Evaders List, the Non-SDN Iran Sanctions Act List, the Sectoral Sanctions Identifications List, the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions and the Non-SDN Palestinian Legislative Council List. Given the number of lists that now reside in the Sanctions List Search tool, it is strongly recommended that users pay close attention to the program codes associated with each returned record. These program codes indicate how a true hit on a returned value should be treated. The Sanctions List Search tool uses approximate string matching to identify possible matches between word or character strings as entered into Sanctions List Search, and any name or name component as it appears on the SDN List and/or the various other sanctions lists. Sanctions List Search has a slider-bar that may be used to set a threshold (i.e., a confidence rating) for the closeness of any potential match returned as a result of a user's search. Sanctions List Search will detect certain misspellings or other incorrectly entered text, and will return near, or proximate, matches, based on the confidence rating set by the user via the slider-bar. OFAC does not provide recommendations with regard to the appropriateness of any specific confidence rating. Sanctions List Search is one tool offered to assist users in utilizing the SDN List and/or the various other sanctions lists; use of Sanctions List Search is not a substitute for undertaking appropriate due diligence. The use of Sanctions List Search does not limit any criminal or civil liability for any act undertaken as a result of, or in reliance on, such use.

Download the SDN List | Sanctions List Search: Rules for use | Visit The OFAC Website

Download the Consolidated Non-SDN List | Program Code Key

Details:

Type:	Entity	**List:**	SDN
Entity Name:	XINGTAI DONG CHUANG NEW MATERIAL TECHNOLOGY CO., LTD.	**Program:**	ILLICIT-DRUGS-EO14059
		Remarks:	(Linked To: JIANGSU BANGDEYA NEW MATERIAL TECHNOLOGY CO., LTD.)

Identifications:

Type	ID#	Country	Issue Date	Expire Date
Unified Social Credit Code (USCC)	91130531MA0GFM1G0U	China		
Organization Established Date	15 Jun 2021			
Website	https://dongchuangchem.com			
Phone Number	8615803390859			

Aliases:

Type	Category	Name
a.k.a.	strong	XINGTAI DONG INNOVATIVE MATERIAL TECHNOLOGY CO., LTD.

Addresses:

Address	City	State/Province	Postal Code	Country
No. 201, Fengjiazhai Industrial Zone Fengjiazhai Town Guangzong County	Xingtai City	Hebei Province		China

Back

SDN List last updated on: 10/8/2024 10:03:42 AM
Non-SDN List last updated on: 9/30/2024 11:33:53 AM

EXHIBIT 121

北方电力
NORTHERN ELECTRIC POWER

Northern Electric Power Hospital Recruitment (Beijing Electric Power Hospital

2024-08-15

What are the state-owned enterprises in Hebei Province?

State-owned enterprises in Hebei Province include Shijiazhuang Development Zone Metalda Microelectronics Technology Develo Ceramic Group Ceramic Machinery Factory, Hebei Shijiazhuang Yafeng Chemical Factory, Hebei Chemical Industry Research Instit Province also include the State-owned Hanguang Machinery Factory, China Light Industry Machinery Shijiazhuang Company, Xua Jiannan Hospital, etc.

Hebei Iron and Steel Group is one of the largest state-owned enterprises in Hebei Province, mainly involved in steel manufacturin businesses. Introduction to Hebei Iron and Steel Group: Hebei Iron and Steel Group is a large enterprise managed by the State-ov Commission of Hebei Province, and is also one of the important steel producers in China. The group has advanced production te products include steel and steel plates, which are widely used in many industries such as construction, machinery, and automobil Outsiders should not be fooled. Some town gas in Hebei is state-owned, and Hebei Natural Gas Co., Ltd. is a state-owned enterpr CSPC Pharmaceutical Group is one of the first large-scale pharmaceutical companies in the pharmaceutical industry to be establis the important enterprise groups in Hebei Province. The group was established on August 21, 1997 and is headquartered in Shijia Group was awarded the title of "National Innovative Enterprise" in 2010. Huaneng Shang'an Power Plant Huaneng Shang'an Powe County, Shijiazhuang City, Hebei Province, and is located in Jingxingkou, on the eastern foot of Taihang Mountain.

"China-made 'Rocket' steam locomotive". Kailuan Coal Mine has left a strong mark in the history of China's national industrial dev Group Co., Ltd. (abbreviated as: Jizhong Energy) is a large state-owned enterprise in Hebei Province. It was established in June 20 reorganized North China Pharmaceutical Group. In June 2010, Jizhong Energy established Hebei Airlines Group and Hebei Airline

How much does it cost for non-locals to give birth in Beijing Electric Power Hospit

1. I don’ t know. My wife also saw that she needed to create a record at the Electric Power Hospital, but we all gave birth at the F

2. Liangxiang Hospital, Fangshan Hospital, Fangshan Traditional Chinese Medicine Hospital, Liangxiang Maternal and Child Health

3. Generally speaking, you can give birth in a regular hospital, but some people are willing to spend more money for peace of mi nothing wrong with the Electric Hospital, which is not crowded and saves money. Of course, the premise is that you don’ t have a

4. [1] Maternal and Child Health Record Handbook. [2] File creation at 6-8 weeks of pregnancy [3] The examination results of this pregnancy file in the obstetrics department. After confirming the pregnancy, first use the file creation calculator to check whether on the last menstrual period and make a file creation plan.

What are the major Chinese-funded enterprises in Pakistan?

1. The core businesses of Chinese enterprises in Pakistan include road and bridge construction, power construction, real estate de communication services, electromechanical products, building materials, international trade, international logistics, factories, expl are thousands of large, medium and small state-owned enterprises, private enterprises and joint ventures.

2. If the China-Pakistan relationship is so strong, why can't China's automobile industry and car companies export to Pakistan? In such as FAW, Foton Motor, JAC Motors and Dongfeng Motor, but they are mainly engaged in truck and light truck business.

3. According to the World Ports and Inland Points Index Handbook published by the People's Communications Press, Pakistan has Karachi, Ktibandar, Krongi, Ormara, Pasni, Port Qasim, and Sonmiani.

4. CMEC, Dongfang Electric, Harbin Electric, and Siemens also tried it, but it was not successful. In addition, a Czech company wer

EXHIBIT 122

UA: 216/16 Index: ASA 17/4869/2016 China

Date: 23 September 2016

URGENT ACTION

FALUN GONG PRACTITIONER SAID TO HAVE BEEN TORTURED IN DETENTION

Falun Gong practitioner Chen Huixia was unable to stand or walk after being tortured, according to a fellow detainee. Suffering from chronic illness and poor health, she currently has no access to her family or a lawyer.

Chen Huixia, along with eight other Falun Gong practitioners, was taken away by police in Shijiazhuang Municipality, Hebei Province, on 3 June 2016. Her family was only notified on 16 July that she was being criminally detained in the Shijiazhuang Municipal No. 2 Detention Centre on the suspicion of “using an evil cult to undermine law enforcement”.

A Falun Gong practitioner who was taken away with Chen Huixia, but has since been released, told her daughter that Chen Huixia, 59, had been strapped to a chair with metal bars and tortured to the point of being unable to stand or walk. She was further subjected to “brainwashing” sessions to get her to renounce her belief.

Chen Huixia’s nephew visited the detention centre on 12 August but was prevented from seeing her. One of the lawyers that was approached by her relatives, which include a judge and a police officer, said that the authorities would not allow him to take the case. No direct contact has been made with Chen Huixia since June and without any access to a lawyer, her family fear for her well-being.

Please write immediately in English, Chinese or your own language:

- Urging authorities to immediately and unconditionally release Chen Huixia, as she has been detained solely for exercising the right to freedom of belief and expression.
- Urging the authorities to ensure that while detained, Chen Huixia is protected from torture or other ill-treatment, and that her treatment is in accordance with the UN Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules).
- Pending her release, urging the authorities to ensure that she has prompt, regular and unrestricted access to her family and lawyers of her choice, and medical care on request or as necessary, .

PLEASE SEND APPEALS BEFORE 4 NOVEMBER 2016 TO:

Director of Shijiazhuang Municipal No. 2 Detention Centre
Shijiazhuang Shi Dier Kanshousuo
Zhaoling Lu, Changan Qu,
Shijiazhuang Shi
Hebei Sheng, 050000
People’s Republic of China
Salutation: Dear Director

Director of Shijiazhuang Municipal Public Security Bureau
Liu Sheng,
Shijiazhuang Shi Gongan Ju
66 Yuannan Lu, Qiaodong Qu
Shijiazhuang Shi
Hebei Sheng 050000
People's Republic of China
Tel: +86 311 8686 2222 (Chinese only)
Salutation: Dear Director

Governor of Hebei Province
Zhang Qingwei,
Hebeisheng Renmin Zhengfu
113 Yuhuadong Lu, Changan Qu
Shijiazhuang Shi
Hebei Sheng 050000
People’s Republic of China
Tel: +86 311 8790 2359 (Chinese only)
Salutation: Dear Governor

Also send copies to diplomatic representatives accredited to your country. Please insert local diplomatic addresses below:

Name Address 1 Address 2 Address 3 Fax Fax number Email Email address Salutation Salutation

Please check with your section office if sending appeals after the above date.

AMNESTY
INTERNATIONAL

URGENT ACTION

FALUN GONG PRACTITIONER SAID TO HAVE BEEN TORTURED IN DETENTION

ADDITIONAL INFORMATION

According to her daughter, Chen Huixia started practicing Falun Gong in 1998 to heal her chronic illness and poor health. She was consequently detained for about three months in 2003 and following her release her family has been subjected to persistent harassment and intimidation by authorities.

The spiritual movement Falun Gong was banned in China for being a "threat to social and political stability" after its practitioners held a peaceful sit-in on Tiananmen Square in July 1999. In response, the government established a dedicated office, the “610 Office”, to oversee the crackdown on the Falun Gong and other “heretical cults”.

As a result, tens of thousands of Falun Gong practitioners have been arbitrarily detained and, often through the use of torture and other ill-treatment, made to renounce their spiritual beliefs. Since the 2013 abolition of “Re-Education Through Labour” (RTL) facilities, Chinese authorities are using alternate methods of arbitrary detention, including the criminal prosecution of individuals.

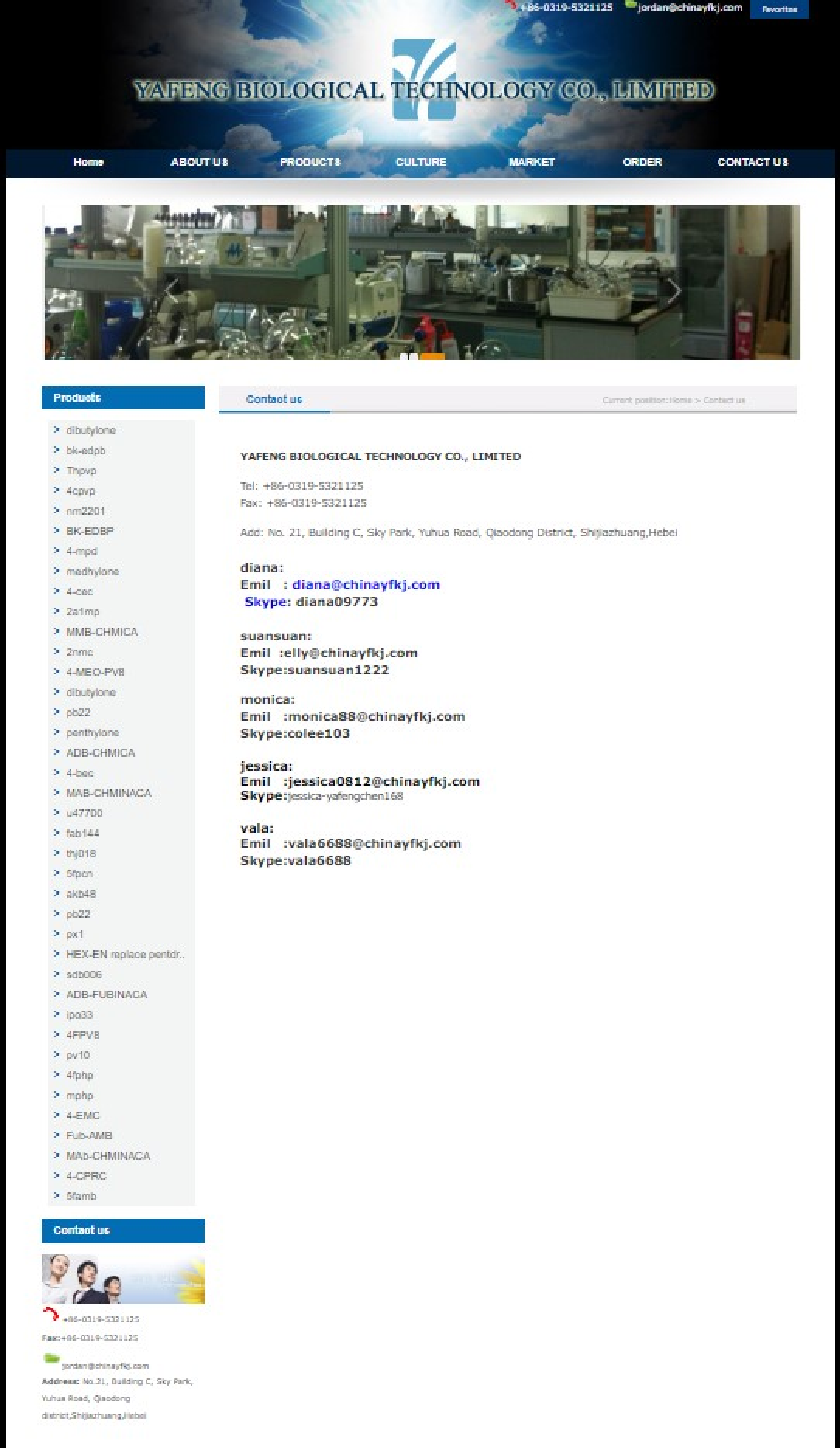
Torture and other ill-treatment are endemic in all forms of detention, although China ratified the UN Convention Against Torture in 1988. Amnesty International receives regular reports of deaths in custody, often caused by torture. Other inmates and “cell bosses” are used by detention centre and prison authorities to monitor the behaviour of fellow inmates and mete out punishment including subjecting resistant detainees to sleep deprivation, stress positions, as well as other physical and mental forms of torture or other ill-treatment.

The criminal justice system in China is roughly divided into three distinct phases: the police-led investigation, the prosecution phase, in which the prosecutors approve of the initial evidence needed to arrest a suspect and engages in further investigation to decide whether to indict a suspect; and the final trial phase carried out by the courts. Similar to previous years, the conviction rate in 2015 was higher than 99.9%, making it very important to voice concerns as early in the criminal justice process as possible, preferably before the decisions to arrest or indict suspects are even made.

Name: Chen Huixia
Gender m/f: Female

UA: 216/16 Index: ASA 17/4869/2016 China Issue Date: 23 September 2016

EXHIBIT 123



+86-0319-5321125 jordan@chinayfkj.com Favorites

YAFENG BIOLOGICAL TECHNOLOGY CO., LIMITED

Home ABOUT US PRODUCTS CULTURE MARKET ORDER CONTACT US

Products

- dibutylone
- bk-edpb
- Thpvp
- 4cpvp
- nm2201
- BK-EDBP
- 4-mpd
- medhylone
- 4-cec
- 2a1mp
- MMB-CHMICA
- 2nmc
- 4-MEO-PV8
- dibutylone
- pb22
- penthylone
- ADB-CHMICA
- 4-bec
- MAB-CHMINACA
- u47700
- fab144
- thj018
- 5fpcn
- akb48
- pb22
- px1
- HEX-EN replace pentdr..
- sdb006
- ADB-FUBINACA
- ipo33
- 4FPV8
- pv10
- 4fphp
- mphp
- 4-EMC
- Fub-AMB
- MAb-CHMINACA
- 4-CPRC
- 5famb

Contact us

☎ +86-0319-5321125

Fax:+86-0319-5321125

jordan@chinayfkj.com

Address: No.21, Building C, Sky Park, Yuhua Road, Qiaodong district,Shijiazhuang,Hebei

Contact us

Current position:Home > Contact us

YAFENG BIOLOGICAL TECHNOLOGY CO., LIMITED

Tel: +86-0319-5321125
Fax: +86-0319-5321125

Add: No. 21, Building C, Sky Park, Yuhua Road, Qiaodong District, Shijiazhuang,Hebei

diana:
Emil : diana@chinayfkj.com
Skype: diana09773

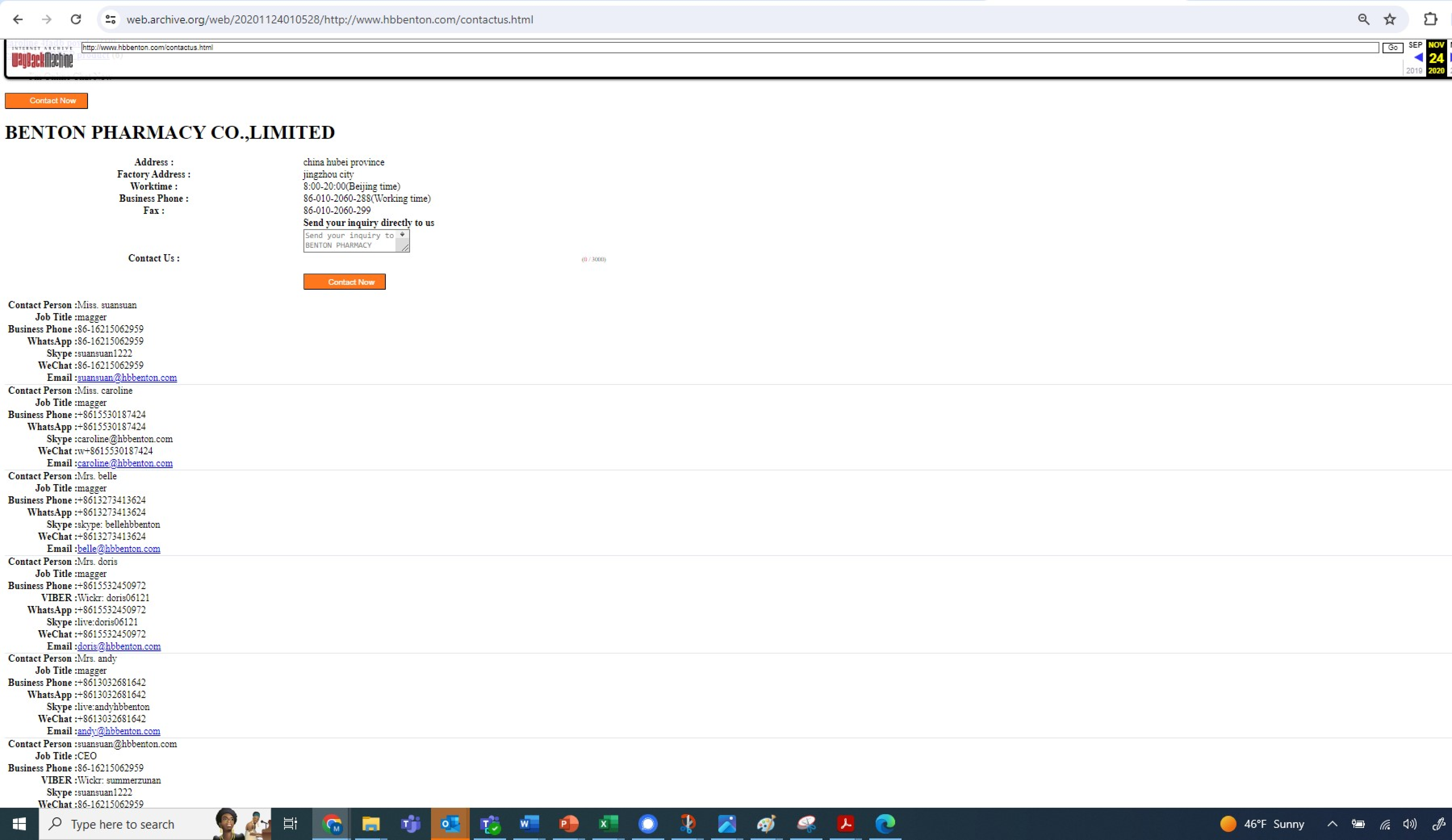
suansuan:
Emil :elly@chinayfkj.com
Skype:suansuan1222

monica:
Emil :monica88@chinayfkj.com
Skype:colee103

jessica:
Emil :jessica0812@chinayfkj.com
Skype:jessica-yafengchen168

vala:
Emil :vala6688@chinayfkj.com
Skype:vala6688

EXHIBIT 124


web.archive.org/web/20201124010528/http://www.hbbenton.com/contactus.html
INTERNET ARCHIVE
WaybackMachine
http://www.hbbenton.com/contactus.html
Go
SEP
NOV
24
2019
2020
Type here to search
46°F Sunny

Contact Now

BENTON PHARMACY CO.,LIMITED

Address : china hubei province
Factory Address : jingzhou city
Worktime : 8:00-20:00(Beijing time)
Business Phone : 86-010-2060-288(Working time)
Fax : 86-010-2060-299

Contact Us : **Send your inquiry directly to us**

Send your inquiry to BENTON PHARMACY

(0 / 3000)

Contact Now

Contact Person : Miss. suansuan
Job Title :magger
Business Phone :86-16215062959
WhatsApp :86-16215062959
Skype :suansuan1222
WeChat :86-16215062959
Email :suansuan@hbbenton.com

Contact Person : Miss. caroline
Job Title :magger
Business Phone :+8615530187424
WhatsApp :+8615530187424
Skype :caroline@hbbenton.com
WeChat :w+8615530187424
Email :caroline@hbbenton.com

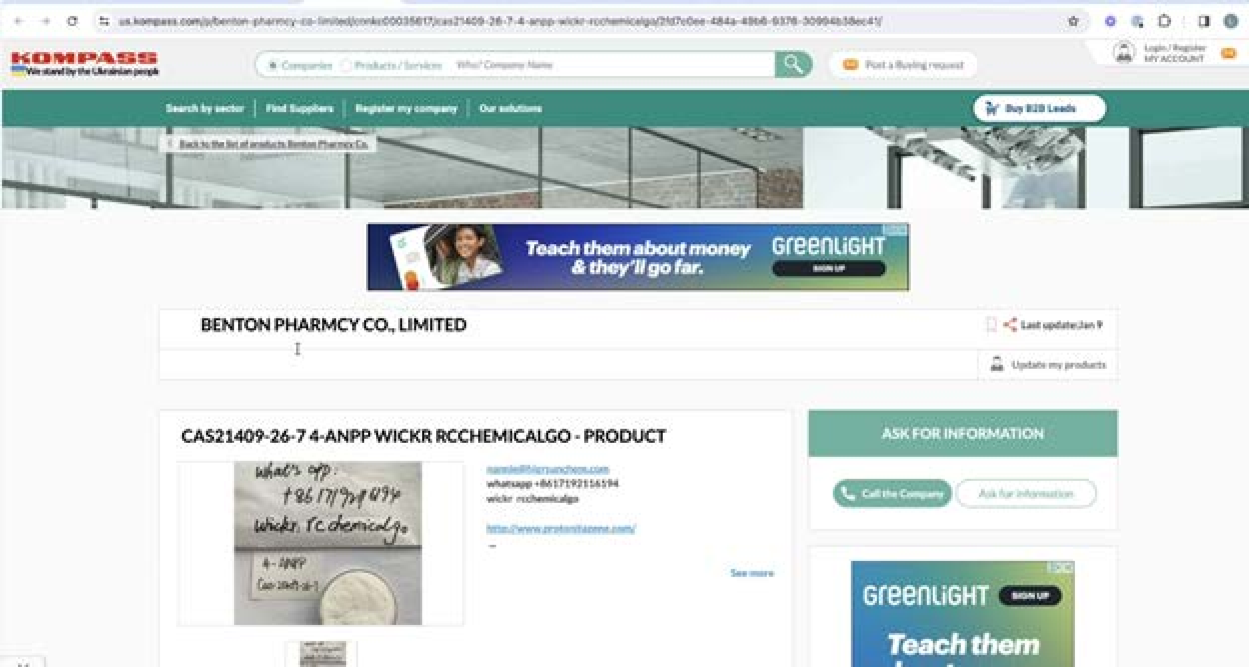
Contact Person : Mrs. belle
Job Title :magger
Business Phone :+8613273413624
WhatsApp :+8613273413624
Skype :skype: bellehbbenton
WeChat :+8613273413624
Email :belle@hbbenton.com

Contact Person : Mrs. doris
Job Title :magger
Business Phone :+8615532450972
VIBER : Wickr: doris06121
WhatsApp :+8615532450972
Skype :live:doris06121
WeChat :+8615532450972
Email :doris@hbbenton.com

Contact Person : Mrs. andy
Job Title :magger
Business Phone :+8613032681642
WhatsApp :+8613032681642
Skype :live:andyhbbenton
WeChat :+8613032681642
Email :andy@hbbenton.com

Contact Person :suansuan@hbbenton.com
Job Title :CEO
Business Phone :86-16215062959
VIBER : Wickr: summerzunan
Skype :suansuan1222
WeChat :86-16215062959

EXHIBIT 125



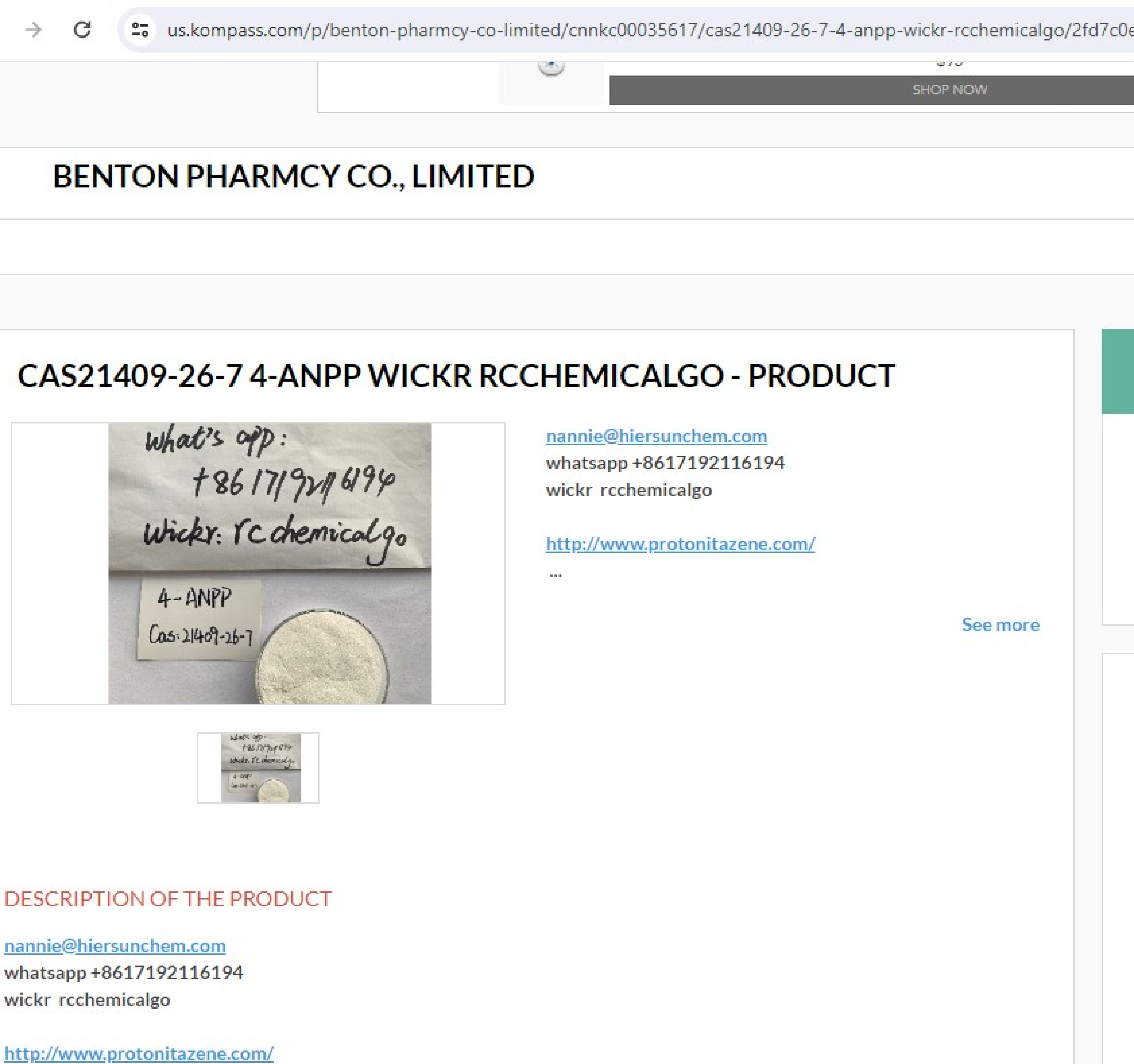
us.kompass.com/p/benton-pharmcy-co-limited/cnmkc00035817/cas21409-26-7-4-anpp-wickr-rcchemicalgo/2fd7c0ee-484a-4866-8376-30994b38ec41/

BENTON PHARMCY CO., LIMITED

CAS21409-26-7 4-ANPP WICKR RCCHEMICALGO - PRODUCT

nannie@hjrunchem.com
whatsapp +8617192116594
wickr rcchemicalgo

http://www.protonitazene.com/



us.kompass.com/p/benton-pharmcy-co-limited/cnnkc00035617/cas21409-26-7-4-anpp-wickr-rcchemicalgo/2fd7c0e

BENTON PHARMCY CO., LIMITED

CAS21409-26-7 4-ANPP WICKR RCCHEMICALGO - PRODUCT

nannie@hiersunchem.com
whatsapp +8617192116194
wickr rcchemicalgo

http://www.protonitazene.com/
...

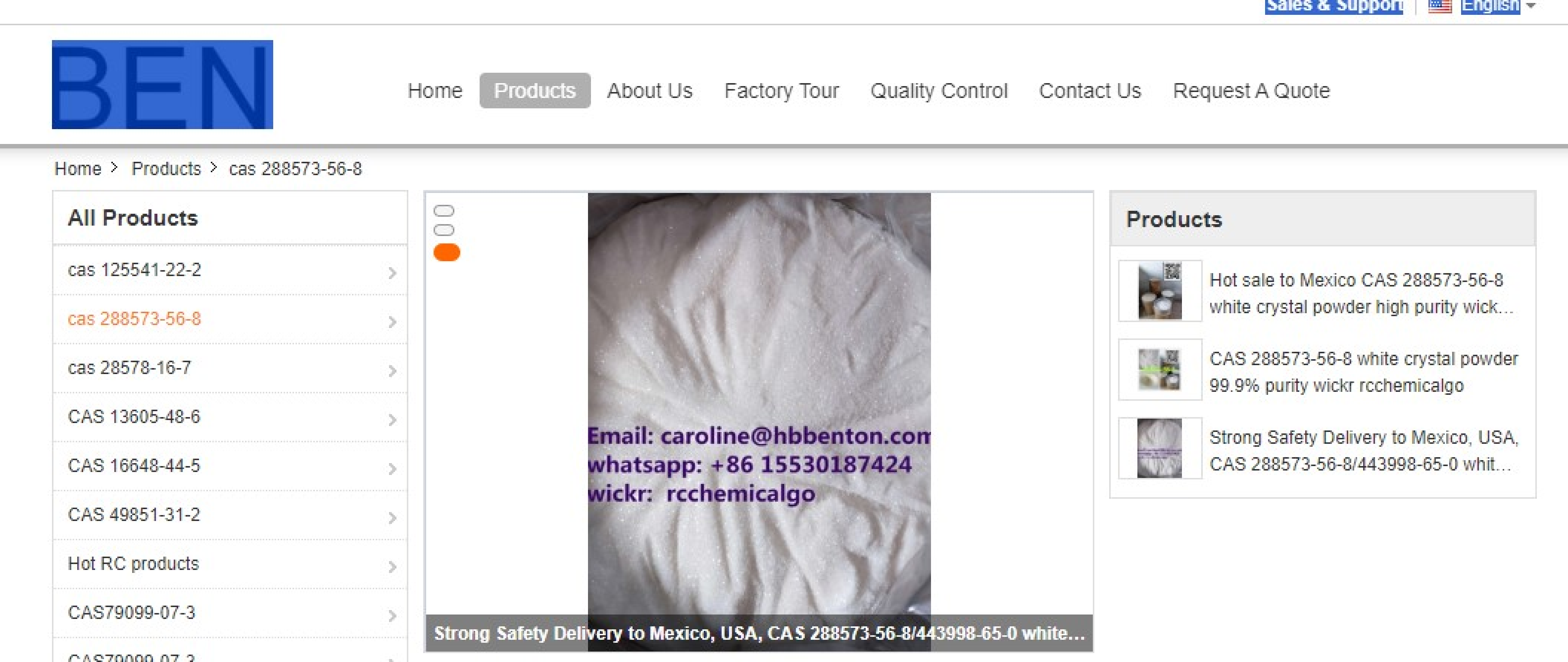
See more

DESCRIPTION OF THE PRODUCT

nannie@hiersunchem.com
whatsapp +8617192116194
wickr rcchemicalgo

http://www.protonitazene.com/

EXHIBIT 126



Sales & Support | English

BEN

Home | Products | About Us | Factory Tour | Quality Control | Contact Us | Request A Quote

Home > Products > cas 288573-56-8

All Products

- cas 125541-22-2
- cas 288573-56-8
- cas 28578-16-7
- CAS 13605-48-6
- CAS 16648-44-5
- CAS 49851-31-2
- Hot RC products
- CAS79099-07-3
- CAS79099-07-3

Email: caroline@hbbenton.com
whatsapp: +86 15530187424
wickr: rcchemicalgo

Strong Safety Delivery to Mexico, USA, CAS 288573-56-8/443998-65-0 white...

Products

- Hot sale to Mexico CAS 288573-56-8 white crystal powder high purity wick...
- CAS 288573-56-8 white crystal powder 99.9% purity wickr rcchemicalgo
- Strong Safety Delivery to Mexico, USA, CAS 288573-56-8/443998-65-0 whit...

EXHIBIT 127

cninf 巨潮资讯 看公告快人一步

front page announcement Information data Serve

Stock F10	Public Information	Margin Trading	Code/Abbreviation/Pinyin/Keyword/	Log in registe
		Shenzhen Stock Exchange		
Company Profile	Convertible bonds	Calendar	Termination/Delisting	A
				S
New share issuance	IPO prospectus	Equity Pledge	Shareholder data	d
Executive Ownership	Performance Forecast	Fund Holdings		

Website	corp.netsun.com	Fax	(+86)0571-87671502
Domicile	3506, Wangsheng Building, No. 788, Liye Road, Changhe Subdistrict, Binjiang District, Hangzhou, Zhejiang	Office	29F, Wangsheng Building, No. 788, Liye Road, Changhe Subdistrict, Binjiang District, Hangzhou, Zhejiang

CSRC Subsector:	Internet and Other-related S
Market:	Main Board of Shenzhen St

Business Summary (Updated: 08/23/2023)

NetSun was established in 1997 and has created e-commerce websites in industries such as ChemNet (https://china.chemnet.com/), TexNet (https://www.texnet.com.cn/), and PharmNet (https ://www.pharmnet.com.cn/). NetSun successfully went public in 2006 and has been focusing on the field of e-commerce. It now has completed its strategic layout in the fields of industrial internet, supply chain finance, and live e-commerce.

NetSun's platforms include ChemNet, 100ppi.com, Toocle.com, Rawmex.cn, and provides industrial internet solutions and supply chain finance solutions. NetSun relies on the above 1+3 major platforms and 2 major solutions to provide various enterprises with:

1. Network promotion services;
2. Commodity price data service;
3. Raw material trading services;
4. Live streaming supply chain services;
5. Supply chain financial services;
6. Industrial Internet solutions;
7. Supply chain finance solutions.

Price Performance

Directors & Executives

Chairman of the Board:	Sun Deliang
General Manager:	Sun Deliang
Chief Financial Officer:	Fang Fang
Board Secretary:	Fan Yuelon
Board Members:	Sun Deliang u Gang, Fu Z ,

Top 5 Shareholders (Ende

Name
Zhejiang Wangsheng Investment Management Co., Lt
Hangzhou Sheqi Network Co., Ltd.
Peng Bing
Hong Kong Securities Clearing Company Limited
Industrial Bank Co., Ltd. - China Southern Financial Thematic Flexible Allocation Mixed Fund

Operating Revenue (Unit: Million ¥)

	1Q	Semi-annual
2024	82	-
2023	167	222
2022	127	245
2021	137	285

supply chain.

4. Live E-commerce: Build a live e-commerce full industry chain service platform that integrates O2O product selection center, live streaming base, live streaming training, and supply chain finance.

5. Industrial Internet: The industrial Internet platform solution provided by NetSun is a solution to provide enterprises with comprehensive Digital transformation. By building an industrial internet platform, enterprises can achieve digital management of various links such as production, supply chain and sales. Solutions can improve operational efficiency, reduce costs, and create more business opportunities for enterprises.

6. Supply Chain Finance: Through supply chain finance services, enterprises obtain financial support and solve the problem of fund turnover in the supply chain. This plan can help enterprises improve capital utilization efficiency, reduce financing costs, and also optimize the operation of the entire supply chain.

environment. If the credit risk of small and medium-size increases, it will have a negative impact on financial ser commerce services. NetSun plans to strengthen cooper and regional industrial clusters, focusing on high-quality

2. Business model risks

Although NetSun has conducted sufficient market resea and trading services, it still needs to undergo certain ma facing the possibility of not being able to generate large term.

3. Market competition risk

The competition between peers has shifted from marke innovation, and NetSun will increase its stabilizing its basic business.

Dividend Data

Cash Div./Share(¥)	Bonus Issue/Share	Stock Div./Share	Date Decl.	Ex-Div.Date	Record Date	Cash Pa
0.050	-	-	06/14/2023	06/21/2023	06/20/2023	1
0.050	-	-	07/16/2021	07/23/2021	07/22/2021	07/23
0.050	-	-	07/16/2020	07/23/2020	07/22/2020	07/23
0.050	-	-	07/03/2019	07/10/2019	07/09/2019	07/10
0.050	-	-	06/30/2018	07/06/2018	07/05/2018	07/06
0.050	-	-	06/08/2017	06/14/2017	06/13/2017	06/14
0.050	0.100	0.100	06/12/2015	06/19/2015	06/18/2015	06/19
0.200	0.300	-	04/29/2014	05/07/2014	05/06/2014	05/07
0.100	-	-	05/16/2013	05/23/2013	05/22/2013	05/23
0.100	-	-	06/01/2012	06/08/2012	06/07/2012	06/08

Per Share Data (FYE: 12/31)

	2023	2022	2021	2020	2019	2018	2017	2016
Earnings(¥)	0.0800	0.0900	0.0900	0.1500	0.1400	0.1400	0.0800	0.0500

Pretax Income	31	37	28	51	50	49	27	12
Income Tax	10	6	6	10	9	11	7	0
Net Income	twenty one	31	twenty three	41	41	38	twenty one	12

Balance Sheet (Unit: Million ¥; FYE: 12/31)

	2023	2022	2021	2020	2019	2018	2017
Assets							
Monetary Capital	687	683	749	866	947	836	820
Current Assets-Total	1,440	1,444	1,447	1,469	1,433	1,353	
Non-current Assets-Total	207	191	170	166	162	144	
Total Assets	1,647	1,634	1,617	1,635	1,595	1,497	
Liabilities							
Current Liabilities-Total	416	411	431	454	439	404	227
Long-term Debt	-	-	-	-	-	-	-
Non-current Liabilities-Total	27	29	twenty three	14	17	2	3
Total Liabilities	444	440	454	468	455	406	229
Stockholder's Equity							
Share Capital	253	253	253	253	253	253	253
Retained Profits	301	296	274	266	244	225	207
Total Owners' Equity	1,203	1,194	1,163	1,168	1,140	1,091	1,066

Cash Flow Statment (Unit: Million ¥; FYE: 12/31)

	2023	2022	2021	2020	2019	2018	2017
Net Cash Flows-Operating	-94	-125	-59	-129	95	-37	-31
Net Cash Flows-Investing	1	8	-5	-39	-34	-2	3
Net Cash Flows-Financing	99	30	-41	66	-7	-9	-32

巨潮资讯 看公告快人一步

front page announcement Information data Serve

Stock F10 | Public Information | Margin Trading | Block Trades | Log in registe

Shenzhen Stock Exchange

Company Profile | Convertible bonds | Calendar | Termination/Delisting | A

S

New share issuance | IPO prospectus | Equity Pledge | Shareholder data | d

Executive Ownership | Performance Forecast | Fund Holdings

Address: Building 10, Shangbu Industrial Park, Hongli West Road, Futian District, Shenzhen, PRC

For more information, please refer to http://webapi.cninfo.com.cn

about Us

Juchao Information Network is the statutory information disclosure platform of the Shenzhen Stock Exchange and is operated by Shenzhen Securities Information Co., Ltd., a wholly-owned subsidiary of the Shenzhen Stock Exchange. The platform has always been committed to protecting investors' right to know and right to participate, and providing investors with one-stop securities market information services.

Friendly Links

Shenzhen Stock Exchange

Shanghai Stock Exchange

Shenzhen Securities Information Co., Ltd.

National Securities Index

Science and Technology

V-Next

Shenzhen Securities Information Technology Data Service Platform

It is recommended to use IE11 and above browsers, with a resolution of 1280*800 or above. This website supports ipv6 access

EXHIBIT 128

Business treasure(002095.SZ)

+ Favo

Company Introduction
Securities Introduction
Share capital structure
List of top ten shareholders
Restricted shares released
Equity holding subsidiaries
Board Member
Member of the Supervisory Board
Senior Management
Management shareholding and compensation
Changes in management shareholding
Enterprise Advanced Search (New)

Balance Sheet
Income Statement
Cash Flow Statement
Financial Summary (Reporting Period)
Financial Summary (Single Quarter)
Income Statement (Single Quarter)
Main Business Structure
By Product
By Industry
By Region
Original financial report (PDF)

Per share indicator
Financial Analysis
DuPont Analysis

Dividend Record
Mergers and acquisitions
Investment of raised funds

Dou Mingqing's personal profile

Name	Dou Mingqing (male) He has held 1 position , click to view>>
Position	Independent Director (Board of Directors)
Date of appointment	2019-06-20
End date of employment	-
Country of Citizenship	China
Education	master
Date of Birth	1975
state	-
Company	Zhejiang Wangsheng Business Information Co., Ltd.
Company Stock	Bizbao (002095.SZ)
Update time	2024/9/3 22:39:46
Personal Profile	Mr. Dou Mingqing: Born in July 1975, member of the Communist Party of China, Chinese nationality, bache Central South University... more>>
Other Board Members	Sun Deliang (Chairman) Sun Deliang (Director) Fu Zhiyong (Director) Tong Maorong (Director) Yu (Director) Lv Gang (Director) Shou Zou (Director) Xu Jiabing (Independent Director) Chen Deren (Inde Director) Li Ying (Independent Director)

Prospective Industry Research Institute

Industry segment reports

Feasibility report

Industrial Planning

Industrial Park Planning

Industrial investment

IP fundra feasib stu

EXHIBIT 129

Business treasure(002095.SZ)

+ Favo

Company Introduction
Securities Introduction
Share capital structure
List of top ten shareholders
Restricted shares released
Equity holding subsidiaries
Board Member
Member of the Supervisory Board
Senior Management
Management shareholding and compensation
Changes in management shareholding
Enterprise Advanced Search (New)

Balance Sheet
Income Statement
Cash Flow Statement
Financial Summary (Reporting Period)
Financial Summary (Single Quarter)
Income Statement (Single Quarter)
Main Business Structure
By Product
By Industry
By Region
Original financial report (PDF)

Per share indicator
Financial Analysis
DuPont Analysis

Dividend Record
Mergers and acquisitions
Investment of raised funds

薪酬 人事档案 查询个人信息 人事档案管理 高级管理人员 个人简历表 人事档案查询系统 财务
近三年财务报表 检测手机号码 查手机号码 身份信息 年度报表 下载pdf 电话号码查公司 可视化数据图

Yu Yi's Personal Profile

Name	Yu Yi (male) He has held 3 positions in 10 listed companies . He has held positions . Click to view >>
Position	Independent Director (Board of Directors)
Date of appointment	2019-06-20
End date of employment	-
Country of Citizenship	China
Education	master
Date of Birth	1965
state	-
Company	Zhejiang Wangsheng Business Information Co., Ltd.
Company Stock	Bizbao (002095.SZ)
Update time	2024/9/3 22:39:46
Personal Profile	Mr. Yu Yi: Born in August 1965, member of the Communist Party of China, Chinese nationality, no permane residence, Shanghai...... more>>
Other Board Members	Sun Deliang (Chairman) Sun Deliang (Director) Fu Zhiyong (Director) Tong Maorong (Director) Yu (Director) Lv Gang (Director) Shou Zou (Director) Xu Jiabing (Independent Director) Chen Deren (Inde Director) Li Ying (Independent Director)

实业公司

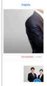
总经理

调研公司

财务分析报告

高级管理人员

工厂车间现场管理



Prospective Industry Research Institute

Industry segment reports

Feasibility report

Industrial Planning

Industrial Park Planning

Industrial investment

IPO fundra feasib stu

调研公司

公司网页

总经理

实业公司

财务分析报表

年会策划公司

高级管理人员

个人简介

上海共享办公室

海归硕士招聘会

EXHIBIT 130

U.S.-China Economic and Security Review Commission

Issue Brief

August 24, 2021

Illicit Fentanyl from China: An Evolving Global Operation

Lauren Greenwood, Congressional Fellow

Kevin Fashola, Former Congressional Fellow

Key Findings

- **China remains the primary country of origin for illicit fentanyl and fentanyl-related substances trafficked into the United States:** In 2019, China fulfilled a pledge to the United States and placed all forms of fentanyl and its analogues on a regulatory schedule. Nevertheless, illicit fentanyl from China remains widely available in the United States. Chinese traffickers are using various strategies to circumvent new regulations, including focusing on chemical precursors, relocating some manufacturing to India, rerouting precursor shipments through third countries, and leveraging marketing schemes to avoid detection. China's weak supervision and regulation of its chemical and pharmaceutical industry also enable evasion and circumvention.

- **Since China's government scheduled fentanyl, the amount of finished fentanyl shipped directly from China to the United States has declined, while the amount shipped from Mexico has increased:** The U.S. Drug Enforcement Administration (DEA) assesses Chinese traffickers have shifted from primarily manufacturing finished fentanyl to primarily exporting precursors to Mexican cartels, who manufacture illicit fentanyl and deliver the final product. U.S. law enforcement has seen a growing trend of Chinese nationals, in both Mexico and the United States, working with Mexican cartels. As Chinese suppliers coordinate more with international partners, the DEA is concerned that fentanyl production is becoming increasingly global and more difficult to track and control.

- **Chinese brokers are laundering Mexican drug money through China's financial system:** Chinese money launderers are using financial technology, mobile banking apps, and social media to evade authorities.

- **Cooperation between the United States and China remains limited:** U.S. law enforcement agencies have established working groups, conducted high-level meetings, and shared information with their Chinese counterparts, which has led to the dismantling of a few illicit fentanyl networks. At the same time, U.S. authorities are reporting that cooperation remains limited on the ground. The Chinese government has cooperated less with U.S. authorities on criminal and money laundering investigations, conducting joint operations, and U.S. requests for inspections and law enforcement assistance.

Overview of Chinese Fentanyl Flows to the United States

According to the U.S. Centers for Disease Control and Prevention (CDC), synthetic opioids—primarily illicit fentanyl—remain the largest cause of overdose deaths in the United States.[1] The CDC estimates that in the United States, there were more than 93,000 drug overdose deaths in 2020, of which an estimated 69,710 were opioid overdoses. This is a more than 30 percent increase from the 50,963 opioid overdoses in 2019.[*2] Stay-home orders, disruption of normal routines, economic hardships, and other stressors related to the novel coronavirus (COVID-19) pandemic contributed to the rise in abuse of illicit opioids in the United States in 2020,[3] despite the increased price of street fentanyl.

In its *2020 National Drug Threat Assessment* report, the DEA assessed that China was "the primary source of fentanyl and fentanyl-related substances trafficked through international mail and express consignment operations, as well as the main source for all fentanyl-related substances trafficked into the United States."[4] Fentanyl is trafficked into the United States by two primary methods: (1) sent from Chinese suppliers via international mail or express consignment services, such as UPS, FedEx, or DHL; and (2) smuggled across the U.S.-Mexican border.

- *International mail:* According to U.S. seizure data, finished fentanyl and related analogues were often mailed from China in parcel packages. Fentanyl shipped this way tends to be above 90 percent purity and is shipped in packages weighing less than 1 kilogram, or 2.2 pounds. [†5] According to U.S. Customs and Border Protection (CBP), only 11.58 pounds of fentanyl was seized in direct shipment from China in the first eight months of 2019 compared to 278 pounds in 2018.[6]
- *U.S.-Mexico border:* According to Thomas Overacker, executive director of the CBP Office of Field Operations, "Most of the illicit fentanyl entering our country by weight does so at ports of entry (POEs) along our southwest border by private vehicles, pedestrian, and commercial vehicles."[7] In 2019, CBP seized more than 2,660 pounds of illicit fentanyl from Mexico compared to 1,500 pounds in 2018.[8] The Mexican government reported that seizures of illicit fentanyl at clandestine labs and ports increased six-fold in 2020, suggesting Mexico is accounting for a greater share of the fentanyl trafficked directly into the United States even though the precursor chemicals originate in China.[9] Reflecting on the impact of the Chinese government's decision to schedule fentanyl, in 2021 the DEA noted that Mexican cartels, "will remain the primary source of supply for heroin and [finished] fentanyl smuggled into the United States, using precursors primarily sourced from China."[10]

Major Developments since 2018

In November 2018, the Commission published a staff report, *Fentanyl Flows from China: An Update since 2017*.[‡] Since the report's publication, there have been several significant developments:

- *China scheduled fentanyl:* At the December 2018 G20 Summit in Argentina, General Secretary of the Chinese Communist Party Xi Jinping made a commitment to then President Donald Trump that China would schedule or control fentanyl.[11] As a result of U.S.-China counternarcotic negotiations, in April 2019 China's Ministry of Public Security, National Health Commission, and State Drug Administration jointly announced that all fentanyl and analogues would be placed on the *Supplementary List of Non-medicinal Narcotic Drugs and Psychotropics Drugs*, effectively controlling all types of fentanyl unless given a special permit.[12] The DEA confirmed the controls went into effect in May 2019.[13] According to David Prince, deputy assistant director of transnational organized crime at U.S. Immigration and Customs Enforcement (ICE), China's scheduling has led to a decline in the number of Chinese manufacturers "willing to sell/export [finished] fentanyl products."[14]

[*] The CDC also continues to update its numbers as new data are made available. According to the CDC, overdose deaths were already increasing in 2019 but further accelerated during the COVID-19 pandemic as a result of the "disruption to daily life due to the COVID-19 pandemic [which] has hit those with substance use disorder hard." Although widely abused, fentanyl is also prescribed legally by medical professionals for pain relief. As a result of the COVID-19 pandemic, opioid and licit fentanyl used to treat patients increased as well. U.S. Centers for Disease Control, *Overdose Deaths Accelerated during COVID-19*, December 17, 2020. *https://www.cdc.gov/media/releases/2020/p1218-overdose-deaths-covid-19.html*.

[†] The DEA assesses that fentanyl of such purity is produced by chemical companies in China, in contrast to fentanyl from Mexico, which has a purity below 10 percent and is often mixed with other illicit drugs (e.g., heroin, cocaine, and methamphetamines). U.S. Drug Enforcement Administration, *2018 National Drug Threat Assessment*, March 2019. *https://www.dea.gov/sites/default/files/2018-11/DIR-032-18%202018%20NDTA%20final%20low%20resolution.pdf*; U.S. Drug Enforcement Administration, *2020 National Drug Threat Assessment*, March 2021. *https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf*.

[‡] See Sean O'Connor, "Fentanyl Flows from China: An Update since 2017," *U.S.-China Economic Security and Review Commission*, November 26, 2018. *https://www.uscc.gov/sites/default/files/Research/Fentanyl%20Flows%20from%20China.pdf*.

- *U.S. increased efforts to stem illicit flows:* U.S. enforcement agencies have stepped up enforcement against Chinese drug traffickers. For example, since 2017 the U.S. Department of the Treasury's Office of Foreign Asset Control (OFAC) has designated at least 14 Chinese nationals and six Chinese entities on the Foreign Narcotics Kingpin Designation list under the Kingpin Act, a significant increase from the 2000–2016 period, when only five Chinese nationals and two entities were designated.[15] Additionally, the U.S. Department of Justice (DOJ) has indicted at least 11 Chinese nationals on money laundering and drug trafficking charges and convicted at least three Chinese nationals of drug-related crimes.[16]
- *Illegal drug traffickers in China began to adjust their operations:* Although the Chinese government has scheduled some precursor chemicals, drug producers can still access critical precursor ingredients from China and manufacture new fentanyl analogues to avoid Chinese law enforcement.[17]

Key Terms

Synthetic opioids: Substances produced in a laboratory using the same chemical structure (synthetic) as natural opioids, which are a class of drugs extracted from the opium poppy plant.

Fentanyl (licit): A potent synthetic opioid approved by the FDA for pain relief, often for cancer patients, and as an anesthetic. It is approximately 100 times more potent than morphine and 50 times more potent than heroin. Fentanyl pharmaceutical products are available in lozenges, tablets, nasal sprays, skin patches, and injectable formulations.

Fentanyl (illicit): Fentanyl produced and sold illegally and typically found in powder or pill form, sometimes mimicking pharmaceutical drugs such as oxycodone.

Drug schedules: Drugs, substances, and certain chemicals used to make drugs are classified into five distinct categories or schedules depending upon the drug's acceptable medical use and the drug's abuse or dependency potential. Schedule I drugs represent the greatest potential for abuse. Fentanyl is a Schedule II narcotic under the U.S. Controlled Substances Act of 1970.

Controlled substance: A drug or other substance that is tightly controlled by the government because it may be easily abused or cause addiction. The government "control" manages how the substance must be made, handled, used, stored, and distributed.

Analogues: A drug that has been designed to mimic the pharmacological effects of the original drug and in some cases is produced to avoid government controls. Some Fentanyl analogues include acetylfentanyl, furanylfentanyl, carfentanil, which are all similar in chemical structure to fentanyl.

Precursor chemicals: Also known as "precursors," these are substances used in manufacturing of other products. Fentanyl precursors, like ANPP, NPP, or 4-AP, are used to produce fentanyl and more easily evade authorities. Many precursors can be used to make both licit and illicit drugs.

Source: Various.[18]

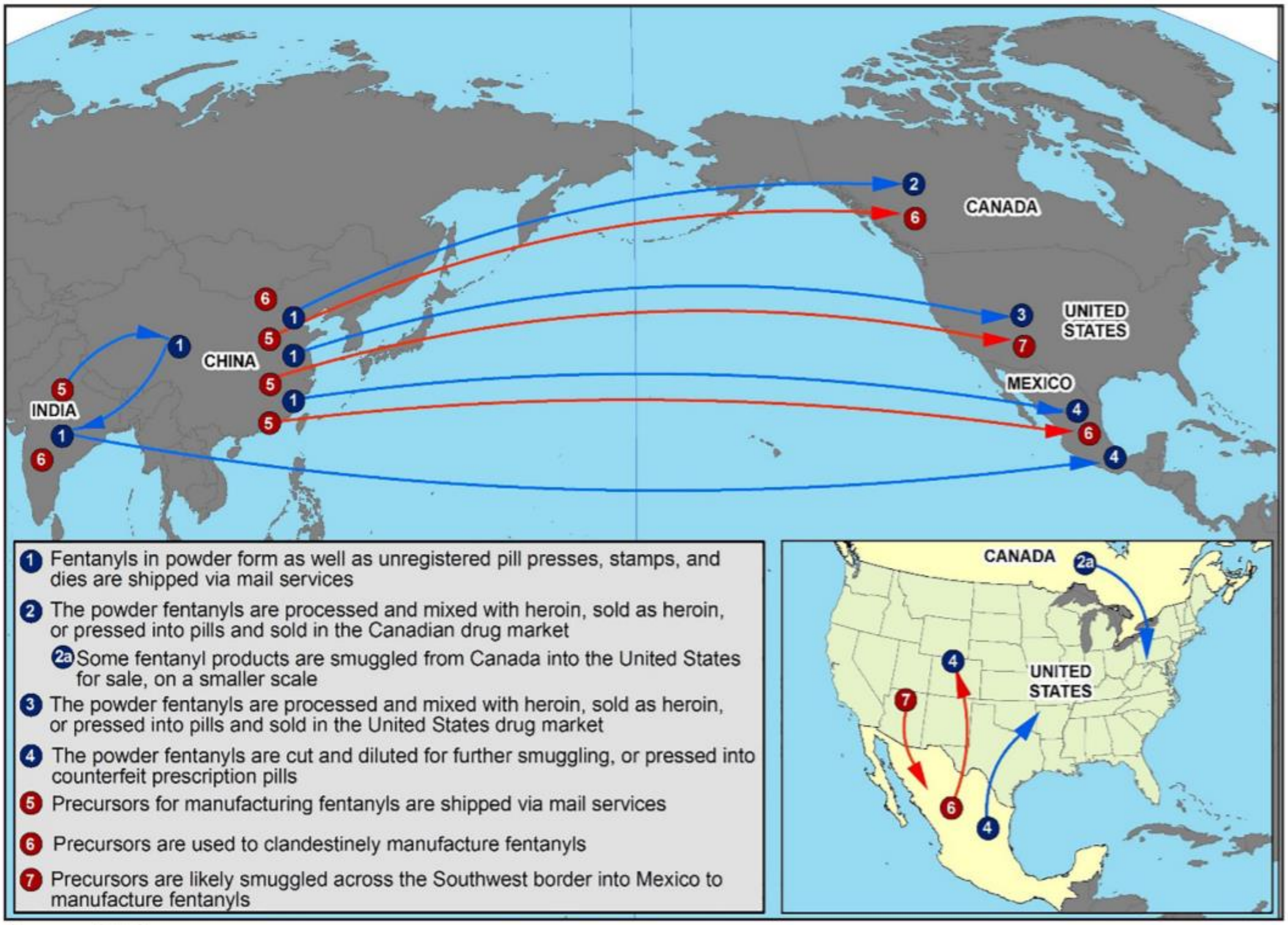
Chinese Illicit Fentanyl Producers Evade Authorities

China's May 2019 fentanyl scheduling announcement has changed the way illicit vendors operate as Chinese authorities have ramped up investigations of known manufacturing sites, cracked down on websites selling illicit fentanyl, begun to enforce shipping rules, and created special investigation teams.[*19] In response, Chinese illegal

[*] As noted in the Commission's 2017 fentanyl report, "the chemicals used to produce fentanyl and fentanyl-like products are illegally diverted from legitimate pharmaceutical uses, with criminals taking advantage of inadequate enforcement protocols to produce unregulated chemicals." This makes it particularly challenging to identify which manufacturing sites are solely used for legal production and which

fentanyl producers began seeking new ways to evade authorities, including developing new fentanyl precursors, working with traffickers in other countries, and using technology to avoid detection. According to a 2020 DEA report, *Fentanyl Flow to the United States*, fentanyl production is becoming a global operation (see Figure 1), which has exacerbated illicit trafficking to the United States by introducing additional countries into the supply chain.[20] While the 2019 scheduling announcement brought heightened scrutiny to illicit fentanyl production, China's regulation and enforcement of its vast chemical and pharmaceutical industries remain weak. In his testimony before the Commission in 2019, Ben Westhoff highlighted how "China's clumsy, understaffed bureaucracy has a difficult time controlling the country's chemical industry. Different layers of government are sometimes at odds with one another, local officials are corruptible, and industry regulations are confusing and poorly enforced."[21] Without effective regulation of China's chemical and pharmaceutical industries, illicit fentanyl manufacturers have an easier time operating.

Figure 1: Fentanyl Flows to the United States, 2019


CANADA
UNITED STATES
MEXICO
CHINA
INDIA
1 Fentanyls in powder form as well as unregistered pill presses, stamps, and dies are shipped via mail services
2 The powder fentanyls are processed and mixed with heroin, sold as heroin, or pressed into pills and sold in the Canadian drug market
2a Some fentanyl products are smuggled from Canada into the United States for sale, on a smaller scale
3 The powder fentanyls are processed and mixed with heroin, sold as heroin, or pressed into pills and sold in the United States drug market
4 The powder fentanyls are cut and diluted for further smuggling, or pressed into counterfeit prescription pills
5 Precursors for manufacturing fentanyls are shipped via mail services
6 Precursors are used to clandestinely manufacture fentanyls
7 Precursors are likely smuggled across the Southwest border into Mexico to manufacture fentanyls

Source: U.S. Drug Enforcement Administration, *Fentanyl Flow to the United States*, January 2020.

New Fentanyl Precursors: In January 2018, China added two fentanyl precursors, NPP and 4-ANPP, to the controlled substance list. U.S. and Mexican authorities reported a decline in seizures immediately following China's 2019 scheduling of fentanyl, but traffickers quickly adjusted, by developing alternative precursors that are not scheduled. As reported by the U.S. Department of State, Chinese traffickers have shifted to alternative precursors chemicals like 4-AP (see Appendix, Table 1).[22] According to the Center for Advanced Defense Studies (C4ADS), since the 2019 scheduling of all fentanyl, Chinese producers have developed at least four more precursor substitutes,

sites are dual-use. U.S.-China Economic and Security Review Commission, *Fentanyl: China's Deadly Export to the United States,* February 1, 2017*, https://www.uscc.gov/research/fentanyl-chinas-deadly-export-united-states.*

which contribute to evading detection.[23] Marketing on the internet for these four substitutes has become increasingly common.[24] The Chinese government has yet to ban these four precursors.[25]

The State Department dubbed China's precursor substitutes "indirect precursors" or "pre-precursors."[*26] Bryce Pardo, an associate policy researcher at RAND Corporation, said this shift may set a worrisome precedent as traffickers are exporting the pre-precursors to Mexico, where they are subsequently made into finished fentanyl.[27] The DEA's *2020 Drug Threat Assessment Report* also expresses concern that Chinese chemists are increasingly focused on precursors to precursors, many of which have legitimate uses and are therefore hard to regulate.[28]

Potential Production Shifts to India and Other Third Countries: In 2020, the DEA noted that India has begun to emerge as a more prominent source country for Mexican drug trafficking organizations and that this trend could accelerate "if China-based traffickers work with Indian nationals to circumvent China's new controls on fentanyl."[29] U.S. law enforcement is also concerned that Southeast Asia's "Golden Triangle" could become the next fentanyl hotspot after India.[†30] The region is also known to have limited drug enforcement and regulation and is already a major source for methamphetamines and other drugs.[31]

Technological and Digital Evasion Methods: Traffickers continue to use the internet and technology to conceal their illicit activities, and their methods have become increasingly more sophisticated. To avoid scrutiny and detection, some Chinese sellers have used the numerical code, scientific names, and technical nomenclature of fentanyl and related precursors in their advertisements on websites, social media, and e-commerce platforms.[32] The complexity and abstract nature of chemical nomenclature and classification systems, rather than the more recognizable terminology, makes it harder for law enforcement to track illicit fentanyl advertising online.[33] This method also allows the sellers to create many different naming combinations for marketing, further outpacing U.S. and Chinese authorities. C4ADS reported that various drug groups operating online are using password-encrypted websites and private groups on social media and messaging apps to operate platforms or virtual marketplaces that connect illicit fentanyl consumers and sellers while avoiding detection by U.S. and Chinese law enforcement.[34] To reduce potential public exposure, many of these websites and groups have deployed web moderators who serve as gatekeepers to ensure only trusted individuals have access.[35]

Chinese Traffickers Increase Cooperation with Mexican Cartels

Mexican cartels have historically been involved in the production of poppies in Mexico that are used to make heroin.[36] With Mexican anti-drug authorities ramping up the destruction of poppy fields across the country, however, the cartels have shifted from heroin to synthetic opioids like fentanyl, which are cheaper to make and more profitable.[37] As Chinese traffickers sought to evade the Chinese government's increased regulation in 2019, Mexican cartels looked to maximize their role in the illicit fentanyl trade.

The China-Mexico connection grew when Chinese traffickers increased fentanyl precursor sales to Mexican cartels.[38] Speaking in March 2021, Matthew Donahue, the deputy chief of foreign operations for the DEA, described "an unlimited and endless supply of precursors chemicals … coming from China to Mexico," noting that Chinese traffickers have virtually ceased making analogues to focus solely on precursors.[39] Mexican officials have worked with the DEA to dismantle established networks of manufacturing plants, or "pill mills," in Mexico City, Mexicali, and other places controlled by the Sinaloa cartel and the Jalisco Nueva Generacion (Jalisco New Generation) cartel.[‡]

[*] According to the DEA's *2020 National Drug Threat Assessment Report*, "Although 4-AP is not a direct replacement for 4-anilino-N-phenethylpiperidine (4-ANPP) in the synthesis of fentanyl, 4-AP can be converted into 4-ANPP in a one-step chemical reaction." Only direct replacements are considered precursors, but experts colloquially refer to 4-AP as a precursor due to its ability to synthesize 4-ANPP. U.S. Drug Enforcement Administration, *2020 National Drug Threat Assessment Report*, March 2021, *https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf*.

[†] The name "Golden Triangle" refers to the region where the borders of Burma, Laos, and Thailand meet. Historically, it is known for its opium cultivation. *https://www.reuters.com/article/us-asia-drugs/asian-drug-lords-likely-producing-precursor-chemicals-in-golden-triangle-idUSKBN2AC0KF*.

[‡] The DEA noted in an interview with the Commission that in addition to supplying vast amounts of precursor chemicals, Chinese traffickers are also shipping large-scale "industrial sized pill presses" to Mexico. Mexican cartels then press loose fentanyl power into pills. U.S. Drug Enforcement Administration, interview with Commission staff, March 15, 2021.

[40] These pill mills in Mexico made finished fentanyl from Chinese-sourced precursors to traffic across the U.S.-Mexico border into the United States.[41]

The Sinaloa and Jalisco cartels are the main entities responsible for manufacturing precursor chemicals into finished fentanyl and smuggling it into the United States.[42] The Sinaloa cartel has developed relationships with suppliers in China and India to purchase precursor chemicals or, in some cases, finished fentanyl powder.[43] Fentanyl and precursors are shipped from China to many ports of entry across Mexico's Pacific coastline, such as Lazaro Cardenas in Michoacán, Manzanillo in Colima, and Ensenada in Baja California.[44] Chinese nationals implicated in trafficking have also been known to travel to Mexico.[45]

A November 2020 investigation by Fox News highlighted an emerging trend of Chinese nationals involved in illicit fentanyl operations in Mexico.[46] The investigation focused on the Zheng DTO (Drug Trafficking Organization), colloquially known as "Los Zheng Cartel," which operates through multiple shell companies that seemingly offer legitimate services such as chemical labs, veterinary care, computers, and retail. Intelligence professionals in Mexico have described the Zheng cartel as having "the largest presence in Mexico for trafficking fentanyl and methamphetamines."[47] The Zheng cartel has developed extensive relationships with suppliers in China, can easily import goods from China into Mexico, and has cultivated relationships on both sides of the U.S.-Mexico border.[48] According to media reporting, the Zheng cartel is suspected of having ties to both the Sinaloa and Jalisco cartels.[49] Effectively, the Zheng cartel serves as an intermediary between suppliers in China and cartels in Mexico.

In 2018, the U.S. Attorney's Office in Cleveland indicted two Zheng cartel leaders on 43 counts of manufacturing and shipping fentanyl analogues and 250 other drugs to 37 states and 25 countries.[50] According to the indictment, since 2008 the Zheng cartel has "engaged in this conspiracy from its base of operations in Shanghai."[51] In August 2019, the Treasury Department designated Fujing Zheng, a Chinese national who leads the Zheng cartel, his father Guanghua Zheng, and the Zheng cartel under the Kingpin Act.[52] Additionally, in July 2020 the Treasury Department added four Chinese nationals to the Kingpin list for their links to the Zheng cartel and fentanyl trafficking; it also designated one company, Global United Biotechnology Inc., saying it was "a virtual storefront of Zheng DTO" through its use of digital currency to launder illegal drug money.[53] Despite the designations and indictments, as of January 2021 the Zhengs and their associates remain at large and continue operating in both China and Mexico.[54] Chinese fentanyl traffickers have survived challenges like China's 2019 scheduling of fentanyl and COVID-19 because of their vast networks inside of Mexico and the United States. Cartels like Los Zheng rely on coconspirators in the United States, Mexico, and elsewhere to retrieve, package, and distribute their shipments.

Separate from the Zheng cartel, individuals and groups of Chinese "chemical brokers" are also operating in Mexico.[55] According to the DEA, these chemical brokers are active in the state of Sinaloa, especially the capital of Culiacan, where an estimated 2,000 Chinese nationals are working to facilitate and coordinate the importation of precursors chemicals.[56]

Chinese Money Laundering in Mexico: A Transnational Web

In February 2020, the U.S. Department of the Treasury described Chinese money launderers as "key threats" and vulnerabilities in the U.S. financial system.[57] A December 2020 Reuters investigation found Chinese money launderers "have come to dominate the international money laundering market."[58] The DEA reports having also seen Chinese money launderers working with drug trafficking organizations in the Dominican Republic and Colombia.[59]

In a high-profile case that shed light on the intersection of financial technology and drug trafficking, Xianbing Gan, a Chinese national based in Chicago, was arrested by U.S. authorities in November 2018 on suspicion of money laundering for a cartel. In March 2020, Gan was convicted on money laundering charges.[60] In addition to the Gan case, in October 2019 U.S. attorneys in Oregon charged Shefeng Su, Xinhua Li Yan, and Xiancong Su with money laundering.[61] In September 2020, Xueyong Wu was convicted in the U.S. District Court Eastern District of Virginia in Richmond and sentenced to five years in prison for laundering money for a Mexican drug cartel.[62] It is difficult to know exactly how much money Chinese nationals have laundered for cartels, but in the Gan case alone, the Department of Homeland Security (DHS) estimated his operation laundered between $25 million and $65 million.[63]

Chinese criminals use complex techniques to launder money for Mexican drug cartels. One common technique is to use "mirror transactions" that involve cross-border currency swaps. In these transactions, an intermediary usually receives one currency (e.g., accepts U.S. dollars earned by drug dealers) and deposits an equivalent amount of another currency in a foreign bank (e.g., deposits renminbi [RMB] in a Chinese bank) (see Appendix, Table 2 for an example of how mirror transactions work).[64] These types of laundering schemes offer a mechanism for cartels to access profits while limiting exposure and risk. Chinese money launderers leverage encrypted mobile communications apps like WeChat to move vast sums of money from the United States to China then back to Mexico with great speed, discretion, and efficiency.[65]

Since they are difficult to track, convertible virtual currencies or cryptocurrencies such as Bitcoin, Ethereum, or Monero have become a popular medium.[66] DEA spokesperson Michael Miller told Reuters that Mexican cartels "are increasing their use of virtual currency because of the anonymity and speed of transactions" and that their use "will only increase in the future."[67] The Reuters investigation revealed that once Chinese money launderers move illicit drug proceeds into China's financial system, some of that money is used to purchase consumer goods or more precursor chemicals, recycling the money back into the economy.[68] The money, consumer goods, or precursors are transferred back out of China to the drug cartel in Mexico.[69]

U.S.-China Cooperation and Enforcement Efforts

Although U.S.-China enforcement cooperation on combating illicit fentanyl has improved, serious gaps remain. While China has increased cooperation by scheduling all forms of fentanyl, participating in counternarcotic working groups, and complying with U.S. shipping requirements, cooperation lags in money laundering investigations, criminal prosecution, and legal assistance in ongoing cases. Chinese regulatory authorities continue to delay requests for access to inspect and investigate potential sites of illegal chemical production where precursors are made. Requests are often delayed for days, allowing any illegal operation to vacate or clean up the premises.

The United States and China first cooperated in a high-profile case that began in 2017, resulting in nine people convicted on drug-related charges in Hebei Province.[70] U.S. authorities carried out three major arrests in New York and Oregon.[71] The DEA gave its Chinese counterparts intelligence that led to the discovery of a sprawling illicit fentanyl network in China.[72] Yu Haibin, vice director of the Office of China National Narcotics Control Commission, said in an interview that China has taken steps to crack down on "distributing, producing and smuggling," expressing hope that this could play a positive role with the United States.[73]

China has also complied with U.S. requests to better regulate its shipping and postal networks. In 2018, Congress passed the Synthetics Trafficking and Overdose Prevention (STOP) Act, which required the U.S. Postal Service (USPS) to receive Advanced Electronic Data (AED) on 100 percent of inbound package shipments from China by December 31, 2018, and 100 percent from all other international shipments by December 31, 2020.[74] AEDs provide basic information about the shipper, the recipient, and package content—information used by postal authorities to monitor potentially harmful or illicit content.[75] According to Gary Barksdale, the chief postal inspector of USPS, China's compliance with the STOP Act and USPS's AED requirements has improved from 32 percent in October 2017 to 85 percent in May 2019—short of the 100 percent threshold but well above the average international AED compliance score, which was 54 percent as of October 2020.[76] Though China's AED compliance is high, the country is also the largest source of packages coming to the United States.[77] The United States must continue to maintain a strong screening process for all mail coming from China.

Since China moved to control all fentanyl in 2019, statements made during congressional testimony from representatives of various U.S. law enforcement agencies have highlighted China's continued cooperation:

- *Department of Justice:* In testimony during a January 2021 hearing before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security, Amanda Liskamm, director of Opioid Enforcement and Prevention Efforts at DOJ, said that through "bilateral communications and bridge-building efforts," DOJ has engaged Chinese counterparts "on the control of fentanyl and other psychotic substances."[78] According to Ms. Liskamm, "When China controls a drug or precursor chemical, we see a significant drop in the use of the substance for illicit purposes in the United States."[79]

- *Customs and Border Protection:* During testimony to the Homeland Security Subcommittee on Investigations on "Combating the Opioid Crisis" in December 2020, CBP Director Overacker said "CBP now regularly shares targeting information with the China Ministry of Public Security (MPS) and the General Administration of China Customs."[80] He also said CBP has initiated a series of "regular meetings between the CBP attaché in Beijing and the China Ministry of Public Security."[81]

- *Drug Enforcement Administration:* During a July 2019 hearing on "Oversight of Federal Efforts to Combat Illicit Fentanyl" before the House Energy and Commerce Committee, Matthew Donahue, then the regional director of the North and Central Americas Operation Division at the DEA, said, "The DEA is committed to working with China in well-established bilateral efforts: liaison presence, the Counter Narcotics Working Group, regular meetings with scientists; and enhancing collaboration with DEA interagency partners."[82] In Congressional testimony, Mr. Donahue said he was encouraged by China's 2019 fentanyl scheduling and its potential to "prevent chemical workarounds to be exploited by clandestine synthetic opioid producers in China by allowing the United States and China to cooperate on a broader range of cases."[83] The DEA currently has an office in Beijing, and in 2020 China's government approved the DEA's request to establish satellite offices in Shanghai and Guangzhou.[*][84]

- *Immigration and Customs Enforcement:* At the same July 2019 hearing, ICE Deputy Assistant Director Prince noted collaborative efforts by ICE and DHS with China regarding information sharing on "certified lab reports" and "shipping labels" and how these efforts led China to control all fentanyl variants and analogues in May 2019.[85]

Despite these positive trends, there remain significant gaps in U.S.-China antidrug cooperation, especially in enforcement and criminal prosecution. For example, the DEA reported it informally asked its Chinese counterparts for assistance with the Gan investigation but did not receive Chinese support despite multiple requests.[86] When asked by Reuters about the lack of cooperation in the Gan case, China's Foreign Ministry first deflected the question and accused the United States of not requesting support, and later claimed the bank account holders U.S. investigators inquired about were "legitimate enterprises and business holders" in China.[87] Retired DEA agent Jeffrey Higgins noted in 2018 that he felt "China is merely seeking to create the appearance of cooperating with U.S. officials, while not enacting any reforms."[88] Other retired U.S. law enforcement personnel echoed this sentiment. In an interview with online investigative reporting project SpyTalk, former DEA agents anonymously expressed frustration about the lack cooperation from China despite the DEA publicly touting Chinese cooperation efforts.[89]

The State Department reported in the *2020 International Narcotic Control Strategy Report (INCSR) on Money Laundering* that "China has not cooperated sufficiently on financial investigations and does not provide adequate responses to requests for financial investigation information."[90] ICE Deputy Assistant Director Prince also described China as "recalcitrant" in ICE's conspiracy and cryptocurrency investigations, echoing the findings in the State Department's report.[91] In a rare admission, in September 2019 the People's Republic of China's Office of China National Narcotic Control Commission said U.S.-China cooperation on investigating and prosecuting fentanyl remains "extremely limited."[92]

The United States, along with 40 other countries, is a signatory to a mutual legal assistance treaty that "allow[s] for the general exchange of evidence and information in criminal and related matters."[93] The United States and China also signed a mutual legal assistance treaty in June 2000.[94] As a signatory, China is required to comply with U.S. requests for legal assistance. According to the State Department, however, "Many outstanding requests by both the United States and China remain unfulfilled," further hindering U.S.-China cooperation efforts.[95]

U.S law enforcement has noted that China's relatively limited cooperation with the United States on curbing fentanyl stands in notable contrast to China's cooperation with Australia on methamphetamines.[96] In 2017, Australia was the only Western country to have a joint task force with China's National Narcotics Control Bureau.[97] This

[*] The DEA noted that the field office in Shanghai is expected to improve anti-money laundering investigations, while the field office in Guangzhou is expected to work with China to stem the flow of precursors. Guangzhou is the capital of Guangdong Province, a major chemical hub in China. Official, U.S. Drug Enforcement Administration, interview with Commission staff, March 15, 2021.

cooperation led to multiple convictions and drug seizures in Australia, including the 2017 seizure of almost 2,000 pounds of crystal meth, the largest seizure of drugs in Australia's history.[98]

Conclusions and Considerations for Congress

The fentanyl challenge has grown in complexity since Chinese suppliers began to evolve their tactics in 2019. Drug producers and smugglers in China are becoming more sophisticated in evading Chinese and U.S. authorities, and the growing involvement of Mexican cartels and advanced money laundering schemes have exacerbated the problem. Law enforcement agencies are struggling to keep pace with a rapidly changing illicit drug environment. As Chinese fentanyl networks diffuse and seek alternatives to China as a source for precursor chemicals, U.S. authorities will have to develop solutions that reflect the more globalized nature of the supply chains. Enforcement can no longer be approached unilaterally or even bilaterally because fentanyl traffickers are operating transnationally. This presents a potential opportunity for the United States to work with other countries on counternarcotic enforcement.

Multilateral Cooperation: Abuse of illegally sourced fentanyl is not a problem for the United States alone. Fentanyl is also being shipped to Canada, Europe, and other destinations via online direct-to-consumer websites and postal delivery. As in the United States, China remains a primary source of illicit fentanyl in Canada, where opioid usage has increased since the start of the COVID-19 pandemic.[99] According to the DEA, fentanyl powder is shipped from China to Canada and sold there or smuggled into the United States.[100] Europe is also a growing market for illicit Chinese-sourced fentanyl, although not nearly on the same level as North America.[101]

Both China and Mexico are signatories to the 1988 UN Drug Convention. At the urging of the United States, in October 2017 the UN required all parties who are signatories to the convention to schedule 4-ANPP and NPP, two popular fentanyl precursors.[102] In January 2018, China scheduled the two precursors. Another key precursor, 4-AP, has no legitimate uses but has not been listed in the UN's schedules; currently, only the United States has scheduled 4-AP and has been urging China to do so as well. Historically, a multilateral approach through international bodies has proven to be effective in pressuring China to introduce additional restrictions on fentanyl.

Joint Operations: In contrast to limited U.S.-China cooperation, the United States and India have achieved a degree of joint operational successes in combating trafficking. For example, in 2017 U.S. and Indian authorities cooperated in an operation leading to the seizure of over one billion tablets of illegally trafficked tramadol, a type of synthetic opioid.[103] In Operation Broadsword in January 2020, the U.S. Food and Drug Administration, CBP, and the Office of Criminal Investigations in India jointly targeted and inspected 800 shipments entering the United States through the international mail facility. These shipments "had been transshipped through third party countries to conceal their place of origin," and many contained counterfeit and illegal opioid drugs.[104] The operations ultimately stopped millions of counterfeit and illegal opioids.[105] The United States and China have yet to conduct similar coordination.

Congressional Role: Digital tools and advanced money laundering techniques are increasingly being used by traffickers. Enforcement on these digital platforms remains highly challenging for U.S. authorities. According to the 2020 Reuters investigative report, when asked about these new advanced forms of money laundering, a source familiar with these operations said, "It is the most sophisticated form of money laundering that's ever existed."[106] Even though traffickers' growing arsenal of tactics presents a unique and complex challenge, Congress could play a significant role in countering these new avenues of illicit transactions. The 2021 National Defense Authorization Act directed the Treasury Department to conduct a comprehensive report to Congress on the illicit financing and money laundering risk posed by Chinese bad actors and to assess the role of Chinese regulations in permitting such risk.[107] The findings from the report are likely to shed more light on this complex means of money laundering and may provide insights into opportunities for future Congressional action.

Appendix

Table 1: Popular Known Fentanyl Precursors China Has Not Banned

Masked substitutes: Chemically altered precursor substitutes meant to escape detection, but can easily be transformed into a controlled fentanyl precursor	• 4-AP • 4,4-PIPERIDINEDIOL
Unmasked substitutes: Are not chemically altered precursors	• 1-BOC-4ANPP • 1-BOC-4-PIPERIDONE

Source: C4ADS, "Lethal Exchanges: Synthetic Drug Networks in the Digital Era," November 17, 2020. *https://www.c4reports.org/lethal-exchange*.

Table 2: How Chinese Brokers Launder Money for Mexican Cartels

Step One	A Mexican cartel wants to bring proceeds from U.S. drug sales back to Mexico. It contacts Chinese money brokers operating in Mexico to see who offers the cheapest rates.
Step Two	The parties agree on a commission and the amount to be laundered, say $150,000.
Step Three	Using encrypted phone messages, the Chinese broker sends the cartel member: 1) A code word; 2) A number from a U.S. burner phone; and 3) A unique serial number from a $1 bill
Step Four	The Mexican cartel shares those details with a cartel-linked drug dealer in the United States, who calls the burner phone and identifies himself using the code word. He arranges to meet a U.S.-based money courier working for the Chinese broker.
Step Five	The drug dealer and the money courier meet in public somewhere in the United States. The courier hands over a $1 bill with the unique serial number. When that checks out, the dealer hands over the cash, keeping the bill as a "receipt."
Step Six	The courier takes the $150,000 to a U.S.-based Chinese merchant, who has a bank account in China. The merchant then performs a currency swap known as a "mirror transaction." He takes possession of the U.S. cash and then transfers $150,000 worth of Chinese RMB from his Chinese bank account to the money broker's Chinese account using an account number provided to him by the courier.
Step Seven	The cartel's drug cash is now sitting in a Chinese bank, outside the view of U.S. law enforcement. The broker has two options to send it on to the drug cartel in Mexico.
Step Eight	(option 1) Do another "mirror transaction." The $150,000 worth of RMB is now transferred from the money broker's Chinese account to the Chinese bank account of a Mexico-based businessperson. That Mexico-based businessperson then provides $150,000 worth of pesos to the money broker in Mexico, who delivers that cash to the cartel. (option 2) The Chinese money broker buys $150,000 worth of consumer products in China, such as clothing, and exports them to Mexico. The goods are then sold and the proceeds are delivered to the cartel.

Source: Drazen Jorgic, "Factbox: Step by Step - How Chinese 'Money Brokers' Launder Cash for Mexican Drug Cartels," *Reuters*, December 3, 2020. *https://www.reuters.com/article/us-mexico-china-cartels-factbox/factbox-step-by-step-how-chinese-money-brokers-launder-cash-for-mexican-drug-cartels-idUSKBN28D1LW*.

Endnotes

[1] U.S. Centers for Disease Control, *Overdose Deaths Accelerated during COVID-19*, December 17, 2020. *https://www.cdc.gov/media/releases/2020/p1218-overdose-deaths-covid-19.html*.

[2] U.S. Centers for Disease Control, *Provisional Drug Overdose Death Counts*, *https://www.cdc.gov/nchs/nvss/vsrr/drug-overdose-data.htm*. U.S. Centers for Disease Control, *Drug Overdose Deaths in the U.S. Up 30% in 2020*, July 14, 2021. https://www.cdc.gov/nchs/pressroom/nchs_press_releases/2021/20210714.htm.

[3] Margaret Williams, "Why Overdose Deaths Are Surging amid COVID-19," *Ohio State University Wexner Medical Center*, July 16, 2020. *https://wexnermedical.osu.edu/blog/why-are-overdose-deaths-surging-amid-covid-19*.

[4] U.S. Drug Enforcement Administration, *2020 National Drug Threat Assessment*, March 2021. https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf.

[5] U.S. Drug Enforcement Administration, *2020 National Drug Threat Assessment*, March 2021. https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf.

[6] U.S. House Energy and Commerce Subcommittee on Oversight and Investigations, *Oversight of Federal Efforts to Combat the Spread of Illicit Fentanyl Hearing*, QFR Response of Thomas Overacker, April 10, 2020. *https://docs.house.gov/meetings/IF/IF02/20190716/109817/HHRG-116-IF02-Wstate-OverackerT-20190716-SD002.pdf*.

[7] U.S. House Energy and Commerce Subcommittee on Oversight and Investigations, *Oversight of Federal Efforts to Combat the Spread of Illicit Fentanyl Hearing*, Q&A, July 16, 2019. *https://energycommerce.house.gov/committee-activity/hearings/hearing-on-oversight-of-federal-efforts-to-combat-the-spread-of-illicit*.

[8] U.S. House Energy and Commerce Subcommittee on Oversight and Investigations, *Oversight of Federal Efforts to Combat the Spread of Illicit Fentanyl Hearing*, QFR Response of Thomas Overacker, April 10, 2020; U.S. Drug Enforcement Administration, *2020 National Drug Threat Assessment*, March 2021. *https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf*. U.S. Drug Enforcement Agency, 2020 National Drug Threat Assessment, March 2021. *https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf*.

[9] *Reuters*, "Mexico Government Says Fentanyl Seizures Up Almost Six-Fold in 2020." *https://www.reuters.com/article/us-mexico-drugs/mexico-says-fentanyl-seizures-up-almost-six-fold-in-2020-idUSKBN2951KV*.

[10] Drug Enforcement Administration, National Drug Threat Assessment, March 2021, https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf.

[11] Mark Landler, "U.S and China Call Truce in Trade War," December 1, 2018. *https://www.nytimes.com/2018/12/01/world/trump-xi-g20-merkel.html*.

[12] Zhang Yang, "From May 1st, the Entire Class Fentanyl Substances Will Be Regulated," *State Council of Information Office of the People's Republic of China*. *http://www.scio.gov.cn/34473/34474/Document/1651166/1651166.htm*.

[13] U.S. Drug Enforcement Administration, *DEA Intelligence Report: Fentanyl Flow to the United States*, January 2020. *https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf*

[14] U.S. House Energy and Commerce Subcommittee on Oversight and Investigations. *Oversight of Federal Efforts to Combat the Spread of Illicit Fentanyl Hearing*, Q&A, July 16, 2019. *https://energycommerce.house.gov/committee-activity/hearings/hearing-on-oversight-of-federal-efforts-to-combat-the-spread-of-illicit*.

[15] U.S. Department of the Treasury, *Counter Narcotics Trafficking Sanction*, January 2021. *https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/counter-narcotics-trafficking-sanctions*

[16] U.S. Department of Justice, *Justice News: Press Releases and Speeches*, January 2021. *https://www.justice.gov/news*.

[17] Michael Lohmuller, Nicole Cook, and Logan Pauley, "Lethal Exchange: Synthetic Drug Networks in the Digital Era," *C4ADS*, January 2020. *https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5fb3077189409576d229502a/1605568376184/Lethal_Exchange_Spread.pdf.*

[18] U.S. Drug Enforcement Administration, *Drug Fact Sheet*, April 2020. *https://www.dea.gov/sites/default/files/2020-06/Synthetic%20Opioids-2020.pdf*; National Institute of Health, Fentanyl DrugFacts, June 2021. *https://www.drugabuse.gov/publications/drugfacts/fentanyl*; U.S. Drug Enforcement Administration, *Drug Fact Sheet*, April 2020. *https://www.dea.gov/sites/default/files/2020-06/Fentanyl-2020_0.pdf*; U.S. Drug Enforcement Administration, *Drug Scheduling*, *https://www.dea.gov/drug-information/drug-scheduling*; National Institute of Health, *National Cancer Institute Dictionaries*, *Definition of controlled substance - NCI Dictionary of Cancer Terms - National Cancer Institute*; U.S. Drug Enforcement Administration, *2020 National Drug Threat Assessment*, March 2021. https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf.

[19] U.S. Drug Enforcement Administration, *DEA Intelligence Report: Fentanyl Flow to the United States*, January 2020. *https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf*.

[20] U.S. Drug Enforcement Administration, *DEA Intelligence Report: Fentanyl Flow to the United States*, January 2020. *https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf*.

[21] U.S.-China Economic and Security Review Commission, Hearing on Exploring the Growing U.S. Reliance on China's Biotech and Pharmaceutical Products, written testimony of Ben Westhoff, July 31, 2019. *https://www.uscc.gov/sites/default/files/Ben%20Westhoff%20Written%20Testimony.pdf* .

[22] U.S. Department of State, *International Narcotic Control and Substance Report Volume I: Drug and Chemical Control*, March 3, 2020. *https://www.state.gov/wp-content/uploads/2020/06/Tab-1-INCSR-Vol.-I-Final-for-Printing-1-29-20-508-4.pdf.*

[23] Michael Lohmuller, Nicole Cook, and Logan Pauley, "Lethal Exchange: Synthetic Drug Networks in the Digital Era," *C4ADS*, January 2020. *https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5fb3077189409576d229502a/1605568376184/Lethal_Exchange_Spread.pdf.*

[24] Michael Lohmuller, Nicole Cook, and Logan Pauley, "Lethal Exchange: Synthetic Drug Networks in the Digital Era," *C4ADS*, January 2020. *https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5fb3077189409576d229502a/1605568376184/Lethal_Exchange_Spread.pdf.*

[25] Michael Lohmuller, Nicole Cook, and Logan Pauley, "Lethal Exchange: Synthetic Drug Networks in the Digital Era," *C4ADS*, January 2020. *https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5fb3077189409576d229502a/1605568376184/Lethal_Exchange_Spread.pdf.*

[26] U.S. Department of State, *International Narcotic Control and Substance Report Volume I: Drug and Chemical Control*, March 3, 2020. *https://www.state.gov/wp-content/uploads/2020/06/Tab-1-INCSR-Vol.-I-Final-for-Printing-1-29-20-508-4.pdf.*

[27] Bryce Pardo, RAND Corporation, interview with Commission staff, February 17, 2021.

[28] U.S. Drug Enforcement Administration, *2020 National Drug Threat Assessment*, March 2021. https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf.

[29] U.S. Drug Enforcement Administration, *DEA Intelligence Report: Fentanyl Flow to the United States*, January 2020. *https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf*.

[30] Michael Lohmuller, Nicole Cook, and Logan Pauley, "Lethal Exchange: Synthetic Drug Networks in the Digital Era," *C4ADS*, January 2020. *https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5fb3077189409576d229502a/1605568376184/Lethal_Exchange_Spread.pdf.*

[31] Michael Lohmuller, Nicole Cook, and Logan Pauley, "Lethal Exchange: Synthetic Drug Networks in the Digital Era," *C4ADS*, January 2020. *https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5fb3077189409576d229502a/1605568376184/Lethal_Exchange_Spread.pdf.*

[32] Michael Lohmuller, Nicole Cook, and Logan Pauley, "Lethal Exchange: Synthetic Drug Networks in the Digital Era," *C4ADS*, January 2020. *https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5fb3077189409576d229502a/1605568376184/Lethal_Exchange_Spread.pdf.*

[33] Michael Lohmuller, Nicole Cook, and Logan Pauley, "Lethal Exchange: Synthetic Drug Networks in the Digital Era," *C4ADS*, January 2020. *https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5fb3077189409576d229502a/1605568376184/Lethal_Exchange_Spread.pdf.*

[34] Michael Lohmuller, Nicole Cook, and Logan Pauley, "Lethal Exchange: Synthetic Drug Networks in the Digital Era," *C4ADS*, January 2020. *https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5fb3077189409576d229502a/1605568376184/Lethal_Exchange_Spread.pdf.*

[35] Michael Lohmuller, Nicole Cook, and Logan Pauley, "Lethal Exchange: Synthetic Drug Networks in the Digital Era," *C4ADS*, January 2020. *https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5fb3077189409576d229502a/1605568376184/Lethal_Exchange_Spread.pdf.*

[36] White House Office of National Drug Control Policy, *White House Office of National Drug Control Policy Announces Record Reduction in Poppy Cultivation and Potential Heroin Production in Mexico*, July 31, 2020. *https://trumpwhitehouse.archives.gov/briefings-statements/ondcp-announces-record-reduction-poppy-cultivation-potential-heroin-production-mexico/*.

[37] Chris Adams, "The Fentanyl Surge," *National Press Foundation*, April 21, 2021. *https://nationalpress.org/topic/the-fentanyl-surge/*.

[38] U.S. House Energy and Commerce Subcommittee on Oversight and Investigations, *Oversight of Federal Efforts to Combat the Spread of Illicit Fentanyl Hearing*, QFR Response of Thomas Overacker, April 10, 2020; U.S. Drug Enforcement Administration, *2020 National Drug Threat Assessment*, March 2021. *https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf*.

[39] Official, U.S. Drug Enforcement Administration, interview with Commission staff, March 15, 2021.

[40] Hollie McKay, "Chinese Cartels Quietly Operating in Mexico, Aiding US Drug Crisis," *Fox News*, November 12, 2020. *https://www.foxnews.com/world/chinese-cartels-mexico-us-drug-crisis*.

[41] U.S. Drug Enforcement Administration, *DEA Intelligence Report: Fentanyl Flow to the United States*, January 2020. https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008*20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf.*

[42] Hollie McKay, "Chinese Cartels Quietly Operating in Mexico, Aiding US Drug Crisis," *Fox News*, November 12, 2020. *https://www.foxnews.com/world/chinese-cartels-mexico-us-drug-crisis*.

[43] Hollie McKay, "Chinese Cartels Quietly Operating in Mexico, Aiding US Drug Crisis," *Fox News*, November 12, 2020. *https://www.foxnews.com/world/chinese-cartels-mexico-us-drug-crisis*.

[44] Hollie McKay, "Chinese Cartels Quietly Operating in Mexico, Aiding US Drug Crisis," *Fox News*, November 12, 2020. *https://www.foxnews.com/world/chinese-cartels-mexico-us-drug-crisis*.

[45] Hollie McKay, "Chinese Cartels Quietly Operating in Mexico, Aiding US Drug Crisis," *Fox News*, November 12, 2020. *https://www.foxnews.com/world/chinese-cartels-mexico-us-drug-crisis*.

[46] Hollie McKay, "Chinese Cartels Quietly Operating in Mexico, Aiding US Drug Crisis," *Fox News*, November 12, 2020. *https://www.foxnews.com/world/chinese-cartels-mexico-us-drug-crisis*.

[47] Hollie McKay, "Chinese Cartels Quietly Operating in Mexico, Aiding US Drug Crisis," *Fox News*, November 12, 2020. *https://www.foxnews.com/world/chinese-cartels-mexico-us-drug-crisis*.

[48] Hollie McKay, "Chinese Cartels Quietly Operating in Mexico, Aiding US Drug Crisis," *Fox News*, November 12, 2020. *https://www.foxnews.com/world/chinese-cartels-mexico-us-drug-crisis*.

[49] Hollie McKay, "Chinese Cartels Quietly Operating in Mexico, Aiding US Drug Crisis," *Fox News*, November 12, 2020. *https://www.foxnews.com/world/chinese-cartels-mexico-us-drug-crisis*.

[50] Eric Heisig, "Chinese Fentanyl, the Dark Web and Over-Prescribing Doctors: AG Sessions Talks Combating Opioid Epidemic in Cleveland," January 30, 2019. *https://www.cleveland.com/court-justice/2018/08/chinese_fentanyl_the_dark_web.html*.

[51] U.S. Immigration and Customs Enforcement, *2 Chinese Nationals Charged with Operating Global Opioid Conspiracy Resulting in Death*, August 22, 2018. *https://www.ice.gov/news/releases/2-chinese-nationals-charged-operating-global-opioid-conspiracy-resulting-deaths*.

[52] U.S. Department of State, *Designation of PRC Foreign Nationals and Entities under the Foreign Narcotics Kingpin Designation Act. https://www.state.gov/designation-of-prc-foreign-nationals-and-entities-under-the-foreign-narcotics-kingpin-designation-act/*.

[53] *U.S. News and World Report*, "U.S. Sanctions Four China-Based Individuals, Firm over Fentanyl, July 17, 2020. *https://www.usnews.com/news/world/articles/2020-07-17/us-sanctions-four-china-based-individuals-firm-over-fentanyl*.

[54] Hollie McKay, "Chinese Cartels Quietly Operating in Mexico, Aiding US Drug Crisis," *Fox News*, November 12, 2020. *https://www.foxnews.com/world/chinese-cartels-mexico-us-drug-crisis*.

[55] Official, U.S. Drug Enforcement Administration, interview with Commission staff, March 15, 2021.

[56] Official, U.S. Drug Enforcement Administration, interview with Commission staff, March 15, 2021.

[57] Drazen Jorgic, "Special Report: Burner Phones and Mobile Banking Apps: Meet the Chinese Brokers Laundering Mexican Drug Money," *Reuters*, December 3, 2020. *https://www.reuters.com/article/us-mexico-china-cartels-specialreport/special-report-burner-phones-and-banking-apps-meet-the-chinese-brokers-laundering-mexican-drug-money-idUSKBN28D1M4*.

[58] Drazen Jorgic, "Special Report: Burner Phones and Mobile Banking Apps: Meet the Chinese Brokers Laundering Mexican Drug Money," *Reuters*, December 3, 2020. *https://www.reuters.com/article/us-mexico-china-cartels-specialreport/special-report-burner-phones-and-banking-apps-meet-the-chinese-brokers-laundering-mexican-drug-money-idUSKBN28D1M4*.

[59] U.S. Drug Enforcement Administration, *2020 National Drug Threat Assessment*, March 2021. https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf.

[60] Drazen Jorgic, "Special Report: Burner Phones and Mobile Banking Apps: Meet the Chinese Brokers Laundering Mexican Drug Money," *Reuters*, December 3, 2020. *https://www.reuters.com/article/us-mexico-china-cartels-specialreport/special-report-burner-phones-and-banking-apps-meet-the-chinese-brokers-laundering-mexican-drug-money-idUSKBN28D1M4*.

[61] U.S. Department of Justice, *Three Indicted for International Money Laundering Schemes Pairing Mexican Drug Traffickers and Chinese Nationals*, October 18, 2019. *https://www.justice.gov/usao-or/pr/three-indicted-international-money-laundering-scheme-pairing-mexican-drug-traffickers-and*.

[62] U.S. Department of Justice, *Chinese Nationals Sentenced for Laundering Millions for Mexican Drug Cartels*, September 29, 2020. *https://www.justice.gov/opa/pr/chinese-national-sentenced-laundering-millions-mexican-drug-cartels*.

[63] Drazen Jorgic, "Special Report: Burner Phones and Mobile Banking Apps: Meet the Chinese Brokers Laundering Mexican Drug Money," *Reuters*, December 3, 2020. *https://www.reuters.com/article/us-mexico-china-cartels-specialreport/special-report-burner-phones-and-banking-apps-meet-the-chinese-brokers-laundering-mexican-drug-money-idUSKBN28D1M4*.

[64] Alexander Weber, Boris Groendahl, and Nicholas Comfort, "Money to Launder? Here's How (Hint: Find a Bank)," *Bloomberg*, April 19, 2019. *https://www.bloombergquint.com/quicktakes/money-to-launder-here-s-how-hint-find-a-bank-quicktake*.

[65] Drazen Jorgic, "Special Report: Burner Phones and Mobile Banking Apps: Meet the Chinese Brokers Laundering Mexican Drug Money," *Reuters*, December 3, 2020. *https://www.reuters.com/article/us-mexico-china-cartels-specialreport/special-report-burner-phones-and-banking-apps-meet-the-chinese-brokers-laundering-mexican-drug-money-idUSKBN28D1M4*.

[66] The White House, *Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids*, August 21, 2019.https://www.fincen.gov/sites/default/files/advisory/2019-08-21/Fentanyl%20Advisory%20FINAL%20508.pdf.

[67] Diego Ore, "INSIGHT - Latin American Crime Cartels Turn to Crypto to Clean Their Cash," *Reuters*, December 8, 2020. *https://www.reuters.com/article/mexico-bitcoin/insight-latin-american-crime-cartels-turn-to-crypto-to-clean-up-their-cash-idUSL1N2IJ01D*.

[68] Drazen Jorgic, "Special Report: Burner Phones and Mobile Banking Apps: Meet the Chinese Brokers Laundering Mexican Drug Money," *Reuters*, December 3, 2020. *https://www.reuters.com/article/us-mexico-china-cartels-specialreport/special-report-burner-phones-and-banking-apps-meet-the-chinese-brokers-laundering-mexican-drug-money-idUSKBN28D1M4.*

[69] Drazen Jorgic, "Special Report: Burner Phones and Mobile Banking Apps: Meet the Chinese Brokers Laundering Mexican Drug Money," *Reuters*, December 3, 2020. *https://www.reuters.com/article/us-mexico-china-cartels-specialreport/special-report-burner-phones-and-banking-apps-meet-the-chinese-brokers-laundering-mexican-drug-money-idUSKBN28D1M4.*

[70] Bill Chappell, "China Jails 9 in Fentanyl Trafficking Case that Began with a Tip from the U.S." *NPR*, November 7, 2019. *https://www.npr.org/2019/11/07/777173066/china-jails-9-in-fentanyl-trafficking-case-that-began-with-a-u-s-tip*.

[71] Bill Chappell, "China Jails 9 in Fentanyl Trafficking Case that Began with a Tip from the U.S." *NPR*, November 7, 2019. *https://www.npr.org/2019/11/07/777173066/china-jails-9-in-fentanyl-trafficking-case-that-began-with-a-u-s-tip*.

[72] Steven Lee Meyers, "China Sentences Man to Death for Trafficking Fentanyl to the U.S.," *New York Times*, November 7, 2019. *https://www.nytimes.com/2019/11/07/world/asia/china-fentanyl-death-penalty.html*.

[73] *South China Morning Post*, "Fentanyl Trafficker in China Sentenced to Death," Interview with Yu Haibing, November 7, 2019. *https://www.youtube.com/watch?v=DrABhGDoJJ8*.

[74] SUPPORT for Patients and Communities Act, Public Law No: 115-271, October 24, 2018. *https://www.congress.gov/bill/115th-congress/house-bill/6*.

[75] U.S. Postal Service Office of the Inspector General, *Implementing Advanced Electronic Data: Challenges and Opportunities*, September 30, 2020. *https://www.uspsoig.gov/document/implementing-advanced-electronic-data-challenges-and-opportunities#:~:text=Advance%20Electronic%20Data%20(AED,opioids%20and%20other%20illicit%20goods*.

[76] Gary Barksdale, written testimony to the Committee on Energy and Commerce Subcommittee on Oversight and Investigations, July 16, 2019. *https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony%20-%20Barksdale%2020190716.pdf*.

[77] U.S. Postal Service Office of the Inspector General, *RISC Report: Implementing Advance Electronic Data: Challenges and Opportunities*, September 30, 2020. *https://www.uspsoig.gov/sites/default/files/document-library-files/2020/RISC-WP-20-010.pdf.*

[78] U.S. House Judiciary Subcommittee on Crime, Terrorism and Homeland Security, *Hearing on Fentanyl Analogues: Perspectives on Classwide Scheduling*, written testimony of Amanda Liskamm, January 28, 2020. *https://www.congress.gov/116/meeting/house/110392/witnesses/HHRG-116-JU08-Wstate-LiskammA-20200128.pdf*.

[79] U.S. House Judiciary Subcommittee on Crime, Terrorism and Homeland Security, *Hearing on Fentanyl Analogues: Perspectives on Classwide Scheduling*, written testimony of Amanda Liskamm, January 28, 2020.

[80] U.S. Senate Homeland Security Committee Subcommittee on Investigations, *Hearing on Combating the Opioid Crisis: Implementation of the STOP Act*, written testimony of Thomas Overacker, December 10, 2020.

[81] U.S. Senate Homeland Security Committee Subcommittee on Investigations, *Hearing on Combating the Opioid Crisis: Implementation of the STOP Act*, written testimony of Thomas Overacker, December 10, 2020.

[82] U.S. House Energy and Commerce Subcommittee on Oversight and Investigations, *Hearing on Oversight of Federal Efforts of Combat the Spread of Illicit Fentanyl*, written testimony of Matthew Donahue, September 6, 2019. *https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony%20-%20Donanue%2020190716.pdf*.

[83] U.S. House Energy and Commerce Subcommittee on Oversight and Investigations, *Hearing on Oversight of Federal Efforts of Combat the Spread of Illicit Fentanyl*, written testimony of Matthew Donahue, September 6, 2019.

[84] Official, U.S. Drug Enforcement Administration, interview with Commission staff, March 15, 2021.

[85] U.S. House Energy and Commerce Subcommittee on Oversight and Investigations, *Hearing on Oversight of Federal Efforts of Combat the Spread of Illicit Fentanyl*, written testimony of David Price, September 6, 2019.

[86] Drazen Jorgic, "Special Report: Burner Phones and Mobile Banking Apps: Meet the Chinese Brokers Laundering Mexican Drug Money," *Reuters*, December 3, 2020. *https://www.reuters.com/article/us-mexico-china-cartels-specialreport/special-report-burner-phones-and-banking-apps-meet-the-chinese-brokers-laundering-mexican-drug-money-idUSKBN28D1M4.*

[87] Drazen Jorgic, "Special Report: Burner Phones and Mobile Banking Apps: Meet the Chinese Brokers Laundering Mexican Drug Money," *Reuters*, December 3, 2020. *https://www.reuters.com/article/us-mexico-china-cartels-specialreport/special-report-burner-phones-and-banking-apps-meet-the-chinese-brokers-laundering-mexican-drug-money-idUSKBN28D1M4.*

[88] Sean O'Connor*, "Fentanyl Flows from China: An Update since 2017," U.S.-China Economic Security and Review Commission,* November 26, 2018. *https://www.uscc.gov/sites/default/files/Research/Fentanyl%20Flows%20from%20China.pdf*.

[89] Elaine Shannon, "China Syndrome: How Xi Played Trump on Fentanyl," *Spycast*. *https://www.spytalk.co/p/china-syndrome.*

[90] U.S. Department of State, *International Narcotic Control Strategy Volume II: Money Laundering*, March 3, 2020. *https://www.state.gov/wp-content/uploads/2020/03/Tab-2-INCSR-Vol-2-508.pdf*.

[91] U.S. House Energy and Commerce Subcommittee on Oversight and Investigations, *Oversight of Federal Efforts to Combat the Spread of Illicit Fentanyl Hearing,* Q&A David Prince, July 16, 2019. *https://energycommerce.house.gov/committee-activity/hearings/hearing-on-oversight-of-federal-efforts-to-combat-the-spread-of-illicit*.

[92] *Reuters*, "China Says Has Only Limited Cooperation with the U.S. on Fentanyl," September 3, 2019. *https://www.reuters.com/article/us-usa-china-fentanyl/china-says-has-only-limited-cooperation-with-u-s-on-fentanyl-idUSKCN1VO0AD*.

[93] U.S. Department of State, *Treaties and Mutual Agreements*, July 29, 2021. https://2009-2017.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm.

[94] U.S. Department of State, *Treaties in Force: A List of Treaties and Other International Agreements of the United States in Force on January 1, 2020*, January 2020. *https://www.state.gov/wp-content/uploads/2020/08/TIF-2020-Full-website-view.pdf.*

[95] U.S. Department of State, *2020 International Narcotics Control Strategy Report*, March 2, 2020. *https://www.state.gov/wp-content/uploads/2020/06/Tab-1-INCSR-Vol.-I-Final-for-Printing-1-29-20-508-4.pdf.*

[96] *Associated Press*, "Australia Police Make Record Crystal Meth Bust," *South China Morning Post*, April 5, 2017. *https://www.scmp.com/news/asia/australasia/article/2084984/australian-police-make-record-crystal-meth-bust-praise.*

[97] *Associated Press*, "Australia Police Make Record Crystal Meth Bust," *South China Morning Post*, April 5, 2017. *https://www.scmp.com/news/asia/australasia/article/2084984/australian-police-make-record-crystal-meth-bust-praise.*

[98] *Associated Press*, "Australia Police Make Record Crystal Meth Bust," *South China Morning Post*, April 5, 2017. *https://www.scmp.com/news/asia/australasia/article/2084984/australian-police-make-record-crystal-meth-bust-praise*.

[99] Holly Honderich, "Opioid Epidemic: The Other Public Health Crisis Killing Canadians," *BBC News. https://www.bbc.com/news/world-us-canada-53954964.*

[100] Andreas Rutauskas, "The Invisible Security of Canada's Seemingly Chill Border," *Wired*, April 1, 2016. *https://www.wired.com/2016/04/invisible-security-canadas-seemingly-chill-border/*.

[101] *BBC*, "Fentanyl Crisis: Is China a Major Source of Illegal Drugs?" September 23, 2018. *https://www.bbc.com/news/world-45564744*.

[102] U.S. State Department, *International Narcotic Control and Substance Report Volume I: Drug and Chemical Control*, March 3, 2020. *https://www.state.gov/wp-content/uploads/2020/06/Tab-1-INCSR-Vol.-I-Final-for-Printing-1-29-20-508-4.pdf.*

[103] Natalie Tecimer, "The Dangerous Opioid from India," *Center for Strategic and International Studies*, January 19, 2018. *https://www.csis.org/npfp/dangerous-opioid-india*.

[104] U.S. Food and Drug Administration, *FDA Takes Action with Indian Government to Protect Consumers from Illicit Medical Products*, February 18, 2020. *https://www.fda.gov/news-events/press-announcements/fda-takes-action-indian-government-protect-consumers-illicit-medical-products*.

[105] U.S. Food and Drug Administration, *FDA Takes Action with Indian Government to Protect Consumers from Illicit Medical Products*, February 18, 2020. *https://www.fda.gov/news-events/press-announcements/fda-takes-action-indian-government-protect-consumers-illicit-medical-products*.

[106] Drazen Jorgic, "Special Report: Burner Phones and Mobile Banking Apps: Meet the Chinese Brokers Laundering Mexican Drug Money," *Reuters*, December 3, 2020. *https://www.reuters.com/article/us-mexico-china-cartels-specialreport/special-report-burner-phones-and-banking-apps-meet-the-chinese-brokers-laundering-mexican-drug-money-idUSKBN28D1M4.*

[107] National Defense Authorization Act for Fiscal Year 2021, Public Law No: 116-283, January 1, 2021. *https://www.congress.gov/bill/116th-congress/house-bill/6395*.

EXHIBIT 131

China Warns Its Citizens on ‘Entrapment’ by US Law Enforcement

Published: Mon Jul 10 14:18:51 EDT 2023

- Unusual warning follows tensions over fentanyl trade
- China has been accused of operating own police stations abroad

By Jacob Gu

(Bloomberg) --

China issued an unusual warning to its citizens traveling to the US to beware of “entrapment” by American law enforcement, in a fresh show of continuing bilateral tensions despite a recent step-up in engagement.

“Chinese nationals who travel to the US should be more vigilant, and beware of falling into US snares and arrest-entrapment,” the Ministry of Foreign Affairs in Beijing said Monday in a security advisory posted on the official Wechat account run by its Department of Consular Affairs.

While Beijing has regularly reminded its citizens of gun and racial violence in the US, it’s rare to explicitly point out the danger of arbitrary detention. China itself has frequently been charged of such detentions of its own people. It’s also faced accusations of running extraterritorial police operations to go after Chinese individuals — something the government denies.

Read More: China Rejects Charge It Runs ‘Illegal’ Overseas Police Stations

Monday’s warning comes on the heels of a high-profile trip to Beijing by Treasury Secretary Janet Yellen, the second Biden administration cabinet member to visit in recent weeks after Secretary of State Antony Blinken. Yellen declared ties between the world’s two largest economies were closer to a “surer footing.”

One area where the US has called for further Chinese efforts is curbing trade in illicit synthetic drugs, to help confront the fentanyl crisis. China’s statement Monday alluded to disagreements in that regard.

The statement cited arbitrary US arrests and the cross-border abduction of Chinese citizens, characterizing the actions as based on fentanyl issues.

Last month, the Justice Department announced the arrest of two individuals and the unsealing of three indictments charging China-based companies and their employees with fentanyl-related crimes.

‘Malicious Smearing’

China’s Foreign Ministry statement also blasted the US for “malicious smearing of China’s pursuit of fugitives.”

In April, the DOJ accused 44 individuals living in China and elsewhere in Asia of harassing Chinese dissidents in the US.

China also asked its citizens in the US to pay close attention to local security situations, citing frequent incidents of gun violence and discrimination against Asians.

To contact the reporter on this story:
Jacob Gu in Houston at jgu3@bloomberg.net

To contact the editors responsible for this story:
Kean Zhang at kzhang65@bloomberg.net
Christopher Anstey

EXHIBIT 132

PRESS RELEASE

Justice Department Announces Eight Indictments Against China-Based Chemical Manufacturing Companies and Employees

Tuesday, October 3, 2023

For Immediate Release

Office of Public Affairs

The Justice Department today announced the unsealing of eight indictments in the Middle and Southern Districts of Florida charging China-based companies and their employees with crimes relating to fentanyl and methamphetamine production, distribution of synthetic opioids, and sales resulting from precursor chemicals.

The indictments build on prosecutions announced in June and mark the second set of prosecutions to charge China-based chemical manufacturing companies and nationals of the People's Republic of China (PRC) for trafficking fentanyl precursor chemicals into the United States.

The indictments complement actions taken today by the Department of the Treasury's Office of Foreign Assets Control (OFAC) to designate 28 individuals and entities involved with the international proliferation of illicit drugs.

“We know that the global fentanyl supply chain, which ends with the deaths of Americans, often starts with chemical companies in China,” said Attorney General Merrick B. Garland. “The United

States government is focused on breaking apart every link in that chain, getting fentanyl out of our communities, and bringing those who put it there to justice."

"The international dimension to the deadly scourge of fentanyl requires the all-of-government response that we are delivering today," said Secretary of Homeland Security Alejandro Mayorkas. "Through the dedication and investigative abilities of agents and officers from HSI, CBP, and our federal partners, we are bringing accountability to ruthless organizations and individuals resident in the People's Republic of China and to the cartel members that seek to profit from the death and destruction that fentanyl causes."

"The charges announced today are another down payment on the Justice Department's pledge to every American family that has lost a loved one to fentanyl poisoning," said Deputy Attorney General Lisa O. Monaco. "Just as we did in the fight against terrorists and cybercriminals, we are deploying a whole-of-government approach – sharing intelligence, combining resources, and relentlessly pursuing justice – to attack the global supply chain fueling the fentanyl crisis. We will not rest until we have rid our communities of this poison."

"Fentanyl is the deadliest drug threat our nation has ever faced. These eight cases are the result of DEA's efforts to attack the fentanyl supply chain where it starts — in China. Chinese chemical companies are fueling the fentanyl crisis in the United States by sending fentanyl precursors, fentanyl analogues, xylazine, and nitazenes into our country and into Mexico. These chemicals are used to make fentanyl and make it especially deadly," said Drug Enforcement Administration (DEA) Administrator Anne Milgram. "DEA will not stop until we defeat this threat. We are grateful to our law enforcement partners whose collaboration and dedication have made these actions possible. I am also deeply grateful for the incredible work by the DEA Miami Field Division. Their pursuit of these organizations demonstrates the drive and determination of the men and women, who are working as one DEA, to defeat the cartels and their entire global supply chain."

"This investigation of a narcotics trafficker utilizing counterfeit postage labels highlights the unique jurisdiction of the Postal Inspection Service," said Chief Postal Inspector Gary R. Barksdale of the U.S. Postal Inspection Service (USPIS). "This indictment is a win in our battle against counterfeit postage and those seeking to use the nation's mail system to distribute dangerous substances."

The DEA led the investigations brought in both districts and used its unique authority to specially schedule protonitazene and metonitazene as Schedule I controlled substances, which was necessary as their adverse health effects, including death, pose an imminent threat to public safety. As a result of that order, the regulatory controls and administrative, civil, and criminal sanctions applicable to Schedule I controlled substances can be imposed on persons who handle or propose to handle these substances. In addition, Homeland Security Investigations (HSI) and U.S. Customs and Border Protection (CBP) seized more than 1,000 kilograms of fentanyl-related precursor chemicals, and the USPIS also traced packages containing the precursor chemicals mailed through the U.S. mail and analyzed their contents after seizure.

Fentanyl is the deadliest drug threat facing the United States. Not only is fentanyl 50 times more potent than heroin and 100 times more potent than morphine, a dose of as little as two milligrams can kill a grown adult. Fentanyl analogues are similar in chemical structure and effects as fentanyl. Fentanyl is the leading cause of death for Americans ages 18 to 49. From February 2022 to January, at least 105,263 Americans died of drug overdoses, the majority of which involved synthetic opioids such as fentanyl and fentanyl analogues.

Protonitazene and metonitazene are synthetic opioids that were emergency listed as Schedule I controlled substances in April 2022. There are no approved medical uses for protonitazene and metonitazene in the United States, or anywhere else in the world. Drug traffickers typically mix protonitazene and metonitazene with other opioids, such as fentanyl, to create new and more powerful cocktails of dangerous opioids. Methamphetamine overdose deaths are also surging in the United States. Methamphetamine is becoming more deadly because it is more frequently being mixed with highly potent fentanyl. There are currently no FDA-approved medications for treating methamphetamine use disorder or reversing overdoses. Drug overdose deaths involving psychostimulants, primarily methamphetamine, rose from 547 deaths in 1999 to 32,537 deaths in 2021.

The manufacture of fentanyl and methamphetamine begins with raw chemicals, known as precursors. Fentanyl and methamphetamine precursors, opioid additives, and synthetic opioids are manufactured and distributed by China-based chemical companies, many of which openly advertise on the internet. These China-based manufacturers ship fentanyl and methamphetamine precursors, opioid additives, and synthetic opioids around the world, including to the United States and Mexico, where drug cartels and traffickers combine the chemicals and then distribute fentanyl and methamphetamines throughout the United States to individual users.

These China-based chemical companies often attempt to evade law enforcement by using re-shippers in the United States, false return labels, false invoices, fraudulent postage, and packaging that conceals the true contents of the parcels and the identity of the distributors. In addition, these companies tend to use cryptocurrency transactions to conceal their identities and the location and movement of their funds.

The primary distributors of fentanyl and fentanyl analogues in North America are the Sinaloa Cartel based in Sinaloa, Mexico, and the Cartel Jalisco Nueva Generación based in Jalisco, Mexico. These two transnational criminal organizations have significant presences throughout Mexico, maintain distribution hubs in various cities across the United States, and control smuggling corridors into the United States.

Organizations such as the Sinaloa Cartel and Cartel Jalisco Nueva Generación receive fentanyl precursors from China that are then synthesized within clandestine laboratories into finished fentanyl at scale. China-based precursor chemical manufacturers ship precursors from mainland China by, among other methods, mislabeling the products being shipped and using containers and other packaging to mask their illicit contents.

Middle District of Florida

Five indictments were unsealed in the Middle District of Florida charging five Chinese corporations and eight Chinese nationals with the illegal importation of fentanyl and fentanyl-related chemicals into the United States.

According to the indictments, the defendants openly advertised their ability to thwart U.S. customs and deliver the chemicals used to make fentanyl to the Middle District of Florida and elsewhere in the United States. The defendants used fake shipping labels and special delivery procedures to ensure the illicit chemicals went undetected. The defendants played various roles, such as coordinators and suppliers, and eight defendants are also charged with international money laundering. According to the indictments, the Chinese companies demonstrated past success delivering a stable supply of product to clients in Mexico for years.

“The protection of our country from the deadly scourge of fentanyl is a key priority of the Department of Justice and my office,” said U.S. Attorney Roger B. Handberg for the Middle District of Florida. “We will continue to pursue cases against Chinese chemical companies who are knowingly manufacturing and exporting fentanyl precursors to profit on the pain and suffering of people in the United States. We thank our partners at the Drug Enforcement Administration for their tireless efforts in support of these prosecutions.”

Hebei Shenghao Import and Export Company, based in Shijiazhuang, Hebei Province, China, is charged with fentanyl trafficking conspiracy, along with Chinese nationals Qingshun Li, 29, who allegedly negotiates the sale of precursor chemicals and maintains a bank account for the receipt of payments; Qingsong Li, 32; and Chunhui Chen, 33, both of whom allegedly maintain cryptocurrency wallets for the remittance of payments of precursor chemicals; Chunzhou Chen, 30, who allegedly received Western Union payments on behalf of Hebei Shenghao.

Lihe Pharmaceutical Technology Company, based in Wuhan, Hebei Province, China, was charged with fentanyl trafficking conspiracy and international money laundering, along with Chinese nationals Mingming Wang, 34, who is the alleged holder for three bitcoin accounts shared by sales agents for Lihe Pharmaceutical, and Xinqiang Lu, 40, the alleged recipient of funds via Western Union on the company’s behalf.

Henan Ruijiu Biotechnology Company, based in Zhengzhou, Henan Province, China, was charged with attempted importation of fentanyl precursor and attempted international money laundering, along with Chinese national Yongle Gao, 30, who is the alleged registered owner of the bitcoin wallet associated with Henan Ruijiu.

Xiamen Wonderful Biotechnology Company, based in Xiamen, Fujian Province, China, was charged with attempted importation of fentanyl precursor and attempted international money laundering, along with Chinese national Guo Liang, 34, the alleged registered owner of the bitcoin wallet associated with Xiamen Wonderful.

Anhui Ruihan Technology Company, based in Hefei, Anhui Province, China, was charged with attempted importation of fentanyl precursor and attempted international money laundering.

DEA investigated these cases.

Assistant U.S. Attorney Daniel Baeza and Special Assistant U.S. Attorney Michael Leath for the Middle District of Florida are prosecuting the cases.

Southern District of Florida

Three indictments were unsealed in the Southern District of Florida charging three Chinese companies and four officers and employees with fentanyl trafficking, synthetic opioid trafficking, precursor chemical importation, defrauding the U.S. Postal Service, and making and using counterfeit postage.

“Targeting those who fuel the opioid epidemic, regardless of who they are and where they are operating from, is one of our district’s top priorities,” said U.S. Attorney Markenzy Lapointe for the Southern District of Florida. “Today, we announced charges against the Chinese companies and employees that manufacture and introduce the raw chemicals at the start of the fentanyl and methamphetamine supply chain. This is only the beginning of our fight. The precursors and synthetic opioids that are being marketed, sold, and shipped to the United States and Mexico are being mixed and re-distributed into our local communities as powerful and potentially deadly cocktails of controlled substances. We commend our partner agencies for their skill and resourcefulness, as we work collectively to prosecute the sources of the poison and protect the public.”

Hanhong Medicine Technology Company, a pharmaceutical company located in Wuhan, Hubei Province, China, was charged in a four-count indictment, along with Chinese nationals Changgen Du, 30, and Xuebi Gan, 28. According to the indictment, Hanhong has exported large quantities of fentanyl precursors and non-opioid additives, like xylazine, to the United States and Mexico, including to a drug trafficker in Pennsylvania and to a drug trafficker in the Sinaloa cartel for the manufacture of fentanyl in Mexico for eventual distribution in the United States. Xylazine is often mixed with fentanyl to increase the effects of the drug for users. Xylazine is a non-opioid drug approved for veterinary use for purposes of sedation, anesthesia, muscle relaxation, and pain relief in horses, cattle, and other animals. It is not approved for human use.

Many opioid users are unaware they are taking xylazine. Overdose deaths involving xylazine have steadily increased year over year. Drug users who inject xylazine, or drug mixtures containing xylazine, often develop necrotic tissue resulting in disfiguring wounds or amputation.

The Du Transnational Criminal Organization is listed on the United States Attorney General's Consolidated Priority Organization Target (CPOT) list. The CPOT list identifies the most significant transnational criminal organizations presenting a priority threat to the United States, including those international drug and money laundering organizations affecting the illicit drug supply of the United States. The CPOT list identifies those criminal organizations by the name(s) of their leaders. Du, as the criminal organization's leader, is the director of Hanhong and allegedly negotiates sales with customers. Gan is an alleged sales representative. Du and Gan each operated a crypocurrency wallet that accepted payment for Hanhong's sales. The four-count indictment charges Hanhong, Du, and Gan with conspiracy to manufacture and distribute fentanyl; conspiracy to manufacture and distribute a fentanyl precursor with intent to unlawfully import it into the U.S.; manufacturing and distributing a fentanyl precursor with intent to unlawfully import it into the U.S.; and conspiracy to commit money laundering.

Jiangsu Bangdeya New Material Technology Company, a pharmaceutical company located in Jiangsu, China, was charged in an eight-count indictment, along with Jiantong Wang, 40, a Chinese national and alleged owner and operator of Bangdeya. The indictment alleges that Bangdeya advertises openly online as an export company for chemicals, including synthetic opioids protonitazene and metonitazene. The introduction of these synthetic opioids into the illicit drug market threatens to exacerbate the overdose problem in the United States. Drug traffickers typically mix protonitazene and metonitazene with other opioids, such as fentanyl, to create new and more powerful cocktails of dangerous opioids. Bengdeya has imported large quantities of these synthetic opioids into the U.S., including to a drug trafficker in the Southern District of Florida.

Bangdeya and Wang were charged with conspiracy to import protonitazene and metonitazene; conspiracy to distribute protonitazene and metonitazene; multiple counts of distribution of protonitazene; conspiracy to defraud the United States and make and use forged and counterfeited postage; and making and printing unauthorized postage meter stamps.

Hubei Guanlang Biotechnology Company, a chemical company located in Shijaizhuang, Hebei Province, China, was charged in a two-count indictment, along with Chinese national Wei Zhang, 28, who allegedly runs the day-to-day operations of the company and operates a cryptocurrency wallet that accepts payment for the company's sales of fentanyl precursors and opioid additives.

According to the indictment, Guanlang openly advertises online and sells an array of chemicals, including methamphetamine precursors like methylamine HCL, to customers in the United

States and Mexico. Methylamine HCL is an essential precursor chemical that Mexican cartels use to manufacture highly pure and potent methamphetamine. Currently, most of the methamphetamine supply in the United States is produced by drug trafficking cartels in Mexico.

Guanlang and Zhang are charged with conspiracy to manufacture and distribute a methamphetamine precursor and unlawfully import into the U.S. and conspiracy to unlawfully import a methamphetamine precursor into the U.S. with the intent to manufacture methamphetamine; and the manufacture and distribution of a methamphetamine precursor that was unlawfully imported into the United States.

The DEA Miami Field Division, HSI Miami, USPIS-Miami, IRS-CI Miami, and FBI Miami Field Office investigated these cases.

Assistant U.S. Attorney Monique Botero and Jon Juenger for the Southern District of Florida are prosecuting the cases. Assistant U.S. Attorney Michell Hyman for the Southern District of Florida is handling asset forfeiture.

The U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) provided assistance with the indictments brought in both districts.

The indictments are a result of Organized Crime Drug Enforcement Task Forces (OCDETF) investigations. The OCDETF mission is to identify, disrupt, and dismantle the highest-level criminal organizations that threaten the United States, using a prosecutor-led, intelligence-driven, multi-agency task force approach. OCDETF synchronizes and incentivizes prosecutors and agents to lead smart, creative investigations targeting the command-and-control networks of organized criminal groups and the illicit financiers that support them. Additional information about the OCDETF Program may be found at www.justice.gov/OCDETF.

Members of the South Florida High Intensity Drug Trafficking Area (HIDTA) Task Force carried out this case and prosecution. HIDTA was established in 1990. This program, which is made up of federal, state, and local law enforcement agencies, fosters intra-agency cooperation among law enforcement agencies in South Florida and involves them in developing a strategy to target the region's drug-related and violent crime threats to public safety, as with the opioid epidemic, fentanyl, and the cocaine threat to our nation. The South Florida HIDTA uses the funding provided by the Office of National Drug Control Policy, out of the Executive Office of the President of the United States, that sponsors a variety of law enforcement initiatives that target the region's illicit drug and violent crime threats to our community.

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

hebei_redacted_indictment_03oct2023_003_redacted.pdf mdfl_anhui_redacted_indictment_03oct2023.pdf

mdfl_henan_redacted_indictment_03oct2023.pdf

mdfl_lihe_redacted_indictment_03oct2023.pdf

mdfl_xiamen_redacted_indictment_03oct2023.pdf

sdfl_bangdeya_indictment_03oct2023.pdf

sdfl_hanhong_indictment_03oct2023.pdf

sdfl_hubei_guanlang_indictment_03oct2023.pdf

Updated October 4, 2023

Attachment

hebei_redacted_indictment_03oct2023_003_redacted.pdf [PDF, 1 MB]

Components

Office of the Attorney General | Drug Enforcement Administration (DEA) | Office of the Deputy Attorney General

Related Content

EXHIBIT 133

PRESS RELEASE

Justice Department Announces Charges Against China-Based Chemical Manufacturing Companies and Arrests of Executives in Fentanyl Manufacturing

Español

Friday, June 23, 2023

For Immediate Release

Office of Public Affairs

Four China-Based Precursor Chemical Manufacturing Companies and Eight Executives and Employees Charged in Global Supply Chain Disruption

The Justice Department today announced the arrest of two individuals and the unsealing of three indictments in the Southern and Eastern Districts of New York charging China-based companies and their employees with crimes related to fentanyl production, distribution, and sales resulting from precursor chemicals. These indictments represent the first prosecutions to charge China-based chemical manufacturing companies and nationals of the People's Republic of China (PRC) for trafficking fentanyl precursor chemicals into the United States. Specifically, the indictments allege the defendants knowingly manufactured, marketed, sold, and supplied precursor chemicals for fentanyl production in the United States in violation of federal law.

During these investigations, the Drug Enforcement Administration (DEA) seized more than 200 kilograms of fentanyl-related precursor chemicals, a quantity that could contain enough deadly doses to kill 25 million Americans.

Fentanyl is a highly addictive synthetic opioid that is 50 times more potent than heroin and 100 times more potent than morphine. Fentanyl and its analogues have devastated communities across the United States and are fueling the ongoing overdose epidemic, which the Centers for Disease Control and Prevention (CDC) recently estimated killed approximately 110,000 Americans in 2022. Fentanyl is now the leading cause of death for Americans ages 18 to 49. Fentanyl analogues, similar in chemical makeup and effect to fentanyl, can be even more potent and lethal than fentanyl.

“When I announced in April that the Justice Department had taken significant enforcement actions against the Sinaloa Cartel, I promised that the Justice Department would never forget the victims of the fentanyl epidemic,” said Attorney General Merrick B. Garland. “I also promised that we would never stop working to hold accountable those who bear responsibility for it. That includes not only going after the leaders of the Cartels, their drug and gun traffickers, their money launderers, security forces, and clandestine lab operators. It also includes stopping the Chinese chemical companies that are supplying the cartels with the building blocks they need to manufacture deadly fentanyl.”

“Today’s announcement is a down payment on our pledge to use every tool in the government’s arsenal, in every corner of the globe, to protect American communities,” said Deputy Attorney General Lisa O. Monaco. “The Justice Department will not rest or relent in investigating and prosecuting every link of the fentanyl supply chain, including the PRC companies and executives who produce and export vast quantities of the precursor chemicals the drug cartels need to peddle their poison. There can be no safe haven.”

“Today’s announcement is a considerable step forward in our unrelenting fight against fentanyl, targeting the threat where it starts,” said DEA Administrator Anne Milgram. “These companies and individuals are alleged to have knowingly supplied drug traffickers, in the United States and Mexico, with the ingredients and scientific know-how needed to make fentanyl – a drug that continues to devastate families and communities across the United States, killing Americans from all walks of life. Targeting entire criminal drug networks, from the source of supply to the last mile of distribution, is critical to saving American lives. DEA will not stop until this crisis ends.”

Southern District of New York

An indictment was unsealed in the Southern District of New York charging the China-based chemical company Hubei Amarvel Biotech Co. Ltd., aka AmarvelBio, (Amarvel Biotech), as well as its executives and employees Qingzhou Wang, 35, aka Bruce (Wang); Yiyi Chen, 31, aka Chiron (Chen); and Fnu Lnu, aka Er Yang and Anita (Yang), with fentanyl trafficking, precursor chemical importation, and money laundering offenses. Wang and Chen, both nationals of China, were expelled from Fiji on June 8, arrested by the DEA, and presented before U.S. Magistrate Judge Wes Reber Porter in Honolulu federal court on June 9. Wang and Chen were ordered detained in Honolulu and will appear in Manhattan federal court following their arrival in the Southern District of New York. Yang, also a national of China, is at large.

“The indictment unsealed today in the Southern District of New York is the next step in our fight against fentanyl,” said U.S. Attorney Damian Williams for the Southern District of New York. “Today, we target the very beginning of the fentanyl supply chain: the Chinese manufacturers of the raw chemicals used to make fentanyl and its analogues. We’ve charged a Chinese precursor chemical company. And that’s not all. We’ve charged and arrested some of the individuals who work at the company. That includes a corporate executive and a marketing manager. They’re in American handcuffs. And they’re going to face justice in an American courtroom.”

According to the allegations contained in the indictment and other court filings, Amarvel Biotech is a chemical manufacturer based in the city of Wuhan, in Hubei province, China, that has exported vast quantities of the precursor chemicals used to manufacture fentanyl and its analogues.

Amarvel Biotech has openly advertised online its shipment of fentanyl precursor chemicals to the United States and to Mexico, where drug cartels operate clandestine laboratories, synthesize finished fentanyl at scale, and distribute the deadly fentanyl into and throughout the United States. Through its website and a host of other storefront sites, Amarvel Biotech has targeted precursor chemical customers in Mexico, including by advertising fentanyl precursors as a “Mexico hot sale;” guaranteeing “100% stealth shipping” abroad; and posting to its websites documentation of Amarvel Biotech shipping chemicals to Culiacan, Mexico, the home city of the Sinaloa Cartel, one of the dominant drug trafficking organizations in the Western Hemisphere and which is largely responsible for the massive influx of fentanyl into the United States in recent years.

Amarvel Biotech has also endeavored to thwart law enforcement interdiction of its precursor chemical shipments. Amarvel Biotech has advertised, for example, the company’s ability to use deceptive packaging – such as packaging indicating the contents are dog food, nuts, or motor oil – to ensure “safe” delivery to the United States and Mexico.

Over the past eight months, during an undercover investigation by the DEA, Amarvel Biotech and its principal executive, Wang, its marketing manager, Chen, and its sales representative, Yang, shipped more than 200 kilograms from China to the United States of precursor chemicals used to make fentanyl and its analogues. Amarvel Biotech, Wang, Chen, and Yang shipped the precursors to the United States intending that the chemicals would be used to produce fentanyl and its analogues in New York, and they agreed to continue supplying multi-ton shipments of fentanyl precursors despite being told that Americans had died after consuming fentanyl made from the chemicals that the defendants had sold.

For example, on or about Nov. 17, 2022, a DEA confidential source (CS-1) wrote to Yang using an encrypted messaging application, “You know I making fentanyl,” and “Is not safe.” Yang replied, “I know.” On or about Dec. 1, 2022, Yang wrote to CS-1, promising that CS-1 would be “happy with our product” and noting that CS-1 would “be able to synthesize fentanyl.” In exchange for payment in cryptocurrency, Amarvel Biotech thereafter shipped from China to New York approximately 999.7 grams of the fentanyl precursor 1-boc-4-AP, approximately 1,002.6 grams of the fentanyl precursor 1-boc-4-piperidone, and approximately 893.6 grams of the methamphetamine precursor methylamine.

In or about March 2023, Wang and Chen met in person with an individual whom CS-1 represented was CS-1’s boss but was in fact another DEA confidential source (CS-2). During the meeting, Wang and Chen discussed Amarvel Biotech’s ability to supply ton-quantities of fentanyl precursors to New York for CS-1 and CS-2’s fentanyl manufacturing operation. After CS-2 stated that CS-2 wanted a different formula for manufacturing fentanyl and that several of CS-2’s American customers had purportedly died, Wang and Chen advised they had “a lot of customers in America and Mexico” who could provide technical assistance with fentanyl production.

After March 2023, Amarvel Biotech, Wang, Chen, and Yang agreed to sell CS-1 and CS-2 approximately 210 kilograms of fentanyl precursors in exchange for payment in cryptocurrency. During an April 10 video call with Wang and Chen, CS-2 stated that the approximately 210 kilograms of fentanyl precursors would be used to manufacture approximately 50 to 55 kilograms of fentanyl – an amount that, as noted above, could contain approximately 25 million deadly doses.

In or about May 2023, Amarvel Biotech, Wang, Chen, and Yang sent to the United States the shipment ordered by CS-1 and CS-2. On or about May 5, the DEA retrieved the precursor shipment from a warehouse near Los Angeles. Lab testing confirmed the presence of a precursor chemical for a fentanyl analogue. In an encrypted messaging group chat with CS-1, CS-2, Wang, and Chen, Yang explained that “New York, the United States, has been strict in checking the precursors of the ‘final product’ some time ago, so for the sake of safety, this time it is sent to California.”

In or about June 2023, Wang and Chen met again with CS-2. During the meeting, Wang and Chen discussed with CS-2 a multi-ton order of fentanyl precursor chemicals. Wang and Chen also discussed the need to take additional measures to protect themselves from detection and interdiction of their shipments “because recently American government . . . seized some Mexican group and they followed the routes to China,” where the U.S. Government found “our competitor in China” – an apparent reference to fentanyl-related charges filed in the Southern District of New York and announced in April 2023 against, among others, leadership of the Sinaloa Cartel and certain China-based precursor chemical company executives.

DEA's Special Operations Division Bilateral Investigations Unit investigated the case, with assistance from the DEA Bangkok Country Office, DEA Wellington Country Office, DEA Beijing Country Office, DEA Honolulu District Office, DEA New York Organized Crime Drug Enforcement Task Force (OCDETF), DEA Riverside District Office, DEA Special Testing Laboratory, the Justice Department's Office of International Affairs, the Royal Thai Police Narcotics Suppression Bureau, the Fiji Police Force Narcotic Bureau, the Fiji Office of the Director of Public Prosecutions, and the U.S. Attorney's Office for the District of Hawaii.

The Southern District of New York's Office's National Security and International Narcotics Unit is prosecuting the case.

Eastern District of New York

Two indictments were unsealed in the Eastern District of New York that detail criminal conspiracies by companies and employees based in China to manufacture and distribute fentanyl in the United States.

The first indictment charges Anhui Rencheng Technology Co. (Rencheng) Ltd.; Anhui Moker New Material Technology Co.; Shutong Wang; and Shifang Ruan, aka Eva, with conspiracy to manufacture and distribute fentanyl, manufacture of fentanyl, and other related offenses. In addition, the indictment charges those same defendants, as well as Xinyu Zhao, aka Sarah, and Yue Gao, aka Ellie, with illegally concealing their activities, including through customs fraud and introducing misbranded drugs into the U.S. marketplace. The indictment also charges Rencheng, Wang, and Ruan with conspiracy to distribute butonitazene, a controlled substance.

The second indictment charges Hefei GSK Trade Co. Ltd, aka Hebei Gesuke Trading Co. Ltd. and Hebei Sinaloa Trading Co. Ltd.; and Ruiqing Li with similar offenses, including conspiracy to manufacture and distribute fentanyl, manufacture of fentanyl, conspiracy to distribute a List I chemical, distribution of a List I chemical, customs fraud conspiracy, introducing misbranded drugs into interstate commerce, and distribution of metonitazene, a controlled substance.

"As alleged, the defendants knowingly distributed the chemical building blocks of fentanyl to the United States and Mexico, even providing advice on how they should be used to manufacture this dangerous drug which inflicts untold tragedy in New York City, Long Island, and across the nation," said U.S Attorney Breon Peace for the Eastern District of New York. "This prosecution shows that the companies and individuals who fuel our nation's deadly opioid epidemic – wherever they are located – will be found and prosecuted to the full extent of the law."

As alleged in the indictments, the defendant companies supplied precursor chemicals to the United States and Mexico, among other places, knowing they would be used to manufacture fentanyl. The defendant companies openly advertised their products all over the world, including to the United States and Mexico, on social media platforms. They also sent their chemical products to the United States and Mexico by boat and by air, using public and private international mail and package carriers. To prevent detection and interception of chemical products at the borders, the defendant companies employed deceptive and fraudulent practices, such as mislabeling packages, falsifying customs forms, and making false declarations at border crossings. The chemicals distributed by the defendants included all the materials necessary to manufacture fentanyl via the most common pathways.

The defendant companies attempted to obfuscate their distribution of fentanyl precursors by adding “masking” molecules, which slightly alter the chemical signature of the underlying precursor chemicals. By changing the chemical signature, an altered substance could evade testing protocols and relevant regulations by appearing to be a new substance. Such masking molecules are easily removed, thus enabling the purchaser to return the substance to its original form as a fentanyl precursor. The defendant companies not only produced and distributed masked precursors, but also provided instructions about how to remove the masking molecules upon receipt, thus helping their customers to more effectively obtain banned precursors and produce fentanyl. The defendants also gave instructions on how to improve fentanyl yield and advice on which chemicals to buy to replace banned precursor products.

Mexican drug trafficking organizations, including but not limited to the Sinaloa Cartel and the Jalisco New Generation Cartel (CJNG), have increasingly availed themselves of the fentanyl precursors and masked fentanyl precursors developed and distributed by the defendant companies and companies like them. The chemicals provided by the defendant companies have enabled such cartels and other drug trafficking organizations to produce fentanyl in clandestine laboratories in Mexico on a massive scale, for subsequent distribution in the United States and elsewhere. The materials and instructions provided by the defendant companies and companies like them have directly caused and contributed to the influx of deadly fentanyl into the United States.

DEA New York, DEA Mexico, DEA Diversion Control Division, DEA Special Testing and Research Laboratory, U.S. Customs and Border Protection New York Field Office, IRS Criminal Investigation New York Division, and U.S. Postal Inspection Service New York investigated the case. The New York City Police Department, the New York State Police, and the Justice Department’s Office of International Affairs provided assistance on the case.

The Eastern District of New York’s Office’s International Narcotics and Money Laundering Section is prosecuting the case.

This effort is part of an OCDETF operation. OCDETF identifies, disrupts, and dismantles the highest-level criminal organizations that threaten the United States using a prosecutor-led, intelligence-driven, multi-agency approach. Additional information about the OCDETF Program can be found at www.justice.gov/OCDETF

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

SDNY Indictment EDNY Indictment 2 EDNY Indictment 1

Updated June 23, 2023

Attachments

edny_unsealed_23-cr-263_anhi_moker_new_marketing_tech._co_et_al_indictment.pdf [PDF, 5 MB]

edny_unsealed_23-cr-264_hefei_gsk_trade_co_ltd._et_al_indictment.pdf [PDF, 5 MB]

sdny_unsealed_2023.06.22_amarvel_biotech_indictment_stamped_redacted.pdf [PDF, 11 MB]

Topics

OPIOIDS | DRUG TRAFFICKING

Components

Office of the Attorney General | Criminal - Office of International Affairs | Office of the Deputy Attorney General | USAO - New York, Eastern | USAO - New York, Southern

Press Release Number: 23-697

Related Content

PRESS RELEASE

Leaders of Dangerous Mexican Drug Cartel Responsible for Extreme Violence Charged with International Drug Trafficking and Firearms Offenses

EXHIBIT 134

RESERVED

EXHIBIT 135

中华人民共和国驻美利坚合众国大使馆

Embassy of the People's Republic of China in the United States of America

Home About the Embassy Consular Services Embassy Tour

Home > Ambassador's Activities

Ambassador Qin Gang Takes an Interview with Newsweek on the Fentanyl Issue

2022/09/30 10:35

On September 29, 2022, Chinese Ambassador to the US Qin Gang took an exclusive interview with *Newsweek* Senior Foreign Policy Writer Tom O'Connor on the Fentanyl issue. The full text of t published on Newsweek’s website (Link attached here) as follows:

Newsweek: What is China's position on the ongoing opioid crisis in the United States and what is your response to claims that China is, in some part, responsible?

Qin: In my past year as Chinese Ambassador to the U.S., I have had many discussions with Americans on opioid overdose. A friend told me that his daughter struggled with drug addiction for yea nephew even died of fentanyl overdose, something that really got me upset. As I understand the importance of this matter, I have paid personal efforts to bring about the dialogue between the U.S. China National Narcotics Control Commission.

China was a painful victim of opium in history. In the 19th century, Britain profited immensely from smuggling opium into China. When China decided to ban the material to save its population ar British launched the Opium War, which started a century of humiliation for China, marked by a slate of unequal treaties and waves of Western aggressions. The repercussions of history are felt eve searing pains in our national memory, China holds an understandably stronger antipathy for narcotics than any other country, as displayed in its zero-tolerance attitude towards all narcotic drugs, as control and tough punishment measures. Thanks to these efforts, narcotics are not endemic in China.

This part of history has made China naturally empathize with the United States and other countries in their fight against narcotics, hence our proactive cooperation with global partners under the fr United Nations conventions on counter-narcotics. This has been fully recognized and respected by the international community.

But to our regret, some Americans believe that China is the primary source of fentanyl in the United States. Some even fantasize that China is shipping fentanyl to the United States "as a form of p Opium Wars," and that "North America has been flooded with precursor chemicals from China, stifling international efforts," as I read from some opinion articles. These comments are false and m

Have the U.S. and China taken substantive measures toward curbing the flow of fentanyl precursors out of China to places such as Mexico and toward curbing the flow of fentanyl into States?

Qin: China and the United States have had decades of productive cooperation in combating narcotics. Though not confronting prevalent fentanyl overdoses or any death case ourselves — because control measures — China has done everything possible on our end, out of goodwill, to help the United States address this problem. On May 1, 2019, China permanently scheduled all fentanyl-rel first country in the world to do so, while the United States has stopped short of doing the same.

On the judicial front, three legal documents have been formulated to support the filing, prosecution, conviction and sentencing of offenses involving these substances. To reinforce fentanyl testing five sub-centers of the National Drug Laboratory have been established across the country.

On the operational level, fentanyl-involved enterprises and personnel have been clearly identified to get a full picture of the precursors and equipment they have and to prevent offenses from the sc and parcel industry has been mandated to verify the real names of both senders and recipients and check the parcel contents, and equipment must be used for security screening, instead of visual in particularly tight examinations for U.S.-bound parcels.

Key provinces and cities have also launched law enforcement operations to enhance inspection. Thanks to these solid efforts, not a single criminal case has been opened in China that involves the i trafficking and smuggling of fentanyl-related substances since their scheduling. In fact, according to the U.S. Customs and Border Protection, the United States has seized no such substances stemi since September 2019.

So just think how shocking it was for China, for all these efforts, to be sanctioned by the United States in May 2020, with its essential institutions on fentanyl profiling and control, such as the Insti Science of China's Ministry of Public Security and the National Narcotics Laboratory, added to America's "entity list," only to curb China's capability to fight narcotics.

The latest accusations have shifted to link China with Mexico, claiming that China is shipping precursor chemicals to the country, where drug cartels produce the lethal drug and smuggle it overlar fact is, however, that China has never received any report or data from Mexico on the use of Chinese precursor chemicals for drug production there, nor has the U.S. provided any evidence about tl chemicals into Mexico for fentanyl production.

Has the United States asked China to take stronger measures against fentanyl flows given the scope of the crisis here, and what further steps could be taken to combat this crisis?

Qin: The United States asks China to monitor the diversion of uncontrolled chemicals and equipment in international flows. But like oil, iron, water and many other substances, uncontrolled chem equipment have an array of legal usages. They are needed to ensure people's normal life. They can be produced, traded and used by any company without reporting to the government. To apply an be used to manufacture both cars and guns, and you cannot ban steel just because you ban firearms.

At the same time, China has faithfully honored obligations under the UN 1988 Convention. China's import/export licensing and international verification system for all listed chemicals has effectiv these chemicals from being diverted into illegal channels through international trade. But the "know your customer" practice that some in the U.S. have been asking about far exceeds the UN oblig According to international practices, it is up to the importer and importing country to ensure that imported goods are not used for illegal purposes, not the exporter. Taking one step back, given the international trade, it is simply impossible for the exporter to thoroughly verify its client located in a different territory. Mexico is a sovereign country; China has no right or capability to fulfill the its behalf.

Ancient Chinese philosopher Mencius advised that if people fail to reach their goal, they should first examine themselves for the reason of their failure instead of blaming others. Blaming China is way to address the fentanyl crisis. In fact, there are other workable ways, such as stepping up law enforcement operations, strengthening border control, enhancing oversight of fentanyl and its syn penalizing over-prescription and overdose of medications, and raising public awareness. Also, it is high time for the United States to permanently schedule the fentanyl-related substances.

The fentanyl crisis in the United States was not created by China. On the contrary, China is a well-intentioned and sincere partner ready for international cooperation and for global co-governance narcotics. We hope that the United States will act to stabilize and improve its relations with China and lift the sanctions on Chinese institutions to remove obstacles for such cooperation to proceed It is my wish to see America resolve its fentanyl crisis and American people walk out of the shadow of narcotic drugs as soon as possible.

相关新闻

Ambassador Qin Gang Takes an Interview with NPR Morning Edition (2022-01-28)

Embassy of the People's Republic of China in the United States of America
3505 International Place, N.W.
Washington, D.C. 20008 U.S.A.
Tel: +1-202-495-2266
Fax: +1-202-495-2138
E-mail: chinaembpress_us@mfa.gov.cn

Visa Office
Address: 2201 Wisconsin Avenue, N.W. Suite 110, Washington, D.C. 20007
Tel: +1 202-855-1555 (12:30-16:30, Monday to Friday, except for holidays)
Fax: +1 202-525-2056
Email for Passport and Travel Document Application: washington_hz@csm.mfa.gov
Email for Authentication Application: washington_gzrz@csm.mfa.gov.cn
Email for Visa Application: washington_visa@csm.mfa.gov.cn

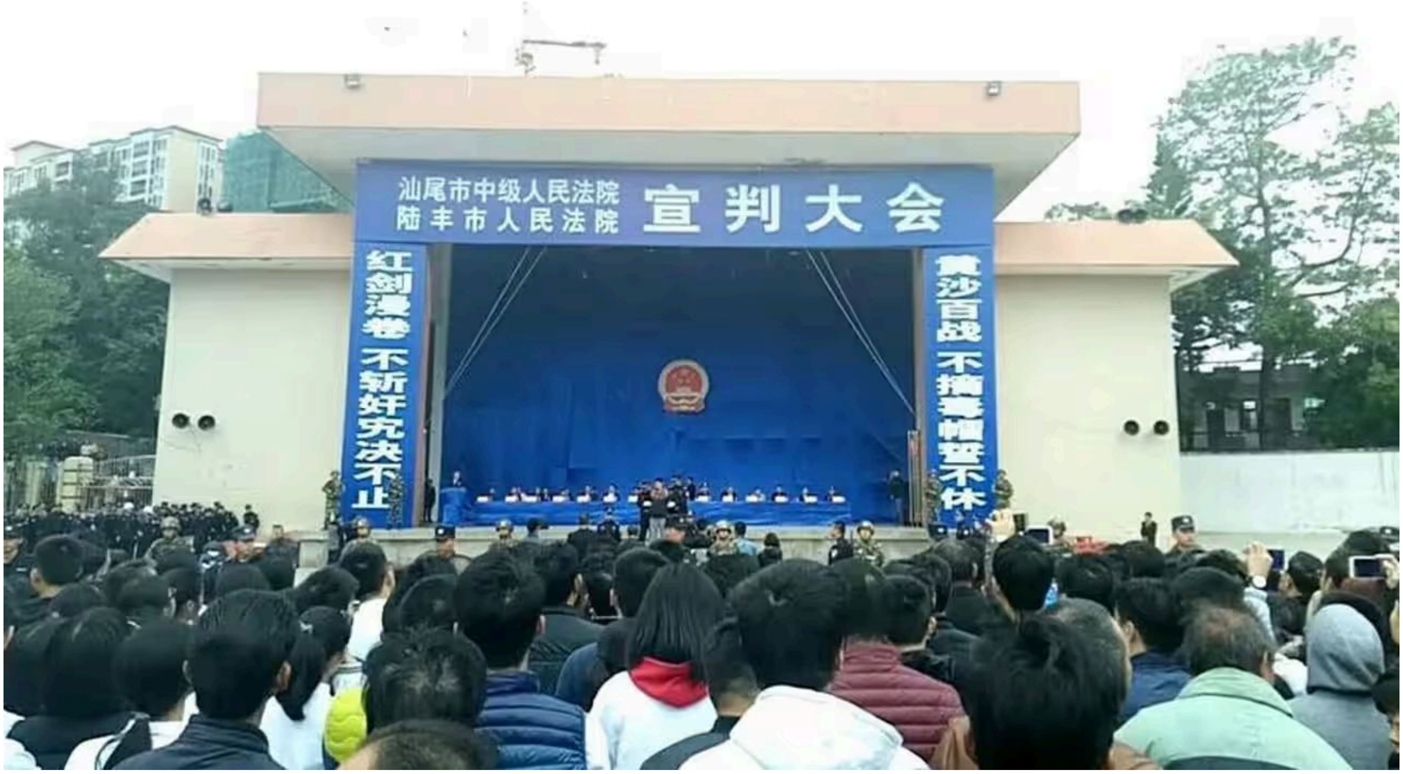
EXHIBIT 136

China

This article is more than **6 years old**

Thousands in China watch as 10 people sentenced to death in sport stadium

Residents in Guangdong invited to see group sentenced before they are taken away for summary execution in wake of drugs crackdown



The scene of the public trial in Lufeng Photograph: The Paper

Benjamin Haas *China correspondent*

Sun 17 Dec 2017 23.34 EST

A court in China has sentenced 10 people to death, mostly for drug-related crimes, in front of thousands of onlookers before taking them away for execution.

The 10 people were executed immediately after the sentencing in Lufeng in southern Guangdong province, just 160km (100 miles) from Hong Kong, according to state-run media.

Seven of the 10 executed were convicted of drug-related crimes, while others were found guilty of murder and robbery.

Four days before the event, local residents were invited to attend the sentencing in an official notice circulated on social media. The accused were brought to the stadium on the back of police trucks with their sirens blaring, each person flanked by four officers wearing sunglasses.

They were brought one by one to a small platform set up on what is usually a running track to have their sentences read, according to video of the trial. Thousands watched the spectacle, with some reports saying students in their school uniforms attended.

Beijing
China
Shanghai
Lufeng
Guangzhou
1000 km

People stood on their seats while others crowded onto the centre of the field, some with their mobile phones raised to record the event, others chatting or smoking.

China executes more people every year than the rest of the world combined, although the exact figure is not published and considered a state secret. Last year the country carried out about 2,000 death sentences, according to estimates by the Dui Hua Foundation, a human rights NGO based in the United States. China maintains the death penalty for a host of non-violent offences, such as drug trafficking and economic crimes.

However, public trials in China are rare. The country’s justice system notoriously favours prosecutors and Chinese courts have a 99.9% conviction rate. The trend to reintroduce open-air sentencing trials is reminiscent of the early days of the People's Republic, when capitalists and landowners were publicly denounced.

The most recent public sentencing and subsequent executions were not a first for Lufeng. Eight people were sentenced to death for drug crimes and summarily executed five months ago in a similar public trial, according to state media.

The town was the site of a large drug bust in 2014, when 3,000 police descended on Lufeng and arrested 182 people. Police confiscated three tonnes of crystal meth, and authorities at the time said the area was responsible for producing a third of China's meth.

Although open-air sentencing hearings are rare in China, they have been revived in recent years in some areas, most notably for cases of alleged terrorism in the country's far western region of Xinjiang.

A crowd of 7,000 watched as 55 suspects were sentenced in 2014, where at least one person was sentenced to death.

EXHIBIT 137

Follow the Money: The CCP's Business Model Fueling the Fentanyl Crisis

Written Testimony

of

John A. Cassara

U.S. House Committee on Financial Services
Subcommittee on National Security, Illicit Finance, and International Financial Institutions
March 23, 2023

Thank you, Chairman Luetkemeyer, Ranking Member Beatty, and members of the House Financial Services Subcommittee on National Security, Illicit Finance and International Financial Institutions for the opportunity to appear before you today.

I am a former U.S. intelligence officer and U.S. Treasury Special Agent. Most of my career has been involved with investigating and studying transnational crime and money laundering. I have written six books on the subjects. My most recent book is *China – Specified Unlawful Activities: CCP Inc., Transnational Crime and Money Laundering.* More information about my background can be found at www.JohnCassara.com

In the following testimony, my intention is to give an overview of the CCP's business model that is fueling the fentanyl crisis. My colleagues will provide specifics that correspond to their particular areas of expertise.

I begin the following testimony with a brief introduction as well as a definition of what I call CCP Inc. I then list 12 categories of transnational crime or specified unlawful activities (SUAs) for money laundering where CCP Inc. is the largest actor. I follow with a broad overview of CCP's involvement with the trafficking of fentanyl. The testimony continues with a description of Chinese-centric money laundering methodologies and enablers which are part of the CCP's business model that is fueling the fentanyl crisis. The methodologies include trade-based money laundering, black market exchanges, and fei-chien or flying money. I conclude with recommendations that emphasize law enforcement.

Introduction and Definition of CCP Inc.

Communist China is an ideological, military, economic, technical, commercial, intelligence, and diplomatic rival of the U.S. and the West. The People's Republic of China (PRC) has a growing exploitative presence in the developing world. While these threats are known, the Chinese Communist Party's (CCP's) involvement with transnational crime and money laundering is not.

Yes, there are plenty of news stories about China's theft of trade secrets and intellectual property. It is widely reported that China is the number one manufacturer of counterfeit goods. The average citizen might be somewhat aware that the African elephant and rhinoceros are endangered because of China's demand for ivory. Tropical forests are being destroyed to satisfy the PRC's demand for wood products. Some might have knowledge of China as the largest manufacturing source of illicit tobacco products. Others might have experienced being priced out of their local housing market due to suspicious Chinese capital flight pushing up property prices. This hearing is about the CCP's involvement in the trafficking of fentanyl. But all of these are single issue, focused stories. What the U.S. and the West have been ignoring is the massive totality of what I call CCP Inc's transnational crime and uniquely Chinese-centric money laundering methodologies and enablers that facilitate the criminality.

My most recent book is *China – Specified Unlawful Activities: CCP/Inc., Transnational Crime and Money Laundering* *(Amazon / Kindle Direct Publishing 2023).* I wrote the book at the end of my long anti-money laundering career because I am simply staggered by facts and observations that demonstrate China's criminal hegemony and how it launders illicit proceeds. Similar to North Korea, today's communist China is a corrupt party-state regime with a significant crime portfolio. Criminal activity has seemingly become part of the CCP's overall strategy to grow its power.

The CCP/Inc. subtitle of the book makes clear that I am talking about communist China's transnational crime and money laundering - not the Chinese people. In many ways, they are the biggest victims of the CCP regime.

Simply referring to China alone or the CCP by itself is ambiguous, unfair, and inaccurate. To be clear, what I am referring to in my book and in this testimony is the centralized autocracy of the CCP and its heretofore unexamined linkages with illicit crime, corruption, and money laundering. Although I will use the term 'China,' and 'Chinese' in this testimony, that is solely in reference to the Party's dominance of the PRC's governance apparatus, and should not be misconstrued to be a condemnation of Chinese culture or the Chinese people, who have no choice in what regime they live under. The "Inc." is a term that signifies how the Chinese state has leveraged its industrial, high tech, global trading, manufacturing might, and illicit connections to turn the country into an economic superpower. It is an apt metaphor for the "business model" that is the focus of this hearing. So, I will use "CCP Inc." as a general descriptor of the subject under discussion.

Specified Unlawful Activities

We cannot look at the fentanyl issue in a vacuum or as an isolated concern. CCP Inc. has a business model that fuels the fentanyl crisis and many other sectors of transnational crime. In my book, I examine perhaps the 12 most significant sectors of transnational crime. In 11 of the 12 categories, CCP/Inc. is the leading criminal actor. The 11 categories of crime are:

- Counterfeit goods
- Intellectual property theft and trade secrets
- Human trafficking, smuggling and forced labor
- Wildlife trafficking
- Illegal logging
- Illegal fishing
- Illicit tobacco
- Trade fraud

- Arms trafficking and WMD proliferation
- Organ harvesting
- Corruption

Each of the above categories of crime are also “specified unlawful activities” (SUAs) or predicate offenses to charge money laundering. Using SUAs and the estimates of illicit funds generated is not an ideal way of assessing money laundering. Measuring the scale of illicit funds derived from criminal or illegal activity is challenging. Likewise, estimating the magnitude of international money laundering in general is fraught with difficulties. By definition, money laundering is opaque and hidden. The Financial Action Task Force (FATF) states, “due to the illegal nature of the transactions, precise statistics are not available and it is therefore impossible to produce a definitive estimate of the amount of money that is globally laundered every year.” [i] With that caveat in mind, the International Monetary Fund (IMF) has estimated that money laundering comprises approximately two to five percent of the world’s gross domestic product (GDP) every year.[ii] Recognizing the IMF approximation as imperfect is probably the best we can do. Money laundering experts frequently use the IMF estimate when they need to discuss the magnitude of money laundering.

Using 2021 IMF data, global GDP totals approximately $94 trillion USD.[iii] So, in very round numbers, the total amount of money laundered worldwide annually is somewhere in the vicinity of roughly $2 to $5 trillion. Of course, the estimate could be far higher depending on what is included in the count. For example, I don’t believe the IMF estimate includes tax evasion, forms of trade fraud, or underground financial systems. Capital flight is another category which could be considered money laundering but is generally ignored.

Putting things in context, let’s use $4 trillion as a rough estimate of the annual magnitude of international money laundering. Using recognized estimates[iv] put forward by the Washington D.C.-based non-profit Global Financial Integrity (GFI) and other sources, a solid argument can be made that by examining China’s leading role in the above listed transnational SUAs, China is responsible for introducing and laundering approximately $2 trillion dollars of illicit proceeds into the world’s economy every year.[v] (Full disclosure: I am proud to sit on the Board of Directors of GFI). In other words, China is responsible for approximately one-half of the money laundered throughout the world every year as measured by SUAs.

The number is staggering. It bears repeating. As measured by the largest categories of SUAs for transnational crime, CCP Inc. and its associated actors are responsible for about half of the money laundered internationally each year. No other country even comes close – not even the United States.

My book, *China – Specified Unlawful Activities,* examines each of the above listed SUAs and quotes recognized sources estimating the amount of illicit proceeds generated. For example, roughly $600 billion is generated annually due to the theft of U.S. intellectual property alone. Many observers feel the theft has been the largest transfer of wealth in world history. According to a 2019 estimate by the European Union's Intellectual Property Office (EUIPO) and the Organization of Economic Development (OECD), global sales of counterfeit and pirated goods amount to an enormous 3.3% of world trade.[vi] Furthermore, according to the U.S. Chamber of Commerce, greater China (including Hong Kong) is the source of 86% of the world's counterfeit goods.[vii] The other SUAs listed above likewise generate enormous illicit proceeds.

Having worked in the U.S. government as well as at one time being actively involved in the Financial Action Task Force (FATF), I understand the political hesitation to officially make the charge that CCP Inc. could be considered an ongoing criminal enterprise and the largest money laundering actor in the world. However, the U.S. State Department does include China on its annual list of "primary countries of concern" for international money laundering.[viii] The National Defense Authorization Act (NDAA), enacted on January 1, 2021, calls for the U.S. Department of the Treasury to conduct a study on the extent and effect of illicit finance risk relating to the PRC. But, generally speaking, both the international community and the U.S. government is silent on the magnitude of China's involvement in transnational crime and money laundering.

We shouldn't be silent. CCP Inc. criminality is exposed. In my view, targeting CCP Inc. via coordinated and comprehensive law enforcement action is where they are most vulnerable.

Narcotics Trafficking and Fentanyl

The twelfth category of transnational crime and SUA for money laundering that I discuss in my book is CCP Inc.'s involvement in narcotics trafficking. As opposed to the other 11 SUAs, China probably does not lead the world in narcotics trafficking. However, it is a very significant player. CCP Inc. is the world's largest producer of synthetic drugs.

According to the China National Narcotics Control Commission (NNCC), China's economic prosperity has turned recreational drug use into more than an $80 billion annual domestic business.[ix] The estimate dates from approximately 2015. I have not been able to find more recent numbers. In all likelihood, the situation today is much worse. The NNCC also announced that over the last few years synthetic drugs—primarily methamphetamine and ketamine—have surpassed heroin and other opioids as the PRC's primary illicit drugs used in the PRC.[x] As this hearing makes clear, China excels in the manufacture of synthetic drugs and precursors.

However, we should be skeptical of all official statistics put forward by CCP Inc. Communist regimes have always used government statistics as a propaganda and disinformation tool. CCP Inc. wants and produces numbers that reflect well upon the state. Truth is relative.

The government of China does not, as a matter of government policy, encourage illicit drug production or distribution, nor is it officially involved in laundering the proceeds of the sale of illicit drugs. However, some senior government officials have been severely punished for taking bribes and laundering illicit profits related to drug trafficking. In fact, in recent years, China has initiated an aggressive campaign of cracking down on narcotics trafficking that affects *domestic* consumption. There is no doubt that China faces growing and significant drug consumption challenges.

China shares borders with drug source countries in both Southeast Asia and along Mekong's Golden Triangle and remains a major destination and transit country for heroin produced in these areas. Its numerous coastal cities with high-volume seaports and its vast network of major international airports make China an ideal destination and transit country for illicit drugs, as well as a major source of synthetic drugs, new psychoactive substances (NPS), and precursor chemicals used to produce illicit drugs. Unsurprisingly, the production of these drugs and the manufacturing of precursor chemicals is strongly linked to the country's developed and dynamic chemical and pharmaceutical industries. Domestic Chinese criminal organizations traffic illicit drugs within China. And in recent years Chinese authorities have noted the presence of international drug trafficking organizations originating from Africa and Mexico operating within the country through joint criminal ventures with Chinese syndicates.

Some may ask: "Since the U.S. is the largest consumer of drugs in the world, how can it be said that China is perhaps the most significant actor?" I am definitely not discounting the insatiable U.S. demand for illegal drugs and readily acknowledge that demand is the catalyst for international narcotics trafficking. For generations, the U.S. drug habit has been a national disgrace. But make no mistake, China is a leading global producer of NPS and related illicit drugs.

As imprecise as they are, let's examine some numbers. According to the GFI report referenced earlier, worldwide drug trafficking is estimated at about $426 billion to $652 billion per year. According to a 2014 study prepared for the U.S. Office of National Drug Control Policy (ONDCP), the U.S. illegal drug habit is approximately $100 billion a year.[xi] That number has also probably increased over the years, particularly due to opioids and other synthetic drugs flooding the U.S. market—more on that below. But in law enforcement and policy circles, $100 billion continues to be used as the most common estimate of illegal drug consumption in the United States. Per the above, according to China's own estimate, recreational drug use in that country is about $80 billion annual domestic business. The Chinese estimate was released in the same time frame as the U.S. study. Without a doubt, U.S. demand is greater than China's and the U.S. population is not as large. Per capita illegal drug consumption in the U.S. far exceeds that of China's. But it appears the illicit proceeds gap is not as pronounced as thought.

What differentiates China from the U.S. and other Western countries that are large consumers of illegal drugs is Chinese actors' direct and indirect involvement in facilitating international narcotics trafficking and laundering the proceeds. And in some instances, CCP Inc. tacitly supports aspects of the international drug trafficking by looking the other way as it does with the fentanyl trade.

In addition to domestic drug trafficking, Chinese organized crime groups increasingly traffic in international markets. Chinese triads were involved in narcotics trafficking long before it became a global phenomenon; the groups have grown as the trade has expanded. China is a major source of NPS and other synthetic drugs, including fentanyl and methamphetamine that are flooding into the U.S., Canada, and increasingly other Western countries.

Fentanyl is similar to morphine but is 50 to 100 times more powerful. Fentanyl is often reported as a single drug, but it is often mixed with other drugs such as heroin, cocaine, methamphetamine, and even processed into counterfeit pills under brand names such as Xanax, Percocet, Adderall, and Oxycontin. It takes very little fentanyl to produce a high, making it not only an addictive, cheaper option, but often times, a more deadly drug.

As testimony from other witnesses in this hearing make clear, deaths due to fentanyl in the United States have been rising. Each individual death and overdose is a tragedy. More than 100,000 Americans died from drug overdoses in 2021; approximately 80,000 died using opioids, including fentanyl and its derivatives found in other drugs.[xii] To put things in perspective, in the 20-year period from 1955 - 1975 approximately 58,000 Americans died in the Vietnam War. Or, using a more current statistic, from 2020 - 2021 about 53,000 Americans between the ages of 18 and 49 died of Covid-19. In the same age group, fentanyl has also claimed more lives than car accidents, suicide, gun violence, and breast cancer, among others.[xiii]

What accounts for the continuing rise in fentanyl deaths despite China's public claims that it has cracked down? According to the U.S. State Department, "following the PRC's implementation of class-wide controls on fentanyl in May 2019, fentanyl-related overdoses and seizures have continued to increase in the United States. Traffickers have adapted their strategies, resulting in the shipment of synthetic opioid precursor chemicals from the PRC to Mexico [and Canada] as well as greater fentanyl production and shipment from Mexico to the United States." [xiv]

This is where the "CCP business model fueling the fentanyl crisis" enters into the equation. Chinese companies make chemical compounds sold globally for legitimate purposes in medicine and industrial processes. Opioid vendors shield themselves behind these companies and layers of other interlinked companies sometimes in related fields such as biotechnology.

Illicit production and distribution are assisted by layer upon layer of traders, brokers, and freight forwarders that we see in other SUAs briefly discussed above. Moreover, Chinese trafficking organizations deliberately misuse this labyrinth to transport drugs, precursors, and contraband through shipping containers that are intentionally mislabeled; however even without the mislabeling it can be difficult for law enforcement and customs, “to track the origin of precursor chemicals or clandestinely-produced fentanyl because of the intricate network of freight forwarding companies commonly employed by criminal groups to conceal the origin of the product.” [xv]

In other words, despite periodic crackdowns by the authorities, some Chinese vendors created new distribution strategies by producing and selling the precursor chemicals to foreign clients so they could make fentanyl. Precursors were not banned. Boutique suppliers also tweaked their formulas taking advantage of regulatory and enforcement loopholes. New transport and mail routes were developed sending the banned substances into Mexico and sometimes other third countries. It’s a very effective and efficient business model. The U.S. is the final destination for most of the finished product.

Over the last few years, there have been increasing cases involving Mexican and Chinese criminal groups cooperating in the manufacture of fentanyl and fentanyl-laced products including candies that target children. They are subsequently smuggled into the U.S. The fentanyl that still enters the U.S. directly from China primarily arrives in small amounts via international mail, express mail, and parcel packages sometimes routed through third countries.

The reality is that in 2021 the DEA announced that U.S. customs and law enforcement seized enough doses of fentanyl to "kill every single American.”[xvi]

Also troubling is that Chinese actors aggressively use the internet and social media platforms to advertise, market, and ship their products. A report by the Senate Permanent Subcommittee on Investigations found that Chinese websites selling fentanyl and carfentanil rapidly and efficiently respond to online orders for the drugs and that they are confident in their ability to get drugs into the United States.[xvii] Carfentanil is 100 times more powerful than fentanyl and 10,000 times more potent than morphine.[xviii]

The Chinese criminals use the open worldwide web to market their illegal and dangerous products in English. They blatantly target Western consumers. In contrast, websites based in the United States only sell fentanyl on the dark web because of law enforcement vigilance in tracking the sale of these illegal drugs. It is difficult for host platforms outside the United States to be taken down. Sometimes crypto-currencies are used for payment. Investigators have found Chinese online merchants are in some cases willing to accept Western Union, PayPal and even credit cards for their product. CCP Inc. has also developed its own robust new payment methods that are web and mobile based.

For example, the Shanghai-based Zheng Drug Trafficking Organization (DTO), run by Fujing Zheng and his father Guanghua Zheng, sold synthetic narcotics including fentanyl and advertised their products on multi-language websites. For more than a decade, the Zhengs ran an agile and sophisticated operation. The Zheng labs manufactured more than 250 different drugs, which were shipped to at least 25 countries.[xix] They were able to quickly modify the formulas of these drugs—creating an analogue—in order to get around China's narcotics "controls."

C4ADS, a nonprofit organization specializing in data-driven analysis and evidence-based reporting on transnational security issues, reports that various Chinese drug groups operating online are also using password-encrypted websites. The Chinese DTOs facilitate private groups on social media and messaging apps and operate platforms or virtual marketplaces that connect illicit fentanyl consumers and sellers while avoiding detection by law enforcement.[xx]

Researchers at Terrorism, Transnational Crime, and Corruption Center (TraCCC) at George Mason University studied over 350 English language websites advertising fentanyl on open-web Chinese hosted web platforms. (Full disclosure: I am a proud Senior Fellow at TraCCC). The TraCCC team primarily used the Chinese search engine Baidu Research. The following findings are taken from a 2020 paper prepared by Dr. Louise Shelley, University professor and Omer L. and Nancy Hirst Endowed Chair at the Schar School of Policy and International Affairs at George Mason University and founder and executive director of TraCCC.[xxi]

TraCCC research identified the registration information of Chinese companies advertising on the websites. The researchers were also able to recognize the countries where fentanyl products were shipped and the key hubs for transport. The analysis was possible because 40% of the websites advertising illicit fentanyl were tied to officially registered Chinese companies. This TraCCC research is important because it contradicts frequently expressed statements that illegal fentanyl is produced primarily by rogue producers in China.

The researchers were also able to follow some of the layering involved. For example, many of the companies in advertisements are fronts, but the use of electronic identifiers and broader economic context facilitated identification to registered legitimate pharmaceutical companies. The TraCCC researchers were able to map and identify the global trade relationships of these chemical and pharmaceutical companies.

One of the prime networks identified through the TraCCC research was the Yuancheng Group, a Chinese chemical company based in Wuhan, China. The Yuancheng Group is comprised of at least 34 companies in China and Hong Kong. Studying identifiers from these companies reveals that the companies have posted advertisements for fentanyl and have registered at least 112 websites, including some devoted to the advertisement and sale of steroids. Further records indicate the Yuancheng Group has shipped to 43 countries across North America, South America, Europe, Africa, Asia, and Australia.

The fact that CCP Inc. allows hundreds of websites advertising fentanyl and its precursors to remain online is deeply troubling. It is important to remember that the PRC is a command state. China controls what its citizens can, or cannot, access, on the internet. It routinely blocks, censors, and takes down sites that do not meet its approval. If the CCP was to direct its robust censorship apparatus that is very effective in thwarting websites it deems a threat to its regime, it could easily do the same with companies' websites advertising fentanyl and other dangerous and illegal drugs. But the authorities do not act. Rather, they allow it flourish. Why?

While some observers blame Chinese organized crime groups for the international trafficking of narcotics, CCP Inc.'s refusal to eradicate websites (which, once again, they can do easily enough) that advertise such poisonous and deadly precursor chemicals and illicit drugs for foreign sales is a major factor in demonstrating official complicity.

There is another troubling indicator. As Channing Mavrellis of GFI writes, "while much of China's response to drug abuse, production, and trafficking could be considered draconian—

such as proactive identification and registration of drug users, compulsory detoxification centers and labor camps for addicts, and the death penalty for traffickers—the punishment for mislabeling shipments of precursor chemicals, the most common diversion tactic, is significantly lighter, typically involving civil penalties and small fines. It is interesting to note the disparity in punishment between those crimes that directly affect the state internally and those that have external impact (i.e., on other countries)."[xxii]

Further exploration of Chinese involvement in other transnational SUAs for money laundering also shows that CCP Inc. has different internal and external standards and enforcement. This necessitates an important question. Is CCP Inc. using or permitting narcotics trafficking to the West as a form of asymmetric warfare to advance its long-term strategic goals? As noted, China's fentanyl trafficking is responsible for the annual death totals of tens of thousands of lives in the United States, and globally. Related products and precursors sourced from China are also responsible for countless ruined lives, families, and communities. Chinese-produced fentanyl and associated products cost the U.S. hundreds of billions of dollars annually in lost productivity, health care, and criminal justice costs. If China perceives itself to be in a silent or cold war with the U.S. these are all very effective and efficient outcomes.

Drug use has long been considered a form of asymmetric warfare. Others have advanced the premise that CCP Inc. is flooding the U.S. and the West with opioids as payback for the Opium Wars during the mid-19th century.

Of course, the ultimate responsibility lies with the user. And without question the U.S. has failed both in both drug interdiction and treatment, not only with fentanyl but also with heroin, opium, and other domestic illegal and legal drugs such as OxyContin. Our unsecured border makes the situation even worse. But from a law enforcement perspective, we must examine the source. And according to a 2020 report by the DEA, "China remains the primary source of fentanyl and fentanyl-related substances trafficked through international mail and express consignment operations environment, as well as the main source for all fentanyl-related substances trafficked into the United States."[xxiii] Moreover, increasing Mexican-Chinese transnational criminal organizations (TCOs) collaboration on crime and money laundering are significant national security threats to the U.S. homeland.

Money Laundering Methodologies and Enablers

In my book, *China – Specified Unlawful Activities,* I discuss a number of money laundering methodologies and enablers with "Chinese characteristics." (The term Chinese characteristics is used by the CCP itself). Many examples are given. Collectively, they are intertwined in the CCP's business model. Some of the methodologies I explore include Chinese underground banking or CUBS, capital flight, gambling, real estate, and the use of offshores and secrecy jurisdictions. Corruption can be both methodology and also a SUA. I also call corruption "the great enabler" for money laundering. Bribery is part of the CCP Inc. business model and gameplan. CCP Inc. has taken their domestic corruption and exported it overseas. The modus operandi abroad is using corruption and "corrosive capital" as instruments of foreign policy. This is further augmented by "elite capture" and sophisticated influence operations. This occurs in the United States and against American interests abroad. Other enablers I discuss in my book include Chinese organized crime, espionage, social monitoring, the promotion of Chinese control of Free Trade Zones (FTZs), lack of Chinese cooperation with international law enforcement, and poor Chinese money laundering compliance.

Three methodologies that are part of the CCP business model and directly impact the trafficking of fentanyl are trade-based money laundering, black- market exchanges, and fei-chien or flying money. I will provide an explanation of each.

Trade-based money laundering (TBML)

Perhaps the most extensive or widespread form of Chinese (and global) money laundering comes from "trade-mis-invoicing" or trade fraud. Trade fraud or customs fraud is a SUA for money laundering. Depending on its form, it can also be a money laundering methodology. In fact, I believe it is the largest and most widespread methodology for both China and the world at large. It is also the least understood, recognized, and enforced.

For a detailed examination of TBML, please see my book *Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement,* Wiley, 2016

Most forms of trade mis-invoicing revolve around invoice fraud and manipulation. Generally speaking, invoice fraud means the contents, description, and/or the value of goods is deliberately misrepresented. Sometimes this is done to facilitate simple customs fraud, i.e., minimize the payment of taxes and duties, avoid currency controls, or move capital or value offshore. International trade via invoice manipulation is also a very common means used by criminals and criminal organizations to illegally transfer value across international borders.

TBML is defined by the FATF as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins."[xxiv] The key word in the definition is *value.* Instead of following the money trail via cash or the electronic bits and bytes of a bank-to-bank wire transfer, with TBML we examine the shipments of commodities and trade goods. Their sale and transfer—real and fictitious—very effectively launders money, evades taxes and tariffs, and transfers value between cooperating parties in the transaction(s).

TBML is very broad. It includes customs fraud, tax evasion, export incentive fraud, value-added tax (VAT) fraud, capital flight or the transfer of wealth offshore, evading capital controls, barter trade, underground financial systems such as hawala and fei-chien (the Chinese "flying money" system), black market exchange systems, and even forms of commercial TBML such as trade diversion, transfer pricing, and abusive trade mis-invoicing.

For money launderers and terrorist financiers, transferring value via trade goods is particularly attractive because it generally does not trigger financial transparency reporting requirements or the filing of financial intelligence or, as it is commonly called in the U.S., "Bank Secrecy Act data." Financial intelligence promotes a degree of financial transparency and is our primary AML/CFT countermeasure.

The most common forms of trade mis-invoicing are:

- Over and under invoice pricing
- Multiple invoicing for the same goods
- Falsely described goods
- Mis-representation of the quantity being shipped

- Mis-representation of voyage to disguise origin from sanctioned countries
- Mis-representation of shipment origin and voyage to evade customs duties

Most of the above are self-explanatory. But I do want to briefly explain how over and under invoicing is used to transfer value and launder money, because I will refer to this below when I discuss the Chinese underground “flying money” system.

The key element of this technique is the misrepresentation of trade goods to transfer value between the importer and exporter or settle debts/balance accounts between the trading parties. When an importer and exporter are working together, they can easily manipulate the invoice to reflect a price that does not adhere to true market value. The shipment (real or fictitious) of goods and the accompanying documentation provide cover for the transfer of money. Invoice fraud is generally considered customs fraud. And customs fraud is the primary predicate offense or specified unlawful activity in TBML cases.

What are the most common invoice scams? First, by under-invoicing goods below their fair market price, an exporter is able to transfer value to an importer while avoiding the scrutiny associated with more direct forms of money transfer. The value the importer receives when selling (directly or indirectly) the goods on the open market is considerably greater than the amount he or she paid the exporter.

For example, Company A located in China ships one million widgets worth $2 each to Company B based in Mexico. On the invoice, however, Company A lists the widgets at a price of only $1 each, and the Mexican importer pays the Chinese exporter only $1 million for them. Thus, extra value has been transferred to Mexico, where the importer can sell (directly or indirectly) the widgets on the open market for a total of $2 million. The Mexican company then has several options: it can keep the profits; transfer some of them to a bank account outside the country where the proceeds can be further laundered via layering and integration; share the proceeds with the Chinese exporter (depending on the nature of their relationship); or even transfer them to a criminal organization that may be the controlling interest behind the business transactions.

To transfer value in the opposite direction, an exporter can over-invoice goods above their fair market price. In this manner, the exporter receives value from the importer because the latter's payment is higher than the goods' actual value on the open market.

Here is a simple way of looking at things:

To move money/value out:

- Import goods at overvalued prices or export goods at undervalued prices

To move money/value in:

- Import goods at undervalued prices or export goods at over-valued prices

Unfortunately, the magnitude of TBML has never been systematically examined by the FATF, international financial institutions (IFIs) —e.g., IMF or World Bank—or the U.S. government. Trade-based value transfer is also not closely examined by intelligence, law enforcement, and customs services. But some academics and non-profits have done very useful work examining TBML and estimating the extent of the challenge.

In the United States, Dr. John Zdanowicz, an early pioneer in the study of TBML, conducted research that identified glaring anomalies in U.S. trade data. For example, he found plastic buckets from the Czech Republic imported with the declared price of $972 per bucket! Toilet tissue from China imported at the price of over $4,000 per kilogram. Bulldozers shipped to Colombia at $1.74 each! Why are non-industrial diamonds being exported to France for $2.32 per carat but imported from South Africa for $929,390.82 per carat? Dr. Zdanowicz compares the declared value of the trade good or commodity against true market value. By examining 2021 U.S. trade data, Dr. Zdanowicz found that approximately $784 billion was moved into the U.S. via over-valued exports and under-valued imports. China was the trading partner for about $85 billion of the total. Approximately $640 billion was moved out of the U.S. via undervalued exports and over-valued imports. Approximately $70 billion was moved out to China via suspect trade. He then compared those numbers to the overall value of U.S. imports and exports. He found (depending on import or export) approximately 14 to 17% of U.S. trade could well be tainted by customs fraud and perhaps TBML.[xxv]

(The above has serious fiscal ramifications. Examining 2021 U.S. trade anomalies, per the above, Dr. Zdanowicz estimates that the U.S. Treasury lost about $640 billion of taxable profits due to trade-based tax evasion and TBML.[xxvi] The same type of trade fraud revenue loss occurs in every country.)

China is the world's largest trading nation. In 2019, the total value of Chinese exports worldwide was $ 2.5 trillion. The total value of Chinese imports was a bit over $2 trillion.[xxvii] In 2021, according to CCP Inc.'s own numbers, even factoring in the worldwide pandemic, China's foreign trade volume hit a record high of $6.05 trillion.[xxviii] So, if we use a very conservative estimate that only ten percent of trade is suspect, mispriced, or related to forms of trade fraud, that could mean that suspect and possibly illicit Chinese trade is approximately $600 billion a year and could very easily be much higher than that!

By its volume and sheer dominance of international trade, Chinese actors are assuredly involved with a massive amount of trade fraud. In addition, trade also masks money laundering methodologies and value transfer schemes that are instrumental in the trafficking of fentanyl and other forms of contraband.

Black Market Exchanges

Illicit proceeds are the catalyst driving the tragedies surrounding the unsecured U.S. border. Yet few realize the quiet ascendency of Chinese money launderers. They are displacing Colombians and Mexicans.

Although various schemes are used to launder illicit proceeds from the sales of narcotics in the United States, for years the preferred methodology has been the Black-Market Peso Exchange (BMPE). It is arguably the largest and most effective money laundering methodology in the Western Hemisphere. The evolution of the BMPE is an excellent case study of how international criminal networks adapt and how CCP Inc. has incorporated this form of TBML into its business model.

Ironically, the BMPE was not created to launder drug money. In 1967, Colombia enacted regulations that strictly prohibited citizens' access to foreign exchange. Colombian merchants who wanted to import U.S. trade goods – for example, John Deer tractors, Bell helicopters or Marlboro cigarettes – through legitimate banking channels had to pay stiff surcharges above the official exchange rate. To avoid these steep add-on costs, importers often turned to Colombian underground peso brokers, from whom they could buy U.S. dollars on the black market for less than the official exchange rate to finance their legitimate trade.

By the 1980s, the underground peso situation was taking on a new dimension. As U.S. cities found themselves awash in Colombian cocaine, narco-traffickers and cartels were faced with a logistical problem. They had to devise ways to launder and repatriate approximately 20 million pounds of U.S. currency they annually accumulated in North America.

The criminal organizations found a partial solution in the first law of economics. Supply met demand in the form of the BMPE.

Consider a Colombian drug cartel that has sold $3 million of cocaine in the United States. A representative of the cartel sells these accumulated dollars to a Colombian peso broker at a discount. The cartel is now out of the picture, having successfully sold its drug dollars in the United States and, in return, obtains pesos back in Colombia.

To complete the BMPE cycle, the peso broker must take two more steps. First, he directs his representatives in the United States to "place" the purchased drug dollars into U.S. financial institutions, using a variety of techniques designed to avoid arousing suspicion or triggering financial intelligence reporting.

Second, he takes orders from Colombian businesses for U.S. trade goods, arranging for their purchase using the laundered drug money he owns in the United States. Some businesses should know better. Via "willful blindness," they don't ask the questions they should. The broker has laundered the $3 million in drug money he purchased from the drug cartel.

This money laundering methodology was so successful that the Colombian BMPE became the premier money laundering methodology in the Western Hemisphere in the 1980s, 1990s, and the first decade of the 2000s.

In 2014 there was a turning point. A large law enforcement investigation called Operation Fashion Police showed how Los Angeles–based garment dealers took U.S. drug money and exported their product not to Colombia but to Mexico.

In addition, some of the clothing exporters mixed customs fraud into the BMPE conspiracy. "Made in China" labels were removed from thousands of imported garments. The fraud saved the co-conspirators from paying taxes on the "Made in China" imports because on paper they appeared to be "Made in the USA," and exempt from customs duties under the North American Free Trade Act (NAFTA).

Once again, with the Mexican BMPE, the proceeds from narcotics trafficking stay on the U.S. side of the border. The same is now true with the cartels' U.S. involvement in human trafficking, trade in opioids, kidnapping, stolen cars, and other illegal activities. In return, trade goods are shipped to Mexico.

About five to ten years ago, the BMPE shifted focus once again. Now, investigators are finding that Chinese manufactured goods are becoming favored instruments in the BMPE and that similar BMPE financial systems are found around the world.

In 2000 bilateral trade between China and Mexico was about 1 billion dollars. By 2021, trade between China and Mexico topped 100 billion dollars. Mexican authorities have said that the surge has allowed drug cartels and their money launderers to piggyback on this burgeoning trade relationship.[xxix] Some of the piggybacking includes TBML, value transfer, and the BMPE.

Fronts for Mexican drug trafficking organizations use illicit proceeds to buy container loads of cheaply made Chinese goods. Using the TBML technique of over-invoicing discussed above, low-quality Chinese manufactured items are made to appear on paper as being worth significantly more. Payment for the goods is sent out of the country. That's the wash.

We see the result of this in our cities and towns but we don't recognize or understand what is going on. Massive quantities of cheaply manufactured Chinese goods including counterfeits are found in black markets as well as souks, bazaars, marketplaces, dollar stores, Mom and Pop shops, swap meets, street kiosks, "China shops," and warehouse stores around the world.

In some cases, brokers under-invoice Chinese products. A variety of goods including electronics, garments, small household appliances, are purchased, imported, and sold in many "China shops" and on the black market in countries around the world. Via this form of value transfer, funds are used to buy contraband including drugs, ivory, endangered and illegal wildlife and their parts, and heavily regulated flora and food items that are later shipped to China. This is why I noted earlier in my testimony that the CCP business model and its involvement with various SUAs are intertwined and cannot be examined in isolation.

The BMPE has evolved further still as Mexican and other foreign national buyers and brokers travel directly to China to place orders for the goods or they avail themselves of e-commerce brokers to purchase consumer products that are made in China. Generally speaking, Chinese merchants also practice willful blindness. They do not conduct customer due diligence and do not care if they are being paid with illicit proceeds.

Chinese organized crime has entered the mix. Chinese actors working with the Mexican cartels have pioneered the growing use of **"mirror accounts" or "mirror swaps"** to launder the proceeds of crime.

With "swaps," Chinese brokers often working with Chinese organized crime groups and the cartels identify Chinese/American cash intensive businesses that are willing to cooperate.

How do the swaps work? The Chinese/American businessperson receives the drug cash from the Chinese broker working with the cartels. The business later "places" the proceeds of crime into its revenue flow and represents the drug cash as legitimate proceeds from the business. Or, the cash is used to assist other Chinese that want to circumvent Chinese capital flight restrictions and, for example, purchase U.S. property, housing or other high-ticket goods.

Meanwhile, these complicit businesses are asked to transfer a designated amount of money through Chinese phone apps to accounts based in China. Using a currency converter app on a smartphone, the participants agree on the exchange rate between the U.S. dollar and the Chinese yuan. Once the money is offshore in China, the value can be further re-routed to Mexico or elsewhere per the instructions of the cartels.

It's called a "swap" because the participating businessperson takes possession of the drug cash, while simultaneously transferring the equivalent in Chinese yuan from his/her account in

China to the account provided by the broker. Of course, the Chinese/American businessperson also receives a commission.

During the original Colombian BMPE, the average commission for the black-market peso broker was about 15%. The Chinese are doing it for 1 to 2% on average.[xxx] And the speed is almost instantaneous. For the traffickers, the big plus is that the Chinese organized crime groups involved absorb all the risk. The cartels know they will get paid.

Communications are generally accomplished via Chinese apps such as WeChat. Law enforcement is reportedly challenged to monitor the communications and monetary transactions. Yet the same transactions are easily monitored by the platforms involved as well as Chinese intelligence entities. Mirror swaps also avoid U.S. financial intelligence reporting requirements – our primary anti-money laundering countermeasure.

I discuss Chinese espionage and Chinese organized crime in my book *China – Specified Unlawful Activities.* I believe China's 2017 National Intelligence Law is pertinent to "swaps" and the use of Chinese/American businesses. The Law requires Chinese organizations and citizens, wherever they are in the world, to support, assist, and cooperate with PRC intelligence services.

Fei-Chien or Flying Money

Chinese underground finance or alternative remittance systems are primarily used to remit wages from the Chinese diaspora back to the homeland. Authorities have no wish to interfere with hard-working immigrants sending money "back to the home country" to help support extended family in China. Most of these money transfers are perfectly benign. Unfortunately, these low-cost and highly efficient financial systems are also abused by criminals to move, transfer, and launder illicit proceeds. Increasingly, the transfers are multi-directional. The system is very attractive to criminals because by its very nature it is opaque. Generally speaking, U.S. law enforcement does not understand or recognize Chinese underground finance. There are few trails for authorities to follow. Chinese underground finance or alternative remittance systems also avoid government scrutiny, taxes, and traditional countermeasures such as the filing of financial intelligence reports. Chinese flying money is used primarily in the layering stage of money laundering.

It is believed that *fei-chien*, sometimes known as "flying money," was started during the T'ang Dynasty (618 to 907 AD).[xxxi] At the time, there was a growing commodity trade within China. Some historians believe it was the rice trade and others the tea trade that were the catalysts for this new financial system. Ironically, as opposed to modern day practices, the transfer schemes were not invented as underground methods of payment transfers, but were rather systems devised by the government to facilitate taxation. Merchants sold their goods and then brought their revenues to provincial "memorial offering courts." The government collected taxes. In turn, the merchants were issued certificates for the remaining value of the commodity sales. When the merchants returned to their home provinces, they would present the certificates to the provincial government for payment. Interestingly, some scholars believe these certificates were the forerunner of the paper banknotes that appeared during the Song dynasty (960 – 1279 AD). The fei-chien system became an efficient way of payment. Completing transactions in this way spared both the merchants and government the risk of transporting large sums of money and ensured all parties to the transaction would get paid.

Over the centuries, the *fei-chien* system continued to evolve. Chinese workers increasingly began to migrate to remote provinces, and then overseas. The Silk Road trade between China, Central Asia, and Europe created a demand for brokers at the ends of the major trade routes who were prepared to settle each other's debts. Negating the need for physical currency or gold to travel was an important security consideration. In addition, families back home needed financial support to maintain their livelihoods. Expatriate Chinese businesses began to develop side businesses of remitting money back to China. The international Chinese diaspora spread this indigenous financial system further still. Today, modern Chinese businesses as well as "Chinatowns" and "China shops" and Chinese organized criminal groups are found around the world. So too is Chinese flying money. Chinese underground banks are a new iteration of an age-old financial system, re-purposing informal value transfer techniques for today's world.

Strong Chinese family bonds are incorporated into "*guanxi,"* which is an overarching social system of rules that govern relationships and social behavior. *Guanxi* is the guarantor of both secrecy and the integrity of the parties to the transaction. Those who violate its prescriptions find themselves as social outcasts, essentially shunned in all circles. *Guanxi* is an integral component of *fei-chien.* In other words, similar to hawala and other better known indigenous informal value transfer systems, an essential element is trust. The trust is based on family, clan, social mores, friendship, and culture. As a result, it is very difficult for outsiders to penetrate the *fei-chien* underground financial networks.

Let's use a simple scenario to illustrate how Chinese flying money works: Wang in Guangdong province wants to send 200,000 Chinese renminbi (RMB) to his brother in New York City. Wang wants to protect his hard-earned money by investing in dollars and the United States. He uses a series of underground flying money transfers to avoid the PRC's tight capital restrictions. Wang gives the Guangdong "flying money" broker the RMB and in turn receives a code number. He trusts the broker as they have a familial relationship. The "flying money" broker in Guangdong directs his counterpart in New York (perhaps a member of the same family) to pay the equivalent in U.S. dollars (approximately $28,000) upon presentation of the code. The code could be transferred in a telephone call or a message contained in an e-mail or perhaps the Chinese messaging system, WeChat. Not many years ago, a playing card or a portion of a currency note with a specific chop, marking, wax seal, or other physical sign would be presented to the broker as a sign of authentication. If it is a recurring transaction, codes aren't necessary. Upon receipt, the New York "flying money" broker pays Wang's brother in New York City. The RMB did not physically leave China. The dollars were already in the U.S. Similar to hawala, the system can be described as "money transfer without money movement." [xxxii] Wang's brother safeguards the $28,000 and following transfers. His brother's capital is now in the United States and authorities are none the wiser.

Money and value are also sent back to China. Like all immigrant groups, Chinese send money back home to help support their families. The same fei-chein brokers are involved. Even though "flying money" largely operates on trust and community ties, the brokers are in business to make money. Occasionally they have to settle accounts. Transactions are multi-directional. Using the above example, the New York broker might be running a deficit or a surplus with his counterpart in Guangdong. Various methods are used to settle accounts including banks, cash couriers, online payment services, mirror accounts, and trade-based value transfer.

Surplus credits could also be used by a client unrelated to the original transaction(s). For example, credits could be used for the purchase of foreign real estate. For a fee, the client that wants money outside China pays RMB in China to a flying money broker and receives credit in the desired foreign location in local currency.

One of the most popular methods of getting RMB or yuan out of China involves finding a willing foreign contact who would like to set up a private exchange for Chinese RMB. Flying money networks are sometimes used but so are informal personal networks and business associates. For instance, the overseas person puts their dollars into an account in Hong Kong or Singapore belonging to the Chinese individual. The Chinese individual in China puts the Chinese RMB in an account in Beijing that is connected with the overseas investor who wants the money in China.

What is often overlooked in hawala, flying money, and other informal underground financial systems is that historically and culturally <u>trade is most often used in the settling of accounts between brokers.</u> Recall the discussion of trade fraud, value transfer, and TBML. Of particular relevance is the section on over-and-under invoicing. Trade-based value transfer has been used as an efficient and effective settlement system for thousands of years. Most "flying money" brokers are directly involved or associated with trading companies - especially now that China is a global economic and trade power.

How do the "flying money" brokers profit? Although commissions are paid to the brokers at both ends of the transaction, the fees are less than banks or traditional money remitters such as Western Union charge. In comparison to large brick-and-mortar banks and money transfer chains, expenses are small. Often the brokers use legitimate businesses as fronts. The businesses include restaurants, "China shops," and trading companies. Of course, in the underground remittance segment of their business they skirt regulations and taxes. In the United States, the flying money brokers are technically classified as a money service business (MSBs) for the purposes of registration, licensing, and reporting financial intelligence. They must register with FinCEN and be licensed in 48 of the 50 states. They are also supposed to file financial intelligence. They do not comply.

After the September 11 attacks in the United States, law enforcement and intelligence agencies began to focus on hawala and its links with terror finance. As a result, hawala has received much worldwide attention and notoriety. There have been a number of successful investigations into how hawala is misused by criminals and terrorists. Because of the worldwide Chinese diaspora, I believe the magnitude of "flying money" is larger than hawala. Together, underground remittance systems could be valued at over $1 trillion per year.[xxxiii] The important point to note is that both of these culturally-based systems are efficient and historically and culturally rely on trade-based value transfer.

I have the utmost admiration and respect for these underground financial systems. They are fast, efficient, reliable, functional, and provide much needed low-cost financial and remittance services for millions of people around the world. The primary drawback, of course, is that criminals take advantage of the systems' opaqueness and anonymity. Flying money is used to launder the proceeds of crime. These "underground," "parallel," or "alternative remittance systems" are very difficult for law enforcement and intelligence services to monitor**.** Most law enforcement at the federal, state, and local levels are not even aware of the existence of flying money**.** There are very few investigations.

Recommendations

CCP Inc.'s criminal activities are increasingly exposed. I believe CCP Inc. is vulnerable via a systematic and coordinated law enforcement approach. The following suggestions are offered in no particular order or priority. Most of them focus on law enforcement and related topics. I have made recommendations for combatting individual SUAs and money laundering methodologies elsewhere.[xxxiv]

Investigate, Prosecute, and Convict Criminals

It all comes down to enforcement.

There are a large number of academic, think-tank, non-profit, and journalistic exposés of CCP Inc. criminality. As noted previously, they generally examine one case or perhaps study one SUA but do not examine the totality of CCP Inc. transnational crime and the corresponding CCP

Inc.-centric money laundering methodologies. Nevertheless, these studies educate diverse communities around the world and are helpful. Unfortunately, scholarship does not solve the problem.

With a few exceptions, we have the laws, rules, and regulations that are necessary to investigate, prosecute, and convict CCP Inc. actors involved with transnational crime and money laundering. U.S. federal criminal investigators have the resources to make cases that meaningfully target China's corruption and criminality by investigating, prosecuting, and convicting criminals. We have the ability to follow the illicit money and value trails and take away the criminals' proceeds of crime. The civilized world is predicated on the rule of law, equal justice and holding wrong-doers accountable. Unfortunately, when it comes to CCP Inc. what is missing is political will, policy, consensus, mandate, and an articulated mission. Enforcement is the key.

Develop a U.S. Law Enforcement Strategic Plan Focused on CCP Inc. Crime

Every U.S. government department and agency has a mission statement. They have a number of strategic plans, five-year plans, performance goals, etc. Most importantly, the plans are used to allocate funding and resources. (Unfortunately, these five-year plans are seldom reviewed five years later. The failures in achieving the articulated goals are rarely noted and those responsible for the failures are never, I repeat, never held accountable.) Having a strategic plan is simply how government bureaucracies work. We do not have an all-encompassing law enforcement-oriented strategic plan to confront PRC-focused crime in the United States and abroad. We need one.

In February 2022, the "China Initiative" targeting CCP Inc. crime—particularly espionage and IPR theft—was cancelled. That same month, the FBI's Director Christopher Wray said that Chinese spying had become so prevalent in the U.S. that on average, the FBI was opening on average two counterintelligence investigations a day, with more than 2,000 such cases already underway.[xxxv]

As disappointing as the cancelation of the China Initiative was, even still the emphasis on just one or two SUAs is not enough. In addition, an effective strategic plan should not fall under the purview of one government department or bureau. CCP Inc. criminality is extensive and wide ranging. There are multiple SUAs that demand attention. Crimes should be looked at as parts of a whole. The target should be considered an on-going criminal enterprise. The totality of CCP Inc. transnational crime and money laundering needs to be understood. These transnational crimes cut across the mandates of several U.S. intelligence, law enforcement, and regulatory agencies. Therefore, I encourage the current administration to review its policies vis a vis CCP-affiliated criminality. Perhaps Congress via the power of the budget and executive branch oversight could mandate a U.S. government-wide law enforcement oriented strategic plan that investigates and holds accountable those involved with CCP Inc. transnational crime and corruption.

Establish CCP Inc. Task Forces

In the United States, the FBI has the mandate to pursue most of the CCP Inc.'s SUAs, money laundering methodologies, and enablers found in the United States. The criminal networks also have overseas ties. Fortunately, the FBI has 63 legal attaché offices—commonly known as legats—and more than two dozen smaller sub-offices around the world, providing coverage for more than 180 countries, territories, and islands. Other federal agencies and departments as well as state and local law enforcement offices have roles to play as well. Some, like the DEA and ICE, also have a large overseas presence.

According to FBI Director Christopher Wray, China poses the biggest threat to the U.S., more than any other nation.[xxxvi] Wray has made numerous statements about the dangers of Chinese espionage and IPR theft. The wide variety of other SUAs do not receive enough attention by the Bureau. There is also a general lack of understanding within the FBI of TBML and how it impacts so many crimes including China-centric money laundering methodologies. All of the above, and many other methodologies and enablers with "Chinese characteristics" are part of the CCP Inc. business model.

Over the last decades, U.S. law enforcement has enjoyed considerable success establishing task forces comprised of federal, state, and local law enforcement. There may be concurrent jurisdiction when, all at the same time, a crime is a violation of federal, state, and local law enforcement. Task forces typically focus on terrorism, organized crime, narcotics, gangs, and human trafficking. Some of the best-known national task forces are the Organized

Crime Drug Enforcement Task Forces (OCDETF) and the Joint Terrorism Task Forces (JTTFs). The Director of National Intelligence and other U.S. intelligence agencies often assist the task forces in gathering and analyzing intelligence related to national security threats.

I propose establishing new task forces comprised of federal, state, and local law enforcement that specifically target the CCP Inc. threat domestically. And, understanding and adhering to the constraints posed by venue and jurisdiction, investigate the Chinese criminal presence overseas. This must be done in concert with our partners. Foreign investigations should include Chinese triads' involvement in illicit trade in ports, FTZs, BRI projects, transnational crime of all sorts, cross-border money laundering operations, and corruption. Per the above, certain CCP Inc.-backed crimes are currently being investigated—for example, espionage and IPR theft. But, once again, we need an understanding of the "totality" of what is going on including the relationships between criminal networks and their enablers engaged in a variety of SUAs. We need to focus on uniquely Chinese ways of laundering money and transferring value. We have to better understand the relationship between the government of China, its intelligence services, and organized crime. An isolated FBI field office or even a task force dedicated, for example, solely to narcotics trafficking is not going to be able to do that.

The new China Inc. task forces should be directed by Assistant U.S. Attorneys that have an aggressive approach but fully adhere to the law and respect and safeguard civil liberties.

Really, Truly, Finally Go After the Money

U.S. law enforcement has consistently talked about the importance of "following the money" and taking away the proceeds of crime from criminals and criminal organizations. Yet in practice those self-evident goals have not been emphasized. To take just one notorious example, in our "War on Drugs" our efforts have been concentrated on interdicting the participants and the products. Another strategy the DEA and other law enforcement organizations pursue is to go after the "kingpins" or the leaders or heads of criminal organizations. The strategy is to decapitate the boss of bosses and kill the organization. A further tactic is to go after the low-level participants—the street-level dealers and the mules and follow them to the top of the organizational structure. However, the most common counter measure of all is to go after the product, from bags of fentanyl and opioid products smuggled across the border to tons of cocaine seized on the high seas. The history of the drug wars over the last 30 years has shown that none of these tactics have been effective.

Having been in federal law enforcement, I'll tell you the truth: We go after the participants and the product because it is far easier than going after the money. Also, the product is not just drugs. It similarly holds true for human beings in trafficking networks, counterfeit goods, illicit tobacco, wildlife trafficking, etc. All of the above and many more are SUAs for CCP Inc. money laundering. Criminals do not traffic in drugs for the sake of drugs or any other illegal good or service. They engage in crime for the money. Following the money trail and taking away proceeds of crime will hurt the criminal organization far more than a prison term or a seizure of contraband. Our emphasis on product and participants has led to failure. But the law enforcement bureaucracies persist in their efforts primarily because of careerism, bureaucratic culture, and lack of imagination. In order to change that paradigm, we need to emphasize the money and value trails including in the trade, cyber, and digital arenas. In other words, we must target and prioritize the proceeds of crime. To make that happen, we have to change the incentives and the culture of the law enforcement bureaucracies. I have written about this important topic elsewhere.[xxxvii]

Civil Forfeiture

I have little expertise in international law. I am not an attorney. So, the following is simply an idea that could be explored by victims of CCP Inc. criminal actions including the trafficking of fentanyl.

Sovereign immunity is a long-standing doctrine that grants immunity to a foreign country against the jurisdiction of the courts in another country. There have not been many exceptions to this principal, yet there may be one that is relevant to our situation with China. The 1976 Foreign Sovereign Immunities Act, or FSIA for short, presents the legal context that allows individuals or organizations to bring a civil lawsuit against foreign states or their representatives as well as foreign organizations. FSIA lists procedures to be followed when suing a foreign country as well as how assets are to be attached for international debt recovery purposes. It is still quite difficult under FSIA and international law to hold foreign countries liable for criminal offenses; however, there are exceptions. Some of these include:[xxxviii]

- When a foreign state conducts commercial activities in, or when those activities directly affect the United States

- When there's a dispute over property taken in violation of international law

- When monetary damages against a foreign country are sought for loss of or damage to property, death, or personal injury resulting from its tortious conduct in the United States

For example, fentanyl and its precursors are produced in China. CCP Inc. could seriously crack down on the production, advertising, sales, and distribution of fentanyl and other opioids and their precursors. It chooses not to. An aggrieved plaintiff in the United States, perhaps the parent of a son or daughter that is a victim of fentanyl, working with an aggressive attorney, could bring a case against the PRC under the FSIA exceptions. Perhaps it could be a class action lawsuit. The same reasoning could hold under CCP Inc.'s peddling of dangerous counterfeit goods in the United States as well as IPR theft, toxic foods and medicines, and possibly other crimes.

The evidence is becoming increasingly clear that Covid-19 was developed in a lab in Wuhan. At the time of the time of Covid-19's release, domestic flights in and out of Wuhan were shut down. International air travel was allowed to continue. The policy spread Covid-19 around the world. Perhaps, one day China could even be held accountable for the development and intentional international spread of Covid-19.

It's currently impossible to go after China-based assets of criminal actors involved in illegal trade. However, there are plenty of Chinese assets in the United States. According to FBI Director Christopher Wray, "Effectively all Chinese companies are in the pockets of the Chinese Communist Party (CCP). . .those [companies] that aren't owned outright are effectively beholden to the government all the same, as Chinese companies of any size are required to host a Communist Party cell to keep them in line.... almost like silent partners."[xxxix] Therefore, since CCP Inc. is an authoritarian state and ultimately all assets belong to the government that condones criminality, in theory, CCP Inc. assets could be subject to civil asset seizure and forfeiture.

Formulate Intelligence Collection Taskings

I am out of the U.S. intelligence and law enforcement communities now, but it appears the concerned bureaus, agencies, and departments are for the most part ignorant about the totality of CCP Inc. transnational crime and, in particular, money laundering methodologies. This will only change when policymakers make it a matter of import. I urge the President of the United States to task the Office of Director for National Intelligence to include in the National Intelligence Priorities Framework (NIPF), and through Intelligence Community directives, to have the Central Intelligence Agency (CIA), National Security Agency (NSA) and other applicable intelligence agencies develop intelligence reporting requirements for HUMINT and SIGINT and other collection means that target Chinese transnational crime and money laundering globally. I further urge the release of unclassified overlays of global illicit markets with significant Chinese corruption and criminality (e.g., BRI). Within classification guidelines, criminal investigators should be given access to the finished intelligence products to assist them in their targeting and investigations.

The FATF Should Name and Shame China

In the world of anti-money laundering/counter-terrorist financing (AM/CFT), it is the Financial Action Task Force (FATF) that makes things happen.

The FATF was created in 1989 by the G-7 to combat international money laundering. The FATF is an international AML/CFT policy making-body. It does so primarily through its 40 recommendations and periodic mutual evaluations that ensure countries adhere to the internationally accepted AML/CFT guidelines. I have been directly involved with the FATF in its annual plenary meetings and the mutual evaluation process serving as a law enforcement "expert." While the FATF, and FATF-style regional bodies, have done much good and have been highly successful in bringing attention to the scourge of international money laundering, the FATF has simply not fulfilled its original mission—curtailing international money laundering. What is not openly discussed is that by the "metrics that matter," i.e., money laundering convictions and asset forfeiture, over the last 30 years our efforts have been disappointing. As Raymond Baker, the Founding President of Global Financial Integrity said, "Total failure is just a decimal point away."[xl] Money laundering enforcement has failed both in the U.S. and around the world. The reasons are many and I have written about them elsewhere.[xli]

Internationally, one reason for failure is that the FATF 40 Recommendations and mutual evaluation process have evolved into a procedural box checking exercise. The boxes reflect debate about whether or not a country is "compliant" with a recommendation/s. What's lost in the discussion is the original founding intent of the FATF and the effectiveness of AML/CFT as measured by the metrics that matter. Moreover, countries are afraid of being put on the FATF "blacklist" (something that doesn't really exist) because of bad publicity and international risk, ratings and credit concerns. So, in response to FATF pressure, countries often pass legislation or create rules or make promises to get the FATF off their back. This is all well and good. Unfortunately, I have seen in my career that after the evaluation process and the checking of boxes some countries soon go back to business as usual. Countries posture and make promises. However, they don't have the political will to use their own initiative and truly combat AML/CFT. And, unfortunately in the arena of combating international money laundering, we are only as successful as the weakest link. The Peoples Republic of China is a classic example of a very weak link. There are others.

In the most recent 2019 FATF mutual evaluation of China, none of the issues raised in this testimony were addressed. In my opinion, the mutual evaluation was simply another box checking exercise with political overtones if not unspoken pressure (China held the presidency of the FATF during the evaluation process) that did nothing to confront CCP Inc.'s involvement with transnational SUAs and money laundering.

As I state in my book *China – Specified Unlawful Activities,* measured by SUAs and China-centric money laundering methodologies and enablers, CCP Inc. represents the greatest money laundering threat in the world. Thus, despite China's latest mutual evaluation report, I urge the U.S. FATF delegation to build consensus within FATF to "name and shame" China. Other like-minded delegations should join the call. The same should happen in the FATF-style regional bodies of which China is a member – the Asia Pacific Group and the Eurasian Group on Money Laundering.

The FATF Should Create a New Recommendation that Specifically Addresses TBML

I have written about this elsewhere,[xlii] and have also addressed it in previous Congressional testimony, but the international community will never seriously make progress against trade-based money laundering (TBML) and associated crimes such as black-market exchanges and flying money unless and until the FATF creates a new recommendation that specifically addresses the issue.[xliii] Trade fraud is a very significant SUA for money laundering. Depending on its varied forms, TBML can also act as a money laundering technique or methodology. I believe it is the largest and most prevalent of all the money laundering methodologies. Moreover, trade fraud and TBML are inextricably intertwined with many of the CCP Inc. criminal activities and money laundering discussed. It has become part of CCP Inc.'s business model. It is time the FATF addressed the issue and create a specific anti-TBML recommendation.

Control the Border

Controlling the border is the single most important countermeasure to combat the scourge of fentanyl, human trafficking, money laundering and other related criminal activity.

References

[i] Financial Action Task Force, "What is Money Laundering?" accessed November 17, 2017; http://www.fatf-gafi.org/faq/moneylaundering/

[ii] Ibid

[iii] Dorothy Neufield, "Visualizing the $94 Trillion World Economy in One Chart," Visual Capitalist, December 22, 2021; https://www.visualcapitalist.com/visualizing-the-94-trillion-world-economy-in-one-chart/

[iv] Channing Mavrellis, "Transnational Crime and the Developing World," Global Financial Integrity, March 27, 2017; https://gfintegrity.org/report/transnational-crime-and-the-developing-world/

[v] Note: Full disclosure – I am proud to be on the Board of Directors of GFI.

[vi] "Counterfeit and pirated goods represent 3.3% of global trade: report," France24, March 18, 2019; https://www.france24.com/en/20190318-counterfeit-pirated-goods-represent-33-global-trade-report

[vii] Casey Hall, "A Turning Point for China's Stance on Counterfeit Luxury Goods," Business of Fashion, December 11, 2018; https://www.businessoffashion.com/articles/global-currents/a-turning-point-for-chinas-stance-on-counterfeit-luxury-goods#targetText=According%20to%20US%20Chamber%20of,at%20a%20staggering%20%24397%20billion

[viii] See U.S. State Department's International Narcotics Control Strategy Report Volume II on Money Laundering. The congressionally mandated report is released in March. The 2022 report can be found here: https://www.state.gov/wp-content/uploads/2022/03/22-00768-INCSR-2022-Vol-2.pdf

[ix] Shannon Tiezzi, "China's Growing Drug Problem: China's drug problem is getting worse, despite harsh penalties," The Diplomat, March 28, 2015; https://thediplomat.com/2015/05/chinas-growing-drug-problem/

[x] International Narcotics Control Strategy Report (INCSR), Volume I, U.S. State Department, March, 2021. China section, page 111; https://www.state.gov/2021-incsr-volume-i-drug-and-chemical-control-as-submitted-to-congress/

[xi] "How Much Do Americans Really Spend on Drugs Each Year?" The White House, 2014; https://obamawhitehouse.archives.gov/blog/2014/03/07/how-much-do-americans-really-spend-drugs-each-year

[xii] Meryl Kornfield, "U.S. surpasses record 100,000 overdose deaths in 2021," May 11, 2022; https://www.washingtonpost.com/health/2022/05/11/drug-overdose-deaths-cdc-numbers/

[xiii] Eric Lendrum, "Fentanyl Overdoses Leading Cause of Deaths in America in 2020," American Greatness, December 17, 2021; https://amgreatness.com/2021/12/17/fentanyl-overdoses-leading-cause-of-deaths-in-america-in-2020/

[xiv] INCSR

[xv] Steven Dudley et al.," Mexico's Role in the Deadly Rise of Fentanyl," Insight Crime, 2019, https://www.wilsoncenter.org/sites/default/files/media/documents/publication/fentanyl_insight_crime_final_19-02-11.pdf

[xvi] Natalie Colarossi, "DEA Seized Enough Fentanyl to 'Kill Every Single American' This Year as Opioid Deaths Top 100K," Newsweek, December 19, 2021; https://www.newsweek.com/dea-seized-enough-fentanyl-kill-every-single-american-this-year-opioid-deaths-top-100k-1660947

[xvii] Bob Portman Press Release, January 30, 2018; https://www.portman.senate.gov/public/index.cfm/2018/1/on-senate-floor-portman-highlights-psi-report-on-drug-traffickers-shipping-fentanyl-into-the-u-s-through-the-postal-service

[xviii] "Carfentanil: A Dangerous New Factor in the U.S. Opioid Crisis," Drug Enforcement Administration, Officer Safety Alert; https://www.justice.gov/usao-edky/file/898991/download

[xix] "Two Chinese Nationals Charged with Operating Global Opioid and Drug Manufacturing Conspiracy Resulting in Deaths," Department of Justice Press Release, August 22, 2018; https://www.justice.gov/opa/pr/two-chinese-nationals-charged-operating-global-opioid-and-drug-manufacturing-conspiracy

[xx] "Lethal Exchange: Synthetic Drug Networks in the Digital Era," C4ADS, 2020; https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5fb3077189409576d229502a/1605568376184/Lethal_Exchange_S

[xxi] Louise Shelley, "Fentanyl, COVID-19, and Public Health," World Medical percent Health Policy 12, no. 4 (2020) p. 392; please see the paper for sub-sources

[xxii] Channing Mavrellis and John Cassara, "Made in China: China's Role in Transnational Crime and Illicit Financial Flows," Global Financial Integrity, October 27, 2022, page 15; https://gfintegrity.org/report/made-in-china/

[xxiii] "Fentanyl Flow to the United States," DEA Intelligence Report, January, 2020; https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf

[xxiv] "Trade Based Money Laundering," the FATF, Paris, June 23, 2006, p. 1; http://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf

[xxv] Data and analysis were given to me by Dr. John Zdanowicz

[xxvi] "U.S. Tax Coffers Lose $640 billion of Taxable Profits due to TBML Evasion and Money Laundering in 2021," SEK Strategies, May 4, 2022; https://www.prnewswire.com/news-releases/us-tax-coffers-lose-640-billion-of-taxable-profits-due-to-trade-based-tax-evasion-and-money-laundering-in-2021-says-sk-strategies-301539461.html

[xxvii] World Integrated Trade Solution, World Bank; https://wits.worldbank.org/CountrySnapshot/en/CHN/textview

[xxviii] "China's foreign trade hits new high in 2021," State Council, Peoples Republic of China, Jan 14,2022; http://english.www.gov.cn/archive/statistics/202201/14/content_WS61e11577c6d09c94e48a3a0a.html

[xxix] Drazen Jorgic, "Special Report: Burner phones and banking apps: Meet the Chinese 'brokers' laundering Mexican drug money," Reuters, December 3, 2020; https://www.reuters.com/article/us-mexico-china-cartels-specialreport-idUSKBN28D1M4

[xxx] Sebastian Rotella and Kirsten Berg, "How a Chinese American Gangster Transformed Money Laundering for Drug Cartels," ProPublica, October 11, 2022; https://www.propublica.org/article/china-cartels-xizhi-li-money-laundering

[xxxi] Much of this section is taken from: John A. Cassara, "Flying Money May Land in the U.S.," Banking Exchange, February 21, 2016; https://www.bankingexchange.com/news-feed/item/6079-flying-money-may-land-in-u-

[xxxii] The definition of hawala was concisely expressed during the 1998 U.S. federal trial of Iranian drug trafficker and money launderer, Jafar Pour Jelil Rayhani, and his associates. The definition was coined by FinCEN analyst and expert witness Patrick Jost.
[xxxiii] According to the World Bank, "official" global remittances totaled approximately $625 billion in 2018. According to the IMF, "unrecorded flows through informal channels are believed to be at least 50 percent larger than recorded flows." For a full explanation and links to original sources, see John Cassara, "Money Laundering and Illicit Financial Flows," pages 99-103
[xxxiv] John Cassara, *Money Laundering and Illicit Financial Flows: Following the Money and Value Trails*, Amazon Kindle Direct Publishing, 2020. Each chapter covering an individual money laundering methodology or technique concludes with recommendations. In addition, see Chapter 14, "More Forward Steps," page 315
[xxxv] Judith Bergman, "China – The Massive Threat," Gatestone Institute, September 27, 2022; https://www.gatestoneinstitute.org/18886/china-massive-threat
[xxxvi] FBI website, International Operations; https://www.fbi.gov/about/leadership-and-structure/international-operations#:~:text=Today%2C%20we%20have%2063%20legal,countries%2C%20territories%2C%20and%20islands.
[xxxvii] I go into specifics on changing the culture and incentives in my book, *Money Laundering and Illicit Financial Flows: Following the Money and Value Trails*. See pages 316 – 318.
[xxxviii] The information on the FSIA draws heavily, including direct quotes, from the article "Can You Sue a Country?" Law 101, September 1, 2021; https://laws101.com/can-you-sue-a-country/#:~:text=Although%20foreign%20nations%20enjoy%20sovereign,commercial%20and%20state%2Dsponsored%20activities.
[xxxix] Judith Bergman
[xl] Raymond Baker, Capitalism's Achilles Heel, Wiley & Sons, 2005, page 173
[xli] John Cassara, *Money Laundering*, Chapter 2 – Sobering Statistics
[xlii] John A. Cassara, *Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement,* Wiley, 2016
[xliii] John A. Cassara, Written Statement for the Hearing On "Trading with the Enemy: Trade-Based Money Laundering is the Growth Industry in Terror Finance," Before the Task Force to Investigate Terrorism Financing, Of the House Financial Services Committee, February 3, 2016; https://financialservices.house.gov/uploadedfiles/02.03.2016_john_a._cassara_testimony.pdf

EXHIBIT 138

The Golden Shield Project of China: A Decade Later An in-depth study of the Great Firewall

Sonali Chandel, Zang Jingji, Yu Yunnan, Sun Jingyao, Zhang Zhipeng
College of Engineering and Computing Sciences, New York Institute of Technology, Nanjing, China
{schandel, jzang, yyu18, jsun19, zzhang36}@nyit.edu

***Abstract* - The Golden Shield Project aka the Great Firewall of China is one of the most popular and vital information security and censorship technology project that is being used very strictly and extensively in the country since 2008. The Great Firewall has been preventing Internet users in China from visiting many foreign websites for one reason or the other and blocking them completely. This particular firewall implements information access control through some stringent security policies and takes the responsibility of controlling and censoring the flow of data. The Great Firewall makes China one of the strictest countries in the world when it comes to the internet freedom of the netizens residing in the mainland. In this paper, we will focus on the development of the Great Firewall that includes the timeline of its development, the censorship policy used for its implementation, its effects and the principles behind the technology used for its application. We will discuss where it stands after a decade of its implementation. We will also present a study of techniques like using a VPN to circumvent the heavily monitored firewall. These circumvention techniques have become very popular in the mainland because of severe information censorship. With this research, we aim to offer a clear understanding of the Great Firewall to the people from across the world.**

Keywords - Great Firewall, Firewall, VPN, Access control, Censorship, Circumvention

I. Introduction

The 'Golden Shield Project' of China started in 1996, but its actual implementation happened in 2008. [1] The foreign media calls it 'The Great Firewall' to indicate the seriousness and extent of the information block it poses on the entire country. According to the definition of the Chinese government, the intention behind the Golden Shield Project is only to filter and censor wrong information originating from outside of China to protect the society from its influence. From the time of its inception two decades ago, the project has evolved and turned into a highly secure, heavily monitored system which is very well described by the term, 'the Great Firewall' as it mesmerizes the rest of the world. The most significant side effects of the Great Firewall implementation can be seen from the fact that some of the most popular social networking apps and websites in the world like Facebook, YouTube, Twitter, WhatsApp, and Instagram are all blocked in the mainland.

A decade has gone by since the Golden Shield Project has been officially implemented in the country, and there is no sign whatsoever of it being removed shortly. The government and the local citizens believe that the Great Firewall contributes to stabilizing Chinese society, both online and offline.

The Great Firewall is not only a powerful political tool but also an exquisitely designed network security program. However, at the same time, it also brings endless worries to some people, especially those who live in China and have to communicate with people from other countries for personal, business, or academic purposes. To scale the wall, they turn towards using VPN applications, which are not necessarily cheap, safe, and stable. From time to time, there is always a government crackdown on VPN sellers and users, causing many issues for everyone involved.

To help people in getting a full understanding of the Great Firewall, this paper researches its development process and the technology behind it. The paper is structured as follows: Section I introduces the topic. Section II presents the related work. In section III, the development of the Great Firewall and the network censorship situation in other countries of the world are discussed. In section IV, the paper talks about the technology behind the Great Firewall. This includes the discussion of the kind of technical methods adopted and the methods implemented during the last two decades. The technology behind VPN is introduced in section V while various conditions concerning the privacy and security issues in using VPN for circumventing the censorship is listed in section VI. In section VII, the paper presents a survey result on local people's view on the Great Firewall and VPN to show how well they know about the network censorship in China and whether they can protect themselves from all kinds of online attacks and information theft that happens while they are trying to scale the wall. Finally, we present our conclusion in section VIII and discuss the future works that can be carried on by someone interested.

II. Related Work

During the research for this paper, we found that the already published articles on this topic mostly focus on various aspects of the Great Firewall individually. Some of them focus only on the technology, some only on cultural and social impact and some only on the issues related to the local laws and policy.

Hounsel, Mittal, and Feamster [10] use natural language processing and search engines to automatically discover a much more extensive range of websites that are censored in China. They focus only on keyword blocking technology, which is just one aspect of the techniques used behind running the Great Firewall.

Stevenson [12] examines the methods of internet censorship employed by China and other nations and proposes a novel combination of existing legislative proposals, recommendations from the Electronic Frontier Foundation, and international cooperation as the best way to address the problem of internet censorship. It provides background information about legal and economic trade for our paper.

978-1-7281-2542-8/19/$31.00 ©2019 IEEE
DOI 10.1109/CyberC.2019.00027

Farnan, Darer and Wright [17] considers the legitimate responses from the DNS servers themselves and present the argument that this type of attack may not be primarily targeted directly at users but at the underlying DNS infrastructure within China. However, the evidence they present needs more experimental data for the verification of their argument.

Zhang et al. [22] talk about secured VPN technology, but we have extended the idea of using VPN technology specifically as a countermeasure to the Great Firewall.

In this paper, we discuss the development of the Great Firewall for over ten years from the technology to the government policy behind it. We have also analyzed some of the significant loopholes of the Great Firewall that other published papers on this topic have not mentioned. We have also connected the Great Firewall and its effects to its countermeasure, known as VPN.

III. The Development of The Great Firewall

3.1 The Timeline of the Great Firewall

The Great Firewall is the nickname, which the western media gave to a sub-system of the Golden Shield Project in 1997. The Golden Shield Project also called as 'National Public Security Work Informational Project,' is a project that includes security management information system, criminal information system, exit and entry administration information system, supervisor information system and traffic management information system. This nationwide network-security fundamental constructional project was started by the Central Cyberspace Affairs Commission of the People's Republic of China. [33]

The Internet first arrived in China in 1994. As the availability of the Internet gradually increased with time, it became the most common communication platform and tool for trading information like everywhere else in the world. [15] With the Internet, also came the western ideologies, which the government was reluctant to embrace. Hence, the birth of the Golden Shield Project.

The entire project was implemented in different phases. The main tasks of the first phase (1998-2006) of the project were the construction of the first level, second-level, and the third-level information communication network, application database, shared platform. The second phase was initiated in 2006, which took only two years to complete. It was mainly focused on enhancing the terminal construction while trying to formalize public security work. [13]

To increase the final construction, along with the public security business application system, the Chinese government started the phase II project in 2006. Compared to phase I, phase II emphasized more on information application types of the public security business and public security information. The primary goals of phase II included the application system construction, system integration, the expansion of information center, and information construction in central and western provinces of the country. With the completion of phase II in 2008, internet censorship in China became more powerful than ever [13]. Table 1 shows a brief timeline for this project.

TABLE 1. The Timeline of The Great Firewall in China

Year	Major Events
1996	The Great Firewall was first set up
2004	The services of keyword screening and sensitive words masking were introduced by Cisco.
2004	Wikipedia got blocked for the first time (It is accessible now) [4]
2007	YouTube launched Hong Kong substation, and somehow its use in Chinese mainland started being blocked.
2008	Facebook got blocked
2009	Twitter got blocked
2010	Google claimed that it was attacked by Chinese hackers because it refused to allow the Chinese government to control its server in Beijing. A few days later, Google was blocked.
2014	Instagram was blocked.
2015	All foreign websites with a domain name co.jp are blocked

Table 2 shows some most common types of information that are censored online. [9]

TABLE 2 Characters of filtered information

Classification	Example
Politically Sensitive Information	Facebook\Twitter\New York Times
Pornographic Information	Baidu.jp
Online scams and other crimes	Some online gambling websites

3.2 The Technology Development of the Great Firewall

This section talks about the four stages of technology developments of the Great Firewall from 1998 to 2018.

1). First stage: The Golden Shield blocks domain names and IP addresses

The first generation of the Golden Shield project proposed an internal filter that blocked specific domain names and server's IP addresses. A multi-level system was implemented to track Internet users who violated the rules. As a result, all Internet cafes in the country are required to install surveillance software either provided or approved by the local police. This system monitors traffic on all computers in the café, including the screens of each user. The system also has direct access to the policy network system. Users at Internet cafes are required to present their ID cards before they can access the Internet. If a violation occurs, the Internet cafe owners will submit their personal information to the local police immediately via the Internet [11]. Many Internet service providers (ISP) for residential users are also required to verify every user's ID information. Many of the web-based forums prohibit anonymous posting. Real names are required to register an ID to submit articles [21]. Many popular smartphone apps also need their users to register using their original ID to be able to keep track of every user's online activities.

2). Second stage: The Golden Shield implements keyword censorship

In the second stage, the keyword-filtering system of Golden Shield was upgraded to detect the content of the websites that netizens visit, even if the internet connection is going through a proxy. If there is some “sensitive content” communicated along with the network connection, the Transmission Control Protocol (TCP) is reset automatically. For example, some phrases that refer to any political dissents, such as “Officials called on," “Persecution activities,” “Illegal detention,” and “Declared anti-communist” will be censored. [10]

3). Third stage: Great Firewall begins detecting VPNs and other circumvention tools

With support from the government, the developers of the Great Firewall finally managed to identify weaknesses in VPNs [44]. They found that there are some distinct features of the commonly used VPN protocols, such as IPSec, L2TP/IPSec, and PPTP, which often use specific ports. When processing the encrypted connection, it leaves a distinctive trace. Again, the Great Firewall was upgraded to detect such connection traces. As a result, there is a very long list of VPNs that cannot be used functionally because the Great Firewall stopped the connection traces, such as Free VPN, Green VPN, Jiguang VPN, Tianxing VPN and many more. [21]

4). Fourth stage: Cybersecurity laws target anonymity and VPNs

In addition to continually upgrading the technology behind the Great Firewall, Beijing has also introduced new laws to criminalize VPN service providers. The first primary law to regulate Internet content was released in 1996. This law was about the “Interim Provisions Governing Management of Computer Information Networks in the People’s Republic of China connecting to the International Network.” These provisions were amended and enhanced in 1998 and 2000 by the “Provisions for the Implementation of the Interim Provisions Governing Management of Computer Information Networks in the People’s Republic of China.” [12] The law stated that all Internet information services must be licensed (if commercial) or registered with the authorities (if private). ISPs must record and retain data about the number of time users spend online, their account numbers, their IP addresses, and their dial-up numbers. The latest addition to this string of regulations came in 2005, which deals specifically with providers of “Internet news information services.” [18]

On January 22, 2017, the Chinese Ministry of Industry and Information Technology (MIIT) announced a “Notice on Clearing Up and Regulating the Internet Access Service Market,” which forbids the unapproved creation of dedicated lines or other information channels to conduct cross-border business activities. It means providing VPNs to the users without official permission is illegal in China now. Table 3 shows the development of cyber laws for VPNs in China. [6]

In December 2017, a man called Xiangyang Wu was sentenced to 5.6 years in prison and fined 500,000 Yuan (73K USD approx.) for illegal business operations of VPNs. [39] According to announcements made by Shanghai Baoshan District People’s Court in October 2018, Dai Mou was also sentenced to three years in jail and was fined RMB 10,000 (US $1,446) for selling and using VPN services in China illegally. [38]

TABLE 3 THE DEVELOPMENT OF CYBER LAWS FOR VPNS IN CHINA

Time	Development
January 22, 2017	the Chinese Ministry of Industry and Information Technology (MIIT) announced a “Notice on Clearing Up and Regulating the Internet Access Service Market” [6]
January 2017 - March 2018	A large amount of Taobao shops were shut & the VPN applications were removed from iPhone market [40]
December 2017	Xiangyang, the VPN service provider, was sentenced to jail for being guilty [39]
October 2018	Dai Mou has been sentenced to three years in jail and a fine for selling and using VPN services.[38]

3.3 Internet Censorship in China vs. the Rest of the World

China is not the only country in the world to implement censorship on its cyberspace. Besides China, there are more than 20 countries around the world that seriously monitors and censors the online activities of their netizens. Apart from these countries, some other countries keep implementing censorship temporarily during some protests or demonstration against its government or when some social disturbance happens in their territory. They do this mostly to control the news from spreading, both real and fake and causing more disruption in society. Given the different cultural background and values, each country's Internet censorship presents a very different picture. [20]

In Table 4, we briefly list the primary methods used by some countries for the censorship of their network. Most of the countries do not directly block access to any legal, foreign websites. Also, there is no official verification system adopted in any other countries as China does. [1]

TABLE 4 CENSORSHIP IN CHINA VS. THE REST OF THE WORLD

Country	Censorship
China	Great Firewall
North Korea	Closed LAN
Cuba	Limit the number of Internet users
Myanmar	Closed Internet
Turkmenistan	High Internet access costs
Vietnam	Limit speed and comments
Iran	Internal Intranet.

IV. THE GREAT FIREWALL – AN EXTENSION OF A GENERAL FIREWALL

4.1 The Firewall Technology

The core technologies behind any general firewall include the concept of Packet filtering, Application Proxy, Stateful Inspection, and Complete Content Inspection.

4.2 Methods used behind the Great Firewall

The Great Firewall technologies combine multiple firewalls technologies, as mentioned in section 4.1. For example, the IP address checking and filtering technology in the Packet Filtering Firewall and the connection blocking technology in the data detecting technology in the Application Proxy Firewall. The Chinese government employs multiple approaches for censorship that includes both technical and non-technical means. [24, 17]

The following section talks about the leading methods that are used behind the Great Firewall:

1) DNS poisoning technology: One of the essential technical methods used by the Great Firewall is DNS poisoning. When the Great Firewall observes DNS queries to specific domains, it responds by sending a poisoned DNS response to the requesting DNS resolver. Due to its position in the network, this typically reaches the requesting DNS resolver before the response from the DNS server. This results in the requesting DNS resolver caching the poisoned DNS response and ignoring the response from the DNS server itself. [17]

2) Self-Censorship: According to laws and regulations mentioned in section 3.2, Chinese companies are responsible for their content, and any violations can lead to severe penalties ranging from hefty fines to closures. Therefore, many large companies have set up their law enforcement teams to monitor and ensure that their platforms do not contain banned topics. [44]

3) Manual enforcement: To enforce censorship and filter harmful content considered detrimental to the progress of China, a large number of Internet watchdogs are employed. These people are contracted by the authorities to monitor online content and inform about any potential violations to the assigned government officials to make an on-site investigation. Some sites offer back-end access, allowing these watchdogs to edit content directly. Recently, advancement in AI technology has allowed the monitoring processes to be automated on a large scale. [44]

4.3 The Working principle of the Great Firewall

The Great Firewall blocks a specific site for many different reasons. However, these reasons entirely depend on the choice of the government. The Great Firewall aims to eliminate criticism and prevent people from being infiltrated by the information that the government decides to be harmful to the peace and harmony of the people in the country [24]. It can include a ban on sensitive words, which can insinuate national leaders, violation of the constitution or reactions that can influence the peace of society. There is much censorship regarding social issues becoming widespread and known to the public or outside world as well. Similar news coming from the outside world that the government feels might spoil the mind of the local citizens is censored as well. Fig.1 shows the working principle of the Great Firewall [5]. Between the times a user submits their request, and the server sends back the response, four things can go wrong [27]. The following points explain how it works in steps.

1) DNS Blocking: When a netizen enters a URL, the DNS finds the corresponding IP address. If DNS is set as not to return that particular IP address, then the user cannot access the site. As shown in Fig.1, the message displayed on the screen is "Cannot find the webpage." Around 2002, China began to use 'Domain Name Hijacking.' They use IDS (Intrusion Detection Systems) monitoring systems provided by routers to hijack domain names, preventing people from accessing filtered websites. At the same time, to prevent advanced users from directly using different domain name servers with normal functions, China has also begun to block overseas DNS servers and has blocked hundreds of North American DNS servers. [17]

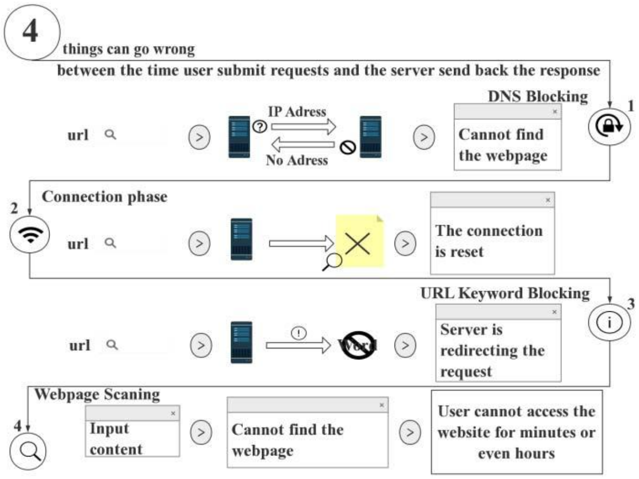


Fig.1 The working principle of the Great Firewall

2) Connection Phase: The monitor will compare the user's request to the list of banned IP addresses [5]. If it belongs to a banned address, the server aborts the request. As shown in Fig.1, the error message displayed is, "The connection is reset."

3) URL Keyword Blocking: Although the URL is not on the blacklist, the connection is reset if the requested URL contains forbidden words [19]. Advanced routing equipment from companies such as Cisco, which supplies 80 percent of China's routers, has helped China achieve keyword filtering. As shown in Fig.1, the error message displayed is, "The server is redirecting the request." [10]

4) Webpage Scanning: Once a user enters their requested site, the monitoring system scans the entire page to see if it can pass. Users may not be able to access the site for a few minutes or even an hour. As shown in Fig.1, the error message displayed is "Unable to display the web page."

4.4 The Aftereffects of the Great Firewall

4.4.1 Effects on Society

The firewall is not meant to separate the Chinese internet from the overseas internet, but it is mainly used to implement targeted blocking of individual foreign websites, mobile applications, and specific web pages. It is important to note that these interception points add up to a tiny fraction of the vast ocean of overseas internet. Some people take the blocking very seriously because some blocked websites used to be very popular among Chinese netizens. For example, Google, Facebook, Twitter, and other mainstream websites in the United States. There are two dominating views about censorship. One is that the western world has taken this as a prominent example of China's "lack of Internet freedom." Moreover, the other half includes the local people who are not at all interested in the blocked sites in any way and do not get affected by its absence. For them, the problem is almost nonexistent. The reality is that both sides are deepening or expanding in their respective directions. [2]

4.4.2 Effects on Businesses – Private and government-related

A. In China

In the past few years, the Golden Shield project has brought a significant impact on the nation when it comes to the e-business. The first thing to notice is the rapid growth of local internet companies, typically the "BAT" (Baidu, Alibaba, and Tencent). Without any powerful competitor from the outside world, these companies have gained almost unlimited and unopposed resources in the Chinese market, including the government's support. [16]

In 2018, the use of Baidu as the only search engine reached 60% of the overall purpose of the local search engine market [42]. The success of Baidu has grown tenfold after Google quit the Chinese market in 2010. Though a survey conducted by 'China Internet Watch' in, August 2018 suggests that over 70% of Chinese will choose Google over Baidu if it ever returns. [43]

The Internet industry in China, without powerful foreign competitors, is prospective yet still in chaos. Big companies like the "BAT" keep ignoring the internet's ethics principles from time to time. For example, Weibo (Twitter's equivalent), a social website where users can post pictures, short videos, and text contents, was denounced by its users for a series of violations of government policies including stealing users' account to post and re-post commercial advertisements and randomly blocking posts from accounts which are not VIP accounts in order to push people to buy its VIP services. However, Weibo is still one of the most popular social websites in the country. In addition, after learning lessons from mistakes made by Facebook and Twitter, Weibo cooperates with the Chinese government very closely.

The Great Firewall not only encourages the growth of local internet enterprise but it also brings profits to VPN service providers even when most of the free VPN applications have been defined as illegal in the last two years. Apart from the restrictions set by the government, there are some side effects, which increases the operating costs of all the foreign and local companies who have a business in other countries. Also, they have to adopt a VPN to ensure their regular communication between their overseas branches and clients. Even though such communications will not be targeted directly, but the ban on non-state sanctioned VPNs and the cost for building VPN servers are still expected to grow extensively. [41]

B. International influence

In China, the cybersecurity law was officially implemented from June 1, 2017. Many enterprises in Europe and the United States, industry associations with a government background, government departments, and mainstream media expressed varying degrees of concern, disappointment, and even anxiety about the Chinese cybersecurity laws. Foreign critics said that the law could shut out foreign technology companies from "important" departments and lead to controversial rules, such as requiring companies to store data on servers in China. Such actions were already taken before the new cyber laws were implemented. For example, Google decided to quit the Chinese market only because it refused to store data in servers under government surveillance, located in Beijing. [1]

4.5 Technology Tricks and Loopholes

Although the Great Firewall is growing to be stronger, there still exists some loopholes that users find very hard to understand. For example, some users can access a few blocked websites such as YouTube, when they use an external LAN port for connecting to the LAN. Some of these problems are still not settled, but some can be explained. For example, some users find that they can still receive notifications from blocked social media apps such as Facebook and Twitter. Take Apple's APNS (Apple Push Notification Service) as an example. The operation behind it can be seen in Fig.2.

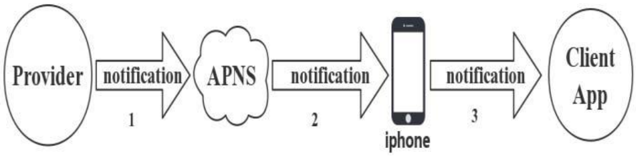
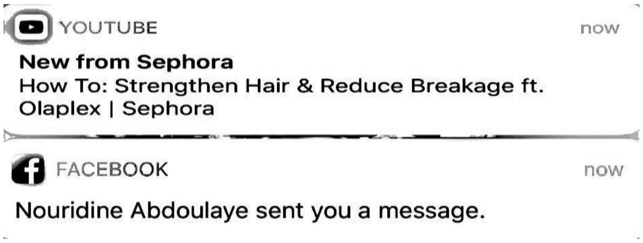


Fig.2 Apple's official APSN mechanism

The Provider is the background server of users' program. The Provider server is blocked, but the APNS server is not as it is in foreign countries (mostly more than one). It can communicate freely with the provider. Therefore, there is no communication problem between APNS and iPhones. As a result, Facebook and other blocked apps can send messages to APNS, and then APNS can push those messages to the iPhone, bypassing the wall as seen in Fig. 3. This also applies to Android phones where users can get a push notification from the blocked app, but they cannot open it.



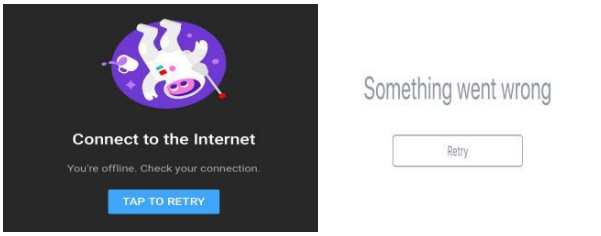
YOUTUBE now

New from Sephora
How To: Strengthen Hair & Reduce Breakage ft. Olaplex | Sephora

FACEBOOK now

Nouridine Abdoulaye sent you a message.

Fig.3 Example of YouTube and Facebook users receiving message notifications



Connect to the Internet

You're offline. Check your connection.

Something went wrong

Fig.4 The messages above shows some error messages received while trying to open and access some blocked sites

Except for a few loopholes, the Great Firewall technology is robust enough to censor everything else without fail. Some local versions of some universal apps like QQ music can even detect that the users are using a VPN to connect and hence decline the users' access to their server.

V. The Technology to Circumvent Great Firewall - VPN

VPN (Virtual Private Network) refers to a private communication environment built on public communication facilities, which is characterized by private and virtual communication. The goal of a VPN is to establish a logical network independent of the physical topology of the system, which allows a geographically distributed set of hosts to interact with each other and can be managed as a separate network [31]. It is commonly used in enterprise-level office systems, but because of the Internet censorship on such a massive scale in China, many people use VPN to scale the wall. VPN provides an end-to-end transmission system, and it is very convenient for users to log in to the company gateway from a remote location with an untraceable IP address. Because of this approach, it can easily avoid institutional scrutiny.

5.1 The Technologies used by a VPN

The mainstream applications that claim to provide VPN services are using one of the following three techniques: Proxy, IPSec, and SSH.

1) Proxy Server: A proxy server is like a courier service which is responsible for nothing but transcending the message. The work of proxy servers is conducted in the HTTP layer and Socket layer in the Open System Interconnection (OSI) model under most circumstances. [21]

2) IPSec: IP security is the most common method used by VPN applications. It works in the third layer of the Open System Interconnection (OSI) model, which is the Network layer. [21]

3) SSH: It is an encrypted channel that needs to be combined with the proxy server to overcome the blocked network. Hence the tool that is used to scale the blocked network which is usually called SSH is, in fact, an SSH agent. It can be considered as an encrypted agent, where the package is kept in a safe case while being sent to the courier. In the TCP/IP five-tier model, SSH is the security protocol that applies to the application layer and transport layer. SSH is a remote shell, an application based on SSL. Although many people use SSH to transmit data, they merely use the SSL proxy function of SSHD software to get this job done. [21]

A. The awareness of Chinese citizens about GFW and VPN

Table 5 shows the results from an online survey that shows the data from the citizens who visited the blocked websites [24]. This survey aimed to find out the awareness of the local netizens regarding GFW and how many still choose to visit the blocked websites. Figure 5 shows the motivation of people who tried to visit those websites. [24]

TABLE 5 THE SURVEY RESULTS OF THE NETIZENS WHO VISITED THE BLOCKED WEBSITES

Relevant factors	The result of the Survey
Gender	92% male
Education background	73% of the participants were university students
Age group	22-25 yrs.
Occupation	Students from an IT background
Methods used to visit the blocked websites	Mostly free VPN
The frequency to scale the wall	66% visited every day
Money spent on scaling the wall	88% paid less than 10 yuan per month

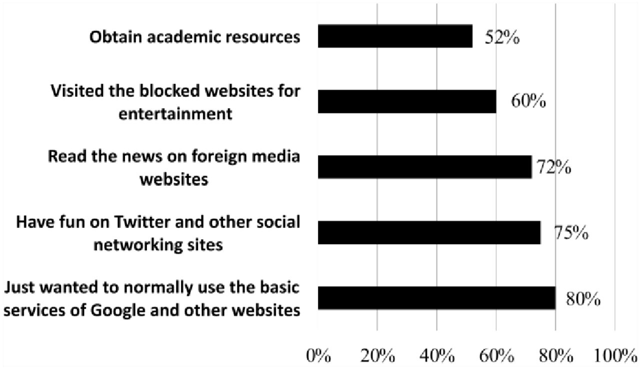


Fig.5 The motivation of people who tried to use VPNs

5.2 Privacy and Security Issues in using a VPN

When it comes to dealing with the Great Firewall, VPN is an inevitable technology. In the past few years, more and more netizens around the world have chosen to use VPN to cover up their online traces. However, the various pros and cons cannot be neglected when it is about paid and free VPNs. Table 6 summarizes the advantages and disadvantages of using various paid and free VPNs. [29] [30] [28]

Also, here are the research results that the researchers found after analyzing the original coding and network behavior of 283 VPN apps in Android's Play store. [7]

1) 18% of VPNs do not encrypt any data, leaving users vulnerable to man-in-the-middle attacks when using open networks like public Wi-Fi.
2) 16% of VPNs embed code in users' network data, such as image transcoding. The purpose of image transcoding is to make the image load faster. Two apps embed Java scripts that push ads and tracks user behavior in their data. JavaScript can be easily modified into malware.
3) 18% of VPNs do not encrypt any data, leaving users vulnerable to man-in-the-middle attacks when using open networks like public Wi-Fi.
4) 16% of VPNs embed code in users' network data, such as image transcoding. The purpose of image transcoding is to make the image load faster. Two apps embed Java scripts that push ads and tracks user behaviour in their data. JavaScript can be easily modified into malware.

TABLE 6 THE ADVANTAGES AND DISADVANTAGES OF USING A VPN

Advantages	Examples	Disadvantages	Examples
The IP address can change	Betternet, VyprVPN, PureVPN	Unstable	Betternet, CrossVPN, WhatsVPN, Astrill
Anonymous use, No Tracking	Betternet, Psyphon, UltraVPN, ExpressVPN, VyprVPN, PureVPN		
Registration and login not needed to use	Betternet	Too many ads	Betternet
Easy to install and use	CrossVPN, Psyphon, NordVPN		
Multiple devices allowed per connection	WhatsVPN, CrossVPN, ExpressVPN, PureVPN, VyprVPN	Security is not guaranteed	CrossVPN
Support several VPN protocols	ExpressVPN, PureVPN, Astrill		

5) 84% of VPNs leak traffic when using IPv6. 66% of VPNs even leak DNS information making users more vulnerable to surveillance or modification attacks.
6) 67% of apps claim to enhance privacy, but 75 percent use third-party tracking codes to monitor users' online behavior. 82% require users to provide sensitive information, such as access to user accounts and text messages.
7) 38% of VPNs contain code classified as malicious by VirusTotal. VirusTotal, provided by Google, is a collection of more than 100 antivirus software antivirus services.

VI. RELEVANT GOVERNMENT POLICIES AND CURRENT SITUATION OF THE GREAT FIREWALL

6.1 Chinese Government's policies towards the Great Firewall

Under normal circumstances, there is no privilege given to anyone at any point of time to access the blocked sites in the country. However, during some very significant international sporting, political or business events like G-20 Summit, World Expo, Youth Olympic Games, etc. the government does allow the visitors from foreign countries to have the privilege of accessing the Internet without any censorship. This exceptional privilege service is provided by the telecom operators and is only allowed within an exclusive scope of a limited zone. These free internet access zones are just set for a limited period for the guests and media reporters until the event ends. Table 7 shows some examples of such events when a censorship-free zone was created for people visiting China from overseas for the same. [32]

TABLE 7 EXAMPLES OF THE GREAT FIREWALL FREE ZONE

Free Zone	Place	Time
World Expo	Shanghai	May 1, 2010- October 31, 2010
G-20	Hangzhou	September 4, 2016- September 5,2016
Asian Games	Guangzhou	November 12, 2010- November 27, 2010
Youth Olympics	Nanjing	August 16, 2014- August 28, 2014

6.2 Chinese Government's policies towards VPN

Although there are many VPN applications available in the market that can help in getting access to the blocked content but selling and using a VPN without an official license is illegal in many cases in China [37]. In January 2017, the Ministry of Industry and Information Technology (MIIT) issued the notice on clearing and regulating the Internet network access service market, which stated: "It is not allowed to establish or rent special channels (including VPN) to carry out cross-border business activities, without the approval of the telecommunications authorities." Through this announcement, we can see that unapproved VPN cross-border business activities are explicitly prohibited [6]. During the time between January 2017 to March 2019, a large number of Taobao shops got shut for selling illegal VPN software. At the same time, a lot of illegal VPN applications have been removed from the iPhone market as it is monitored by the local government now after its local data center moved to Guizhou, a province in southwest China, in March 2018 [36]. Although fears of a blanket block on services have not materialized, VPN connections often face outages during the time of major political events in China. [30]

6.3 Current Situation and Future Plans

The government regulation allows foreigners to invest in China's virtual private network but caps foreign ownership at 50% [3]. The government intends to turn Hainan province into a free trade zone to let Hainan become the foundation of an international tourist center and encourage overseas companies to establish regional headquarters there. Google has been away from China for eight years, but now the company has been quietly testing the waters by investing in different products in China. Google has launched its Drive and Docs products in Shenzhen in China, adding to a growing list of services it wants to offer in the world's biggest Internet market [26]. On January 19, 2018, Tencent and Google announced that they had signed a cross-licensing agreement for patents covering a wide range of products and technologies, and they said they would be open to further collaboration on future innovations. [35]

VII. CONCLUSION & FUTURE WORK

As a result of this research, we have concluded that there are four stages in the technology development of the Great Firewall. We talked about the leading technologies used behind the Great Firewall, including DNS poisoning, Proxy server technology, and Network address translation technology. We can also conclude that the Great Firewall is being developed and updated continuously. Therefore, the power of the Great Firewall cannot be ignored. The increasing importance of the Internet attracts people's attention on network and data security. The Great Firewall plays a vital role in protecting national information security. It has been preventing Internet users in China from visiting certain foreign websites, which the rest of the world considers as a prominent example of China's "lack of Internet freedom." Blocking some external sites is proving out to be extremely beneficial for the rapid growth of local internet companies. Organizations and netizens are rampantly using VPNs to circumvent and scale the wall. However, nowadays, there have been some new local laws that prohibit users and sellers from using and selling VPNs, respectively. Overall, we hope that our work can be used as a complete reference to learning more about the principles and policies of the Great Firewall.

Further study needs to be done on how to improve the firewall technology to better prevent illegal users from entering the Intranets. We hope that our work on the Great Firewall can help others to learn and know more about the Great Firewall. This paper offers a reference for studying the technologies and development of the firewall.

REFERENCES

[1] People's Daily Online: The cybersecurity act and the national security review system. http://theory.people.com.cn/n1/2016/0622/c40531-28469973.html

[2] Global times: what impact does the firewall have on China's Internet http://tech.163.com/15/0128/14/AH26MQKQ000915BF.html

[3] Expats Allowed to Invest in China's VPN Services in Hainan https://mp.weixin.qq.com/s/KGt3b5iMbhyScEzxc3in6A

[4] "China Now Blocked from Accessing Wikipedia." The Epoch Times. 8 June 2015. Archived from the original on 10 June 2017. Retrieved 4 May 2017.

[5] One picture shows you the data behind the Great Firewall of China. Web. https://www.svlik.com/704

[6] The evolution of China's Great Firewall: 21 years of censorship. Web. https://www.hongkongfp.com/2017/09/03/evolution-chinas-great-firewall-21-years-censorship/

[7] VPN is illegal. Use it carefully, even if it is not illegal. Web. https://www.sohu.com/a/125475123_354973

[8] US takes China VPN ban to the WTO. JobTubeDaily. 25 Feb.2018. Web. http://mp.weixin.qq.com/s/68hyFB156fj3fp36UV4JgA

[9] "GreatFire.org - Bringing Transparency to the Great Firewall of China." Archived from the original on 18 May 2018. Retrieved 19 May 2018.

[10] Austin Hounsel, Prateek Mittal, Nick Feamster, "Automatically Generating a Large, Culture-Specific Blocklist for China." presented at the Advanced Computing Systems Association, 2018

[11] Introduction on the Golden Shield. Web. http://www.china.org.cn/chinese/zhuanti/283732.htm.

[12] Christopher Stevenson, "Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World," 30 B.C. Int'l & Comp. L. Rev. 531, 2007.

[13] Golden Shield Project. Web. https://en.wikipedia.org/wiki/Golden_Shield_Project#cite_note-ccw-22

[14] VPN Seller Sentenced to 3 Years in Jail. Web. https://mp.weixin.qq.com/s/j10ai_Sr1Xx09cnpk0yAjg

[15] Internet Access to China. Web. http://www.chinanews.com/special/guoqing/60/2009/06-25/122.shtml chinanews.com. Retrieved28 August 2013.

[16] S. Chandel, T. Ni and G. Yang, "Enterprise Cloud: Its Growth & Security Challenges in China," 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Shanghai, 2018, pp. 144-152.

[17] Oliver Farnan, Alexander Darer, Joss Wright, "Poisoning the Well – Exploring the Great Firewall's Poisoned DNS Responses," Workshop on Privacy in the Electronic Society, ACM, 2016.

[18] Jyh-An Lee & Ching-Yi Liu, Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China, 13 Minn. J.L. Sci. & Tech. 125, 2012.

[19] Ignoring the Great Firewall of China. Web. https://www.lightbluetouchpaper.org/2006/06/27/ignoring-the-great-firewall-of-china/

[20] C. Mulvenon, James & S. Chase, Michael. Breaching the Great Firewall. Journal of E-Government, vol.2, pp.73-84. 2005.

[21] Z. Zhipeng et.al. "VPN: a Boon or a Trap? A Comparative Study of MPLS, IPSec, and SSL Virtual Private Networks," 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2018, pp. 510-515.

[22] JobTubeDaily (2018). How to use a VPN in China without Breaking the Law. http://mp.weixin.qq.com/s/BWSac-wv-f-xT0RRqJEMzw.

[23] Santoro, Michael A. "China 2.0: Illusion and Promise behind the 'Great Firewall.'" pp. 106–123, China, 2020

[24] Shao Zhuqing. "The survey about the status of Chinese citizens who visited the blocked websites." The checkout(blog) http://shaozhuqing.com/?p=2295

[25] Google Drive and Docs in China? Web. https://www.abacusnews.com/big-guns/google-drive-and-docs-china/article/2158441

[26] How Goldkorn, Jeremy, et al., editors. "The Chinese Internet: Unshared Destiny." Shared Destiny, Anu Press, 2015.

[27] January 2018 different VPN ranking list. Web. https://www.pingceji.com/guowai-vpn-ranking-2018-1

[28] Five of the most useful foreign VPNs in 2018 - based on a comprehensive comparison of multi-party performance. Web. https://www.pingceji.com/best-vpn-services-in-2018/

[29] PureVPN depth evaluation. Web. https://www.pingceji.com/purevpn-review-the-good-vpn-for-chinese/

[30] China Steps up VPN Blocks Ahead of Major Trade Expo. Web. https://mp.weixin.qq.com/s/xGv1X2GotYbyi8NK3irBjA

[31] Liu, Yakun and Yang, Dingcai. "Security Analysis of VPN." Journal of Beijing University of Posts and Telecommunications. 2003 (140-143), Vol. 26.

[32] Baijiahao (2018). An analysis of the supervision of VPN in China and how to use VPN services in compliance. https://baijiahao.baidu.com/s?id=1596346285526322054&wfr=spider&for=pc

[33] "What is internet censorship?" Amnesty International Australia. 28 March 2008. Archived from the original on 27 April 2015. Retrieved 21 February 2011.

[34] "Golden Shield Project phase II will focus on information integration and application." CCW Research (in Chinese). Archived from the original on 2009-05-31.

[35] Google and Tencent reached a patent cross-licensing agreement. Web. https://baijiahao.baidu.com/s?id=1589990616004104862&wfr=spider&for=pc

[36] Alert: VPN user fined for accessing international websites. Web. https://mp.weixin.qq.com/s/YabPj0nVaRESdqmIPZa8ZA

[37] China Begins Issuing Fines for Using VPNs - Yes, They are Illegal. Web. https://mp.weixin.qq.com/s/NrdAsCbgJGb-hVx49sLxAQ

[38] VPN Seller Sentenced to 3 Years in Jail. Web. https://mp.weixin.qq.com/s/j10ai_Sr1Xx09cnpk0yAjg

[39] Build a private VPN profit sentence about VPN; you do not know 10 things! Web. http://news.wehefei.com/system/2017/12/21/011170115.shtml

[40] VPN was banned, and only a few hundred over the wall software remained in the App Store in China. Web. https://www.aiyingli.com/48563.html

[41] "How to use VPNs in China without breaking the law," https://www.techworld.com.au/article/632635/how-use-vpns-china-without-breaking-law/

[42] "Search Engine Market Share China." http://gs.statcounter.com/search-engine-market-share/all/china

[43] "Over 70% Chinese will choose Google over Baidu if it returns". https://www.chinainternetwatch.com/26275/google-uncensored-search/

[44] How China Built the Great Firewall and How it Works. Web. https://mp.weixin.qq.com/s/J-NJm9we3q0zhLL0IzyMAA

EXHIBIT 139

Free speech vs Maintaining Social Cohesion

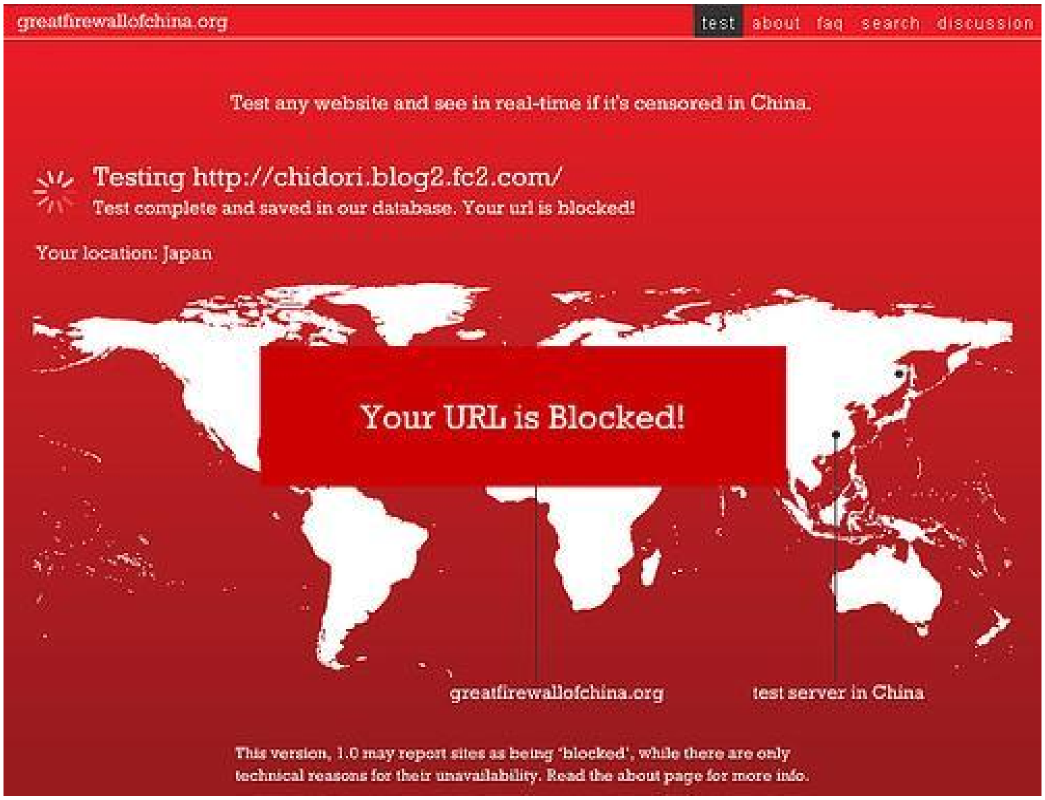
A Closer Look at Different Policies

- Home
- European Union Policy
- China's Great Firewall
- US Policy
- Google

Background Information

China is known for its strict policies regarding information control in comparison to the regulations adopted in other countries. The Golden Shield Project, often called the "great firewall of China", is an initiative managed by the Ministry of Public Security division of the Chinese government. As the nickname implies, the focus of this project is to monitor and censor what can and cannot be seen through an online network in China. This project started in 1998 and is still continually improving in restriction techniques through multiple methods. The OpenNet Initiative performed an empricial study that concluded that China has "the most sophisticated content-filtering Internet regime in the world". Some technical methods used are IP blocking, which denies the IP addresses of specific domains, packet filtering, which scans packets of data for controversial keywords, credit records, and speech and facial recognition.

To get an idea of how strict the policy is, http://www.alexa.com/topsites/countries/US consists of a list of the most popular sites in the United States. Google, Facebook, and Yahoo are the top 3; of these top 3, none are allowed in China. This is to be expected due to the quick information dissemination possible through these social domains. The website http://www.greatfirewallofchina.org/ lets users see whether their inputted domains are blocked in China, and is a convenient tool for demonstrating the widespread filtering employed by China.



Test any website and see in real-time if it's censored in China.

Testing http://chidori.blog2.fc2.com/

Test complete and saved in our database. Your url is blocked!

Your location: Japan

Your URL is Blocked!

This version, 1.0 may report sites as being 'blocked', while there are only technical reasons for their unavailability. Read the about page for more info.

China's primary search engine and most accessed website, Baidu, employs heavy censorship within its own search algorithms. Baidu "has a long history of being the most proactive and restrictive online censor in the search arena" (China Digital Times). Baidu claims to do this to help enforce existing censorship policies. In April 2009, certain Baidu documents that reveal some topics the search engine looks to censor have been leaked. These topics range from "Letters" to "Rights".

- # China's Great Firewall

- - Background Information
  - Opinions
  - References

Stanford CS181: Computers, Ethics, and Public Policy Final Project

EXHIBIT 140

The New York Times | https://www.nytimes.com/2023/04/26/business/china-censored-search-engine.html

China's Search Engines Have More Than 66,000 Rules Controlling Content, Report Says

Researchers from the Citizen Lab, a cybersecurity research group, found that the most diligent censor in China is Microsoft's search engine Bing, the only foreign search engine operating in the country.

By Steven Lee Myers

April 26, 2023

China's internet censorship is well known, but a report has quantified the extent of it, uncovering more than 66,000 rules controlling the content that is available to people using search engines.

The most diligent censor, by at least one measure, is Microsoft's search engine Bing, the only foreign search engine operating in the country, according to the report, which was released on Wednesday by the Citizen Lab, a cybersecurity research group at the University of Toronto.

The findings suggested that China's censorship apparatus had become not only more pervasive, but also more subtle. The search engines, including Bing, have created algorithms to "hard censor" searches deemed to be politically sensitive by providing no results or by limiting the results to selected sources, which are usually government agencies or state news organizations that follow the Communist Party's line.

"You might get no results if it is a very sensitive topic, but if your query is subject to this kind of self-censorship, what happens is you actually appear to get results as normal, but that's not actually happening," said Jeffrey Knockel, a senior researcher at Citizen Lab and an author of the report. "You're getting results only from certain pre-authorized websites."

The organization's researchers studied eight online platforms that offer search tools: the search engines Baidu, Sogou and Bing; the social media sites Weibo, Douyin, Bilibili and Baidu Zhidao; and the e-commerce giant Jingdong.

All are subject to extensive legal restrictions that have long censored criminal activity, obscenity, pornography, violence and gore, in addition to virtually any political, ethnic or religious content viewed as threatening to Communist Party rule and social stability.

More recent restrictions have extended to defamation of the country's heroes or martyrs, illegal surrogacy and misleading or false information about Covid-19 in Beijing.

Each of the companies have created mechanisms to comply with the government's ever-evolving restrictions.

The report found that Weibo, China's equivalent of Twitter, restricted search results for the term "Chinese spy balloon" so that only information from official Chinese sources would appear to those seeking to learn about the surveillance airship shot down by the United States in February.

Baidu blocked all results for searches that included the country's leader, Xi Jinping, President Vladimir V. Putin of Russia and the international warrant for the Russian president's arrest issued days ahead of Mr. Xi's visit to Moscow in March.

The report said that the Chinese tech companies had adopted more rules than Bing, one of the few foreign tech platforms allowed in the country, but compared with Baidu, Bing's rules were broader and affected more search results. They also on average restricted results from more domains.

Caitlin Roulston, a spokeswoman for Microsoft, said the company would look into the findings but had not yet fully analyzed them. "We are reaching out to Citizens Lab directly to get more information so that we can conduct any further investigation needed," she said.

Microsoft is one of the few foreign technology companies that still operates inside China, and it has acknowledged that to do so required complying with the country's censorship laws, something other companies, most prominently Google, refused to do.

Conditions in China have often been fraught for Microsoft, with the company's products facing crackdowns from the authorities. In 2019, Bing itself was blocked temporarily. In 2021, Microsoft shut down LinkedIn in China after seven years in the country, citing regulatory and competitive obstacles.

Mr. Knockel said the study reinforced the argument that foreign tech companies could do little to restrict censorship or other demands from the government. China, for example, has signaled that it will restrict the operations of artificial intelligence in chat bots, which Microsoft has already unveiled for Bing.

"Just simply allowing American tech companies to do business in China isn't going to solve any of the censorship or larger human rights issues that we would like to be solved in China," Mr. Knockel said.

Steven Lee Myers covers misinformation for The Times. He has worked in Washington, Moscow, Baghdad and Beijing, where he contributed to the articles that won the Pulitzer Prize for public service in 2021. He is also the author of "The New Tsar: The Rise and Reign of Vladimir Putin." More about Steven Lee Myers

EXHIBIT 141

(https://citizenlab.ca)

Missing Links

A comparison of search censorship in China

By Jeffrey Knockel (https://citizenlab.ca/author/jknockel/), Ken Kato (https://citizenlab.ca/author/kenkato/), and Emile Dirks (https://citizenlab.ca/author/emile/)

April 26, 2023

Download this report (https://tspace.library.utoronto.ca/bitstream/1807/127271/4/Report%23166-MissingLinks-050323.pdf)

This report has an accompanying FAQ (https://citizenlab.ca/2023/04/faq-a-comparison-of-search-censorship-in-china/).

Key findings

- Across eight China-accessible search platforms analyzed — Baidu, Baidu Zhidao, Bilibili, Microsoft Bing, Douyin, Jingdong, Sogou, and Weibo — we discovered over 60,000 unique censorship rules used to partially or totally censor search results returned on these platforms.
- We investigated different levels of censorship affecting each platform, which might either totally block all results or selectively allow some through, and we applied novel methods to unambiguously and exactly determine the rules triggering each of these types of censorship across all platforms.
- Among web search engines Microsoft Bing and Baidu, Bing's chief competitor in China, we found that, although Baidu has more censorship rules than Bing, Bing's political censorship rules were broader and affected more search results than Baidu. Bing on average also restricted displaying search results from a greater number of website domains.
- These findings call into question the ability of non-Chinese technology companies to better resist censorship demands than their Chinese counterparts and serve as a dismal forecast concerning the ability

of other non-Chinese technology companies to introduce search products or other services in China without integrating at least as many restrictions on political and religious expression as their Chinese competitors.

Introduction

Search engines are the information gatekeepers of the Internet. As such, search platform operators have a responsibility to ensure that their services provide impartial results. However, in this report, we show how search platforms operating in China infringe on their users' rights to freely access political and religious content, by implementing rules to either block all results for a search query or by only selectively showing results from certain sources, depending on the presence of triggering content in the query.

In this work we analyze a total of eight different search platforms. Three of the search platforms are web search engines, including those operated by Chinese companies — Baidu and Sogou — and one operated by a North American company — Microsoft Bing — whose level of censorship we found to in many ways exceed those of Chinese companies. While China's national firewall blocks access to webites, the role that Baidu, Microsoft, and Sogou play in controlling information is in overcoming two of the firewall's limitations. First, due to the increasingly ubiquitous use of HTTPS encryption, China's firewall can typically only choose to censor or not censor entire sites as a whole. However, these search engine operators overcome this limitation by selectively censoring sites depending on the type of information that the user is querying. Second, China's firewall operates opaquely, displaying a connection error of some kind in a user's web browser. By hiding the very existence of sites containing certain political and religious content, Baidu, Microsoft, and Sogou aid in preventing the user from being informed that they are being subjected to censorship in the first place.

We also examine search censorship on Chinese social media companies, namely Baidu Zhidao, Bilibili, Douyin, and Weibo. Perhaps more familiar to non-Chinese audiences are Douyin and Weibo. Douyin, developed and operated by TikTok's ByteDance, is the version of TikTok operating in China, and Weibo is a microblogging platform similar to Twitter. Perhaps less known are Baidu Zhidao and Bilibili. Baidu Zhidao is a question and answer platform similar to Quora operated by the same company as the Baidu search engine, and Bilibili is a video sharing site similar to YouTube. We also look at e-commerce platform Jingdong, which is similar to Amazon.

Given the strict regulatory environment which they face, users in China have limited choice in how they search for information. However, even among those limited choices, we nevertheless found important differences in the levels of censorship and in the availability of information among these search platforms. Most strikingly, we found that, although Baidu — Microsoft's chief search engine competitor in China — has more censorship rules than Bing, Bing's political censorship rules were broader and affected more search results than Baidu. This finding runs counter to the intuition that North American companies infringe less on their Chinese users' human rights than their Chinese company counterparts.

The remainder of this report is structured as follows. In "Background" and "Related work", we summarize the legal and regulatory environment in which Internet companies in China operate as well as existing research on Chinese search censorship. In "Model", "Methodology", and "Experimental setup", we describe how we model censorship rules, the manner in which we discover each platform's censorship rules, and the conditions in which we executed our experiments. In "Results", we reveal our findings of over 60,000 unique censorship rules being discovered, and we attempt to characterize which platforms censor more of what kinds of material. Finally, in "Limitations" and "Discussion", we discuss the limitations of our study, what our findings say about non-Chinese companies entering the Chinese market, and implications for future research.

Background

Internet companies operating in China are required to comply with both government laws concerning content regulations as well as broader political guidelines not codified in the law. Multiple actors within the government – including the Cyberspace Administration of China and the Ministry of Public Security – hold companies responsible for content on their platforms, either through monitoring platforms for violations or investigating online criminal activity. Companies are expected to dedicate resources to ensure that all content is within legal and political or ideological compliance, and they can be fined or have their business licenses revoked (https://firstmonday.org/ojs/index.php/fm/article/view/2378) if they are believed to be inadequately controlling content. China's information control system is characteristically one of intermediary liability or "self-discipline (https://www.mcclatchydc.com/opinion/article24570625.html)", which allows the government to push responsibility for information control to the private sector.

To understand the kind of information which is expected to be censored by companies in China, we can lean on at least four kinds of sources: (1) state legislation and regulations, (2) official announcements about state-led internet clean-up campaigns, (3) government-run online platforms where users can report prohibited material, and (4) official announcements about what kinds of prohibited material has been reported to the authorities.

Chinese government legislation and regulations have included provisions specifying what kinds of online content are prohibited. These documents include the *Measures for the Administration of Security Protection of Computer Information Networks with International Interconnections* (https://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/computer-information-network-and-internet-security-protection-and-management-regulations-1997.html) (1997), the *Cybersecurity Law* (https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/) (2017), *Norms for the Administration of Online Short Video Platforms and Detailed Implementation Rules for Online Short Video Content Review Standards* (https://www.chinalawtranslate.com/en/norms-for-the-administration-of-online-short-video-platforms-and-detailed-implementation-rules-for-online-short-video-content-review-standards) (2019), and *Provisions on the Governance of the Online Information Content Ecosystem* (https://wilmap.stanford.edu/entries/provisions-governance-online-information-content-ecosystem) (2020). Many of the categories of prohibited content are shared among these four documents, as indicated in Figure 1. Shared categories include pornography and attacks on China's political system. However, it is also clear that more recent documents – in particular, the 2019 *Norms for the Administration of Online Short Video Platforms* and the 2020 *Provisions on Ecological Governance of Network Information Content* – have provided new categories of prohibited content. These include specific prohibitions against "harming the image of revolutionary leaders or heroes and martyrs (https://www.chinalawtranslate.com/en/norms-for-the-administration-of-online-short-video-platforms-and-detailed-implementation-rules-for-online-short-video-content-review-standards/)" [损害革命领袖、英雄烈士形象] and more vague prohibitions against material which promotes "indecency, vulgarity, and kitsch (https://wilmap.stanford.edu/entries/provisions-governance-online-information-content-ecosystem)" [低俗、庸俗、媚俗].

Measures for the Administration of Security Protection of Computer Information Networks with International Interconnections (1997)

Article 5:

No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information:

1. Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations
2. Inciting to overthrow the government or the socialist system
3. Inciting division of the country, harming national unification
4. Inciting hatred or discrimination among nationalities or harming the unity of the nationalities
5. Making falsehoods or distorting the truth, spreading rumors, destroying the order of society
6. Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder
7. Terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people
8. Injuring the reputation of state organs
9. Other activities against the Constitution, laws or administrative regulations

Cybersecurity Law (2017)

Article 12:

Any person and organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they must not endanger cybersecurity, and must not use the Internet to engage in activities endangering national security, national honor, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts.

Norms for the Administration of Online Short Video Platforms and Detailed Implementation Rules for Online Short Video Content Review Standards (2019)

4. Technical Management Regulations:

Based on the basic standards for review of online short video content, short video programs broadcast online, as well as their titles, names, comments, Danu, emojis, and language, performance, subtitles, and backgrounds, must not have the following specific content appear (commonly seen problems):

1. Content attacking the national political system or legal system
2. Content dividing the nation
3. Content harming the nation’s image
4. Content harming the image of revolutionary leaders or heroes and martyrs
5. Content disclosing state secrets
6. Content undermining social stability
7. Content harmful to ethnic and territorial unity
8. Content counter to state religious policies
9. Content spreading terrorism
10. Content distorting or belittling exceptional traditional ethnic culture
11. Content maliciously damaging or harming the image of the state’s civil servants such as from people’s military, state security, police, administration, or justice, or the image of Communist Party members
12. Content glamorizing negativity or negative characters
13. Content promoting feudal superstitions contrary to the scientific spirit
14. Content promoting a negative and decadent outlook on life or world view and values
15. Content depicting violence and gore, or showing of repulsive conduct and horror scenes
16. Content showing pornography and obscenity, depicting crass and vulgar tastes, or promoting unhealthy and non-mainstream attitudes towards love and marriage
17. Content insulting, defaming, belittling, or caricaturing others
18. Content in defiance of social mores
19. Contents that is not conducive to the healthy growth of minors
20. Content promoting or glamourising historical wars of aggression or colonial history
21. Other content that violates relevant national provisions or social mores and norms

Provisions on the Governance of the Online Information Content Ecosystem (2020)

Article 6:

A network information content producer shall not make, copy or publish any illegal information containing the following:

1. Violating the fundamental principles set forth in the Constitution
2. Jeopardizing national security, divulging state secrets, subverting the state power, or undermining the national unity
3. Damaging the reputation or interests of the state

4. Distorting, defaming, desecrating, or denying the deeds and spirit of heroes and martyrs, and insulting, defaming, or otherwise infringing upon the name, portrait, reputation, or honor of a hero or a martyr
5. Advocating terrorism or extremism, or instigating any terrorist or extremist activity
6. Inciting ethnic hatred or discrimination to undermine ethnic solidarity
7. Detrimental to state religious policies, propagating heretical or superstitious ideas
8. Spreading rumors to disturb economic and social order
9. Disseminating obscenity, pornography, force, brutality and terror or crime-abetting
10. Humiliating or defaming others or infringing upon their reputation, privacy and other legitimate rights and interests
11. Other contents prohibited by laws and administrative regulations

Article 7:

A network information content producer shall take measures to prevent and resist the production, reproduction and publication of undesirable information containing the following:

1. Using exaggerated titles that are seriously inconsistent with the contents
2. Hyping gossips, scandals, bad deeds, and so forth
3. Making improper comments on natural disasters, major accidents or other disasters
4. Containing sexual innuendo, sexual provocations, and other information that easily leads to sexual fantasy
5. Showing bloodiness, horror, cruelty, and other scenes that causes physical and mental discomfort
6. Inciting discrimination among communities or regions
7. Promoting indecency, vulgarity, and kitsch
8. Contents that may induce minors to imitate unsafe behaviors, violate social morality, or induce minors to indulge in unhealthy habits
9. Other contents that adversely affect network ecology

Figure 1 : Types of prohibited online content listed in government legislation and regulations.

The government legislation and regulations listed in Figure 1 are not the only official sources detailing what kinds of online content are either legally prohibited or are politically undesirable. Another indicator of what online material is censored are official descriptions of internet clean-up campaigns. Since 2013, China’s cyber regulator (https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/) the Cyberspace Administration of China (http://www.cac.gov.cn/), the Propaganda Department’s Office of the National Working Small Group for “Combating Pornography and Illegal Publications” (https://www.shdf.gov.cn/), the Ministry of Public Security (https://www.mps.gov.cn/), and other party-state organs have conducted annual special operations for internet purification (https://archive.ph/CZA6j) [净化网络环境专项行动, abbreviated as 净网]. These special operations involve identifying websites, platforms, and accounts which contain prohibited content, compelling the removal of content, and punishing those responsible through warnings or administrative or criminal penalties.

Internet purification operations initially concentrated on “obscene pornographic information (https://archive.ph/XjLEj)” [淫秽色情信息]. But between 2013 and 2022, the focus of these special operations as stated in annual and semi-annual announcements widened to include a broader range of legally or politically prohibited content. An aggregate list of the targets of internet purification campaigns mentioned in these announcements is provided in Figure 2. Prohibited content mentioned in these announcements has recently included material which is “emotionally manipulative (https://archive.ph/AytbF)” [情感操控] (mentioned in 2020), “historical nihilistic (https://archive.ph/qjaIQ)” [历史虚无主义] (mentioned in 2021), or promotes “divination and superstition (https://archive.ph/3dM76)” [占卜迷信] (mentioned in 2022). An indication of the increasing breadth of these operations can be found in annual or semi-annual announcements made online by the Cyberspace Administration of China (https://archive.ph/E7N3Y) and the Ministry of Public Security (https://archive.ph/TAU6t) about the progress of these operations. These announcements include information of the kinds of prohibited content which authorities have identified and removed. It is not clear if these annual announcements provide a full list of the material authorities targeted for removal during the year in question. Nonetheless, these announcements make clear that state-led internet purification campaigns routinely identify and remove not only pornographic online material, but many other kinds of prohibited content listed in relevant legislation.

- Political rumors; historical nihilism; misusing the 100th anniversary of the founding of the Communist Party to engage in commercial activity; tampering with the history of the Party and the nation; slandering heroes and martyrs; opposing basic Constitutional principles; information which threatens national security
- Violence; weapons; terrorism
- Harmful material related to ethnic groups and religion; promotion of heterodox faiths, feudal superstitions, and online divination
- Pornographic and vulgar content; socially harmful material; flaunting wealth and money worship; emotionally manipulative websites and platforms
- Gambling
- Fraud; illegal collection, editing, and publishing of financial information; publication of false information; blackmail; illegally buying and selling bank cards; sale of rare and endangered animals and plants
- Illicit drugs
- False advertising; false job recruitment posts; underhanded “black public relations”; paid internet posters
- False pharmaceutical information; sale of counterfeit drugs; copyright infringement and counterfeiting
- Illegal surrogacy; dishonest marriage websites

- Unauthorized providing of online news services; fake news; misleading or false information on the epidemic situation in Beijing
- Managing disorderly fan communities and online user accounts

Figure 2 : Aggregate list of targets of special operations for internet purification mentioned in annual or semi-annual announcements, compiled from 2013 (https://archive.ph/XjLEj), 2014 (https://archive.ph/lO6TR), 2015 (https://archive.ph/4JIx5), 2016 (https://archive.ph/KyTkm), 2017 (https://archive.ph/E7N3Y), 2018 (https://archive.ph/Z1Pw4), 2019 (https://archive.ph/TAU6t), 2020 (https://archive.ph/AytbF), 2021 (https://archive.ph/qjaIQ), and 2022 (https://archive.ph/3dM76).

Beyond the targets of internet purification campaigns noted in Figure 2, further insight into what kind of online content is censored can be found on the Cyberspace Administration of China's Illegal and Undesirable Information Reporting Center (https://archive.ph/s8eir) [中央网信办（国家互联网信息办公室）违法和不良信息举报中心]. As part of the special operations for internet purification, the Cyberspace Administration of China encourages domestic internet users to make named or anonymous reports of prohibited "undesirable content" [不良信息内容] or "harmful information" [有害信息] through the Reporting Center. As part of the reporting process, users are asked to identify the kind of prohibited content they have found according to nine categories provided by the Reporting Center, which are listed in Figure 3: politics, violent terrorism, fraud and blackmail, pornography, vulgarity, gambling, rights infringement, rumors, and a broadly defined category of "other." The nine categories listed in Figure 3 broadly match both the kinds of content proscribed under Chinese government legislation and regulations covering online content, as well as the targets of internet purification special operations listed in announcements made by the Cyberspace Administration and the Ministry of Public Security.

- Politics
- Violent terrorism
- Fraud and blackmail
- Pornography
- Vulgarity
- Gambling
- Rights infringement
- Rumors
- Other, including: online borrowing and lending; online criminal activity; online commercial disputes; online false and illegal advertising; online extortion and post deletion; email and telephone harassment; intellectual copyright infringement; piracy; fake media and fake journalists; gang activity; online cultural market activity including music, performance, and animation; and telecommunications user services

Figure 3 : Categories of prohibited material listed by the Cyberspace Administration of China's Illegal and Undesirable Information Reporting Center.

Online announcements made by the Cyberspace Administration of China about the number of reports of prohibited content also suggest the kinds of content the Chinese state seeks to censor. These announcements arrange prohibited content into various categories, which only partially match those listed by the Reporting Center. Over the years these subcategories have included pornography, politics, vulgarity, gambling, rights infringement, rumors, terrorism, fraud, online extortion, paid post deletion (https://www.cyberctm.com/zh_TW/news/mobile/detail/2364079), and other forms of content.

We performed searches on Google and Baidu for terms associated with these announcements — "全国网络举报受理情况" [national situation of the handling of online reports] and "全国网络举报类型分布" [national distribution of categories of online reports] — during February and March 2023. We collected websites which provided breakdowns of the categories reports of prohibited content made by Cyberspace Administration offices across China ("全国各地网信办") and specific websites ("各网站"). We found some of these announcements on websites run by the national Cyberspace Administration of China (https://archive.ph/WOshY) or reporting websites run by provincial authorities (https://archive.ph/ISXed), while others were published on news media websites (https://archive.ph/cFadf).

These announcements do not appear to be consistently available, and we were only able to find ten announcements: nine monthly announcements released between January 2016 and January 2017, and one annual announcement for the year 2020, which are presented in Table 1. Nonetheless, the announcements which are available indicate the kinds of material that are reported and censored across platforms and websites in China. In addition, these announcements provide statistical information on the number of reports of prohibited content per category. We have provided a breakdown of this statistical data in Table 1. Based on the statistical data contained in these announcements, the majority of reported prohibited content is pornographic, followed by either political content or "other" material which does not fall into any of the other categories.

	2016 Jan (https://archive.ph/ISXed)	**2016 May (https://archive.ph/4**
Pornography	64.7	60.4
Politics	8.9	12.9
Vulgarity	n/a	n/a
Gambling	1.4	1.3
Rights Infringement	2.5	5.7
Rumors	n/a	n/a
Terrorism	0.1	2.1
Fraud	4.5	8.2
Online Extortion and Paid Post Deletion	0.2	0.1
Other	17.7	9.3

Table 1: For announcements spanning 2016 to 2020, the % of reports in that announcement spanning each prohibited online content category. Archived copies for these announcements are linked through the respective date.

Other Chinese government announcements give an indication of which platforms are responsible for hosting prohibited content. These reports provide monthly or annual totals of the number of pieces of prohibited content reported to the authorities, broken down according to the website or platform on which the content was found. Alongside warning, fining, or in other ways punishing companies for hosting prohibited content, these public reports have the function of naming and shaming companies for failing to fully comply with Chinese laws on online content management.

Platform	# of Reports
Weibo	53.126 million
Baidu	25.961 million
Alibaba	11.689 million
Kuaishou	6.59 million
Tengxun	6.309 million
Douban	3.514 million
Zhihu	2.143 million
Jinri Toutiao	2.063 million
Sina Wang	934,000
Sogou	331,000

Table 2: For different Internet platforms, the number of reports of prohibited content for 2021 (https://archive.ph/w4h0x).

The most recent announcement we found concerning reports of prohibited content broken down by platform is for the year 2021. The statistical data contained in this announcement, presented in Table 2, indicates that Weibo was subject to the majority of reports of prohibited content with 53.126 million reports, followed by Baidu (25.961 million) and Alibaba (11.689). The ten platforms listed in Table 2 account for roughly 110 million reports. According to the government announcement from which these data come, these 110 million reports are 75.6% of the 166 million reports of online prohibited content made in 2021.

Related work

There is a large body of previous research analyzing search platform censorship in China. Much of the earliest work focused on comparing censorship across web search engines accessible in China. In 2006, Reporters Without Borders tested (https://rsf.org/en/test-filtering-sohu-and-sina-search-engines-following-upgrade) by hand six keywords across multiple search engines accessible in China, finding that Yahoo returned the most pro-Beijing results among the first ten results compared to other search engines. In the same year, Human Rights Watch tested (https://www.hrw.org/sites/default/files/reports/china0806webwcover.pdf) by hand 25 keywords and 25 URLs, finding that Baidu and Yahoo were the most censored. This earliest work was limited in analyzing keyword-based censorship by attempting to characterize and compare the top *n* results for a searched keyword.

This type of analysis is limited due to its subjectivity and its inherent assumption that the search engine with the most politically sensitive results must be the least censored when there may be other explanations for fewer sensitive results than the application of censorship rules.

In 2008, in a follow up to the previous studies, Citizen Lab researchers tested (https://citizenlab.ca/wp-content/uploads/2011/08/nartv-searchmonitor.pdf) 60 hand-picked keywords across multiple search engines using an approach in which search queries were formed by combining a keyword with a web domain preceded by the "site:" operator to determine which domains were censored from the results of which keywords. Of all of the previous work we review, this work is the closest to ours. However, there are nevertheless fundamental differences. The work, like its predecessors, was limited to small sample sizes and relies on hand-picked samples. More importantly, its methods also cannot differentiate between a search query which is censored and one that genuinely has no results. While this may not seem significant in the context of testing hand-picked keywords, in our work we develop a method which can test whether a string of text triggers a censorship rule even when it would ordinarily return no results, and our method can isolate the exact keyword or keywords present in that string which are triggering its censorship. This capability was necessary for bridging the gap between testing lists of curated keywords versus testing long strings of arbitrary text, which is a necessary component for automated and ongoing testing of strings of text from sources such as news articles.

In a 2011 work, to instrument automated and ongoing censorship testing, Espinoza et al. developed a novel method using named entity extraction (https://en.wikipedia.org/wiki/Named-entity_recognition) to select (https://www.cs.unm.edu/~amajest/foci11.pdf) interesting keywords from a long string of news article text to use in search engine testing. Specifically, their method was designed to extract certain nouns, namely, the names of people, places, and organizations. The significance of this work is that it facilitates automatic censorship testing which does not rely on hand curation of keywords but instead can take as input long strings of arbitrary text, such as from news articles, automatically selecting from that text certain keywords to test. However, it is limited in that it makes assumptions about what type of content is likely to be sensitive, namely, certain kinds of nouns, and was used to test keywords for censorship individually. In contrast, we have found that censorship rules often require the presence of multiple, typically related keywords and commonly consist of a variety of parts of speech. Instead of selecting interesting keywords from a long string of text to test individually, our method tests a long string of text for the presence of censored content as a whole, even if it would not otherwise have any search results. We can then, using additional search queries, isolate the exact keyword or keywords triggering the censorship of that text. Our method is completely agnostic to and requires no assumptions concerning parts of speech, semantics, word boundaries, or other aspects of language and effortlessly generalizes to Chinese, English, Uyghur, and Tibetan languages, among others.

In another 2011 work, Zhu et al. use automated methods to test (https://arxiv.org/pdf/1107.3794.pdf) curated keywords consisting of the 44,102 most-searched keywords on Baidu and Google.cn, 133 keywords known to be censored by China's national firewall, 1,126 political leaders of the Chinese government, and 85 keywords chosen by hand based on current events. This work is to our knowledge the first to speculate about the existence of different "white lists" of domains allowed to appear in the results for censored queries, whereas previous work has been framed in measuring which domains were blocked. In our work, we confirm the existence of these lists of authorized domains and attempt to quantify how many different lists exist, characterize when each list is applied, and measure which domains appear on each one.

More recently, in 2022 Citizen Lab researchers analyzed (https://citizenlab.ca/2022/05/bada-bing-bada-boom-microsoft-bings-chinese-political-censorship-autosuggestions-north-america/) Microsoft Bing's autosuggestion system for Chinese-motivated political censorship, finding that not only was it applied to users in mainland China but that it was also applied, partially, to users in North America and elsewhere. While this work is unlike ours in that it analyzed for Chinese censorship queries' autosuggestions as opposed to the queries' results proper, it is related to our work in that it studies the censorship of Bing, the only remaining major non-Chinese web search engine accessible in China.

Most recent work studying search platform censorship in China has analyzed the search censorship performed by social media platforms, namely that of Chinese microblogging platform Sina Weibo. For instance, in 2014, as part of the ongoing Blocked on Weibo (http://blockedonweibo.com/) project, Ng used automated methods to test (https://citizenlab.ca/2014/11/tracing-path-censored-weibo-post-compiling-keywords-trigger-automatic-review/) for the censorship of 2,429 politically sensitive keywords previously curated (https://docs.google.com/spreadsheet/ccc?key=0Aqe87wrWj9w_dFpJWjZoM19BNkFfV2JrWS1pMEtYcEE) by China Digital Times, finding that 693 were censored with explicit notifications. In a follow-up study months later, Ng found that most of these no longer had explicit censorship notifications but still returned zero results. Ng speculated that this may be due to either the removal of keywords from search censorship which were still being applied to post deletion censorship or due to Weibo transitioning to a more covert form of censorship. Our findings in this report suggest that both hypotheses for his findings could be true, as in Appendix A we demonstrate a method for evading Weibo search censorship but which often still yields zero results due to a simultaneous application of search censorship rules to post deletion, but also much of our analysis of Weibo focuses on a form of soft censorship which subtly restricts which results can appear for sensitive queries.

Often work looking at Weibo censorship is ad hoc and non-methodological, performed quickly in response to ongoing events, often to be featured in news articles or social media. For example, in 2017, Citizen Lab researchers studied (https://citizenlab.ca/2017/07/analyzing-censorship-of-the-death-of-liu-xiaobo-on-wechat-and-weibo/) Weibo search censorship of human rights advocate Liu Xiaobo leading up to and in the wake of his passing. They found that censorship of his name and surrounding topics intensified immediately following his passing but eventually returned to baseline levels. In our work we facilitate a method to automatically and methodologically detect search censorship rules introduced in response to developing news events with the intention to aid such rapid investigations.

In response to a 2022 incident in which Canadian Prime Minister Justin Trudeau had a heated, public conversation (https://www.bbc.com/news/world-asia-china-63654337) with Chinese President Xi Jinping, journalist Wenhao Ma tweeted (https://mobile.twitter.com/ThisIsWenhao/status/1593056079403167750) his discovery that "特鲁多" [Trudeau], "小土豆" [little potato] (a Chinese nickname for Trudeau), and the English word "potato" were censored by Weibo search. We highlight this example for two reasons. First, Ma identified these keywords as being censored even though they had search results because their search results seemed to only contain results from official accounts with blue "V" insignia, recognizing that Weibo was applying a more subtle, softer form of censorship compared to simply displaying zero results. In our work, we develop a method to measure unambiguously when such keywords are subject to this type of censorship without attempting to glean it from the number of results from official accounts. Second, however, Ma's claim that the English word "potato" was censored by Weibo was, while correct, misleading in that its censorship had nothing to do with Trudeau or potatoes but because it contains the substring “pot”, a slang term for marijuana. To avoid this type of inadvertent misattribution, in our work, we use a carefully designed algorithm to extract the exact keywords or combination of keywords triggering the censorship of a string of text.

Model

In previous work (https://www.usenix.org/system/files/foci19-paper_xiong.pdf) studying automatic censorship of messages on WeChat, we determined that WeChat automatically censors messages if they contain any of a number of blocked keyword combinations, and we had defined a keyword combination as a set of one or more keywords such that, if each keyword in the combination was present somewhere in a text, the text would be censored. For instance, if WeChat censors the keyword combination {“Xi”, “Jinping”, “gif”}, then any message containing all of these keywords, anywhere in the message, in any order, is censored. Thus, this combination would censor “Xi Jinping gif” and “gif of Xi Jinping” but not “Xi gif”. In this model, keywords can overlap as well, so even “Xi Jinpingif” would be censored since it contains the strings “Xi”, “Jinping”, and “gif” somewhere in the message, although the latter two overlap.

To our knowledge, this manner of modeling WeChat’s automated chat censorship rules as a “list of unordered sets” of blocked keywords completely captured WeChat’s censorship behavior. However, other censorship systems fitted with different censorship implementations may not be able to be adequately modeled using this model. For instance, a “list of ordered sequences” censorship system might require that the keywords appear in a specific order. For example, the rule (“Xi”, “Jinping”, “gif”) would censor “Xi Jinping gif” but not “gif of Xi Jinping”. A censorship system which implemented rules as a series of regular expressions (https://en.wikipedia.org/wiki/Regular_expression) would not only require the keywords to appear in an order but also that they not overlap. For example, the regular expression /Xi.*Jinping.*gif/ would censor “Xi Jinping gif” but neither “gif of Xi Jinping” nor “Xi Jinpingif”. Finally, a censorship system might use some machine learning algorithm to classify which queries to censor. However, we have not previously observed such systems used to perform real-time, political censorship, likely due to the requirements of such a system to operate with low false positives and to possess a nuanced, day-by-day understanding of what content is politically sensitive.

To attempt to capture the censorship behavior of as many search platforms as possible, in the remainder of this work we chose to use a “list of ordered sequences” model as in doing so we are being as conservative in our assumptions as possible. For instance, by using ordered sequences, we can still model unordered rules, although this may require multiple ordered sequences to capture every possible permutation (e.g., (“Xi”, “Jinping”, “gif”), (“gif”, “Xi”, “Jinping”), etc.). In our model we allow for the possibility that keywords triggering censorship in a query may be overlapping, but by facilitating this possibility we can still measure systems where keywords cannot.

Throughout the remainder of this work, we use the term *keyword combination* to refer to such a “list of ordered sequences”, and we will express them as keywords separated by plus signs, e.g., “Xi + Jinping + gif”. Later in our work, we reflect on this model more. In our “Methodology” section, we explain exactly how we measure which sequence of keywords is triggering the censorship of a censored query, and in our “Results” section we reflect on how effective our model performed in capturing the actual censorship behavior of the search platforms which we measured.

Methodology

In this section we describe our overall experimental methodology and then detail the methodologies of three different experiments which we perform.

Search platforms analyzed

We aimed to analyze the most popular platforms across different kinds of Internet platforms ranging from web search engines and e-commerce platforms to social media sites. Overall, we selected to analyze eight different search platforms, including three web search engines, four varying types of social media network, and one e-commerce platform (see Table 3 for the full list).

Website	Description	Object o
Baidu	Web search engine	Web page r
Baidu Zhidao	Q&A platform	Q&A post re
Bilibili	Video sharing platform	Video result
Bing	Web search engine	Web page r
Douyin	Operated by TikTok's ByteDance, the version of TikTok accessible from mainland China	Video result
Jingdong	E-commerce platform	Product rec
Sogou	Web search engine	Web page r
Weibo	Microblogging site similar to Twitter	Microblog r

Table 3: The search platforms that we analyzed and the object of censorship which we measured on them.

Notably, our selection includes one platform not operated by a Chinese company — Microsoft Bing — whereas the remaining are all operated by Chinese companies.

Measuring whether a query is censored

When a user using a search platform searches for a query, this query is sent to a server. If the query is not censored, the server will respond with the corresponding matches to the query. However, with a censored query, there are two possibilities depending on the search platform:

1. The server returns a unique notification when the user's query contains sensitive content. We call this *transparent* censorship because the signal is unambiguous.
2. The server spuriously omits some or all search results despite that content matching the user's query. We call this *opaque* censorship due to there existing an ambiguity as to whether the query was censored or whether those matches never existed.

For search platforms which employ transparent censorship, measuring whether a query is censored is straightforward: test the query and check if there is a notification that the query is censored. However, for search platforms which censor opaquely, we were required to employ a more sophisticated methodology to distinguish between cases where there are genuinely zero matches and cases of opaque censorship. In the following section we discuss the method we used to distinguish between these cases.

Measuring whether a string of text is opaquely censored

On platforms which employ opaque censorship, in order to distinguish between cases where there are genuinely zero matches and cases where matches exist but are being opaquely censored, we use a technique of creating test queries for a string of text such that they should always return matches unless the string of text is censored, tailored to each platform. We call such a modified query a *truism*, which Wikipedia (https://en.wikipedia.org/w/index.php?title=Truism&oldid=1119858100) defines as "a claim that is so obvious or self-evident as to be hardly worth mentioning, except as a reminder or as a rhetorical or literary device". Our truisms are search queries which should obviously return results but are used as devices to unambiguously detect the presence of censorship of a string of text.

As an example, on Baidu Zhidao, we create a truism by surrounding the string in question with "the -(" before the string and ")" after the string. Thus, for Baidu Zhidao, to test the string "习近平" we would test the truism "the -(习近平)". On Baidu Zhidao this syntax indicates to the search platform to logically negate whatever is in between the parentheses and can be interpreted as searching for all results containing "the" which do *not* contain "习近平". In the case of Baidu Zhidao and many other platforms, we have discovered that even content which is negated in a query can still trigger the query's censorship.

Website	Transformation	
Baidu	"site:com.cn␣-(" + *string* + ")"	Since there is no character or string which is present on every web pa
Baidu Zhidao	"the␣-(" + *string* + ")"	Since posts exist containing "the", this query requesting pages contai
Bilibili	*string*	Transparent censorship (although Bilibili does not report a censorshi
Bing	"microsoft␣|␣" + *string*	Since web pages exist containing "microsoft", this query requesting pa
Jingdong	*string*	Transparent censorship (although Jingdong does not report a censors
Sogou	"site:com.cn#齉" + *string*	Although Sogou does not support disjunction (X | Y) or negation (-X), w
Weibo	*string*	Transparent censorship (Weibo displays a censorship notification)

Table 4: Rules for transforming a query for string *to a truism testing for censorship of* string *such that* string *is censored if and only if its corresponding truism returns zero results.*

As another example, while Baidu Zhidao and many other platforms seemed to naively scan queries for the presence of strings to trigger censorship, Bing's censorship system seemed clever enough to not allow the content of negated content to trigger censorship. However, we were still able to create a truism on Bing by searching for "(microsoft | 习近平)". On Bing this syntax indicates to the search platform to return results that contain either "microsoft" or "习近平". Since we know that there exist pages on the Internet containing "microsoft" and since "microsoft" is not censored, then, if there are no results, it must be because "习近平" is censored. See Table 4 for the rules which we used to create truisms to test each site employing opaque censorship.

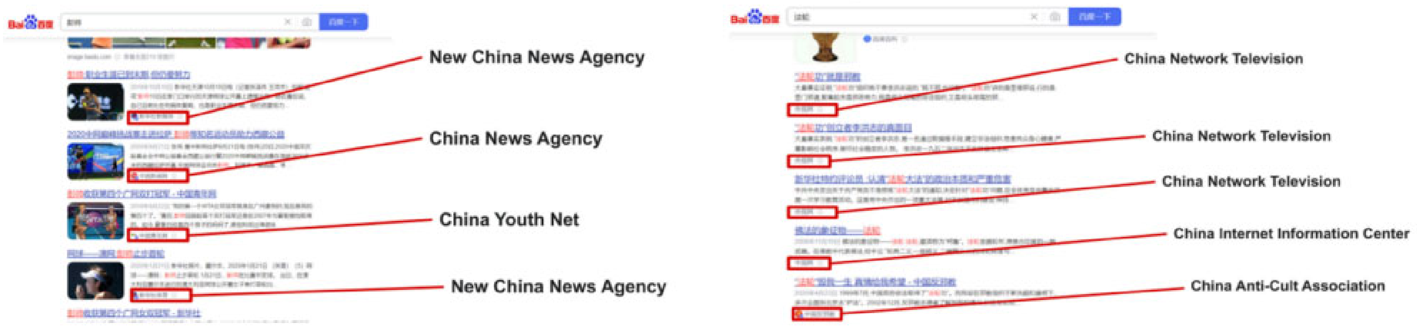
Although we could theoretically construct such queries, note that truisms are not necessarily *tautological*, i.e., they are not guaranteed to return results *a priori*. For instance, we could construct a query "(习近平 | -习近平)" which would request any result that either contains 习近平 or does not contain 习近平 (i.e., every result). However, in our testing search platforms did not seem designed to recognize such queries as tautologies and often the results would be logically inconsistent (e.g., "习近平" reporting more results than "(习近平 | -习近平)"). As such, by "truism" we refer to queries which when not censored are merely certain to return results in practice although not necessarily *a priori*.

Since whitespace and punctuation characters can induce unpredictable behavior on censorship systems and because it can potentially interfere with the syntax added by our truisms, we strip all whitespace and punctuation from strings before testing. While it is possible that by performing this practice we may be failing to discover some censored rules which require punctuation, we found that in our previous study of WeChat that WeChat strips whitespace and punctuation from messages before testing them for censorship and that failing to strip these characters ourselves resulted in the spurious inclusion of them in our results. Therefore, out of caution, because we prefer accuracy of our results over the possibility of a slightly larger size of results, we strip whitespace and characters from our test strings before testing.

By using the method described in this section of testing using truisms, we can be certain that if our query does not have any returned matches then it must be due to the result of censorship. Thus far, we have discussed how we measure *hard* censorship, that is, censorship which denies the user from any matches. However, in this following section, we discuss how to measure a more subtle form of censorship in which the matches may be partially censored.

Measuring whether a query is partially censored

Across the three web search engines we tested, many queries which did return results only returned results linking to websites which were Chinese state-owned or state-approved media outlets (see Figure 4 for an illustration).



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/04/Wire-2023-04-24-at-3_47-PM.png&nocache=1)

Figure 4: On Baidu, an example of a query whose results are only from Chinese state media.

Moreover, for some social media search platforms, we noticed that, for some queries that did return results, these results seemed to be only from accounts which have received a certain amount of verification or approval. We call this type of censorship in which results are only allowed from authorized sources *soft* censorship and censorship in which no results are allowed *hard* censorship (see Table 5 for a breakdown of each platform we discovered performing soft censorship).

Website	Soft censorship
Baidu	Only shows results from authorized domains (typically Chinese government sites, Chinese state media,
Bing	Only shows results from authorized domains (typically Chinese government sites, Chinese state media,
Douyin	Only verified accounts
Sogou	Only shows results from authorized domains (Chinese government sites, Chinese state media, etc.)
Weibo	Only verified accounts

Table 5: Platforms which we discovered performing soft censorship and the manner in which they perform it.

To detect this form of soft censorship, for each web search engine, we modified its truism by restricting the results to only be allowed from unauthorized sources. For example, on Baidu, we only allow results from microsoft.com, a site we chose because it is both popular and accessible in China but foreign operated and unlikely to be pre-approved for voicing state propaganda. For Baidu, we surrounded the tested string with "site:microsoft.com -(" on the left and ")" on the right in order to transform it into a truism and test it for soft censorship but with the restriction that results were only allowed from an unauthorized source. Thus, for the string "彭帅", we would test the truism "site:microsoft.com -(彭帅)", which can be interpreted as searching for any page on microsoft.com not containing "彭帅". See Table 6 for the rules which we used to create truisms to test each site employing soft censorship.

Website	Transformation	
Baidu	"site:microsoft.com␣-(" + *string* + ")"	Same as in Table 4 except restricted to microsoft.com, ar
Bing	"site:microsoft.com␣(microsoft␣|␣" + *string* + ")"	Same as in Table 4 except restricted to microsoft.com, ar
Douyin	*string* + "␣‰‰"	Douyin normally displays results for any query, no matte
Sogou	"site:microsoft.com#" + *string*	Same as in Table 4 except restricted to microsoft.com, ar
Weibo	"‰‰␣-(" + *string* + ")"	Only non-verified accounts have posted the string "‰‰

Table 6: Rules for transforming a query for string *to a truism testing for soft censorship of* string *such that* string *is soft censored if and only if its truism returns zero results.*

Notably, although many sensitive queries on Douyin returned zero results, we did not find any evidence of hard censorship on Douyin that could not be explained by the soft censorship system which we explain in Table 6. As such, on Douyin, we only measure its soft censorship system.

Isolating which keywords are triggering censorship

Thus far we have discussed how to determine whether a string of text is either hard or soft censored across each of the search platforms which we tested. However, given that a string of text is censored, we still desire to know which keyword or combinations of keywords present in that text are responsible for triggering its censorship. In this section, we outline the method we employ of *isolating* which combination of keywords is triggering a text's censorship by making additional queries.

To isolate keywords triggering censorship of a string of text, we make use of an algorithm called CABS which we originally introduced (https://www.usenix.org/system/files/foci19-paper_xiong.pdf) in 2019 and continue to maintain here (https://github.com/citizenlab/censored-keyword-isolation). Our original algorithm was motivated by discovering censored keyword combinations on WeChat, which we modeled as a "list of unordered sets", but, as we model censorship in this work as a "list of ordered sequences", we adapted (https://github.com/citizenlab/censored-keyword-isolation/blob/master/algorithms-left-ordered.py) the algorithm to fit this model. Fortunately the changes required were trivial, essentially replacing all sets and set operations with tuples and their corresponding tuple operations (e.g., set union is replaced with tuple concatenation). To fully understand the algorithm and to access its code, we recommend visiting the previous links in this paragraph. However, in the remainder of this section we will briefly outline the intuition behind how this isolation algorithm works.

The algorithm works by performing bisection and attempting to truncate as much of the text being isolated at a time while preserving the property that it is still censored. For example, initially it will attempt to remove the second half of the text and measure if it is still censored. If it is, then it will attempt to remove the last three quarters of the text. If it is not, then it will attempt to remove only the last quarter of the text. By iteratively repeating this procedure, the algorithm eventually discovers the final character of one of the keywords triggering the censorship of the string. It next attempts to discover the first character of this keyword. Once the complete keyword is discovered, the algorithm tests if the keyword it has discovered thus far is sufficient to trigger censorship. If not, it repeats this process of finding another keyword in the censoring keyword combination on the remaining text up to but not including the final character of the keyword most recently discovered. It repeats this process until enough keywords have been discovered to trigger censorship, producing the censored keyword combination in its entirety.

There are, as it turns out, many subtleties to doing this correctly and efficiently, especially when keywords can overlap or when there may be present multiple keyword combinations triggering censorship. However, through careful design and testing, our algorithm is correct even in the presence of such corner cases.

Website	Character	
Baidu	"‰"	Efficiently encoded in GB18030, the encoding under which our testing query length on B
Baidu Zhidao	"‰"	Efficiently encoded in GBK, the encoding under which our testing query length on Baidu
Bilibili	"😃"	Sufficient to separate keywords.
Bing	"😃"	In our testing, we found that different join characters could produce different results, su
Douyin	"😃"	Sufficient to separate keywords.
Jingdong	"␣"	Sufficient to separate keywords.

Sogou	“齉”	Efficiently encoded in GB18030, the encoding under which our testing query length on S

Table 7: For each tested search platform the “join” character that is used when isolating the combination of keywords triggering the censorship of a string of text.

The one way in which the algorithm must be adapted to a given search platform is by choosing a “join” character. This selection is necessary as not every platform considers the same characters as splitting a keyword. For instance, on one platform, putting spaces in between the characters of a censored keyword may not prevent it from being censored but on another it may. A desirable “join” character for a platform is one whose insertion into a censored keyword would prevent it from censoring but also one that it is unlikely to appear in censored keywords that we wish to measure and that can be encoded efficiently in whatever character encoding a search platform internally uses. For a breakdown of the “join” characters that we used for each tested search platform with corresponding motivations, please see Table 7.

By using this algorithmic technique, we can determine the exact keyword or combination of keywords necessary to trigger censorship of a censored string of text. The results are not statistical inferences, approximations, or in any way probabilistic. Moreover, the algorithm is agnostic of and makes no assumptions concerning language, including concerning parts of speech, semantics, word boundaries, or other aspects of language, and it effortlessly generalizes to Chinese, English, Uyghur, and Tibetan languages, among others.

Overcoming testing hazards

During the preliminary design and testing of our methods, we observed that our methodology would need to overcome multiple hazards in order to provide thorough and accurate results, including captchas, various restrictions on query length, and inconsistent results returned by search platforms. Below we outline how we overcome these hazards.

Captchas

We found that, after a period of automated testing, Sogou and Baidu began displaying captchas instead of displaying search results until the captchas were solved. We did not investigate attempting to solve the captchas automatically. However, for Sogou, we found that whenever presented with a captcha we could restart the browser session to resume testing for some substantial period of time until the next captcha appeared, at which point we could simply restart the browser session again. For Baidu, restarting the browser session was typically ineffective. However, we found that solving a captcha would allow a browser session to test for 24 hours uninterrupted by captchas. Thus, to instrument Baidu’s testing, every 24 hours we manually solve a captcha for each browser session, requiring only seconds of manual intervention each day. However, if Baidu’s captcha displays became more frequent or if we wanted to completely automate the testing, future work might look at applying software designed to automatically solve these captchas.

Douyin also displayed captchas. However, unlike with Sogou and Baidu, even after solving Douyin’s captchas, repeated search querying would inevitably begin yielding zero results for any search query, regardless of its sensitivity. As such, we were not able to complete every experiment with Douyin, as we stopped testing it early in our analysis due to this limitation.

Query length limitations

The search platforms we tested have limitations in the length of query which we could test. Exceeding these limits had various consequences, such as the platform returning an error message, silently truncating the query, or all content beyond the limit evading censorship. As such, for each platform, we performed testing to determine the value of any applicable limit. As characters can take varying space in different representations or encodings, we also had to determine the unit of the limit, which we found to vary across platforms as being a function of the number of raw Unicode characters or the number of bytes in some character encoding such as UTF-8, UTF-16, GB18030, etc. (see Table 8 for a complete breakdown).

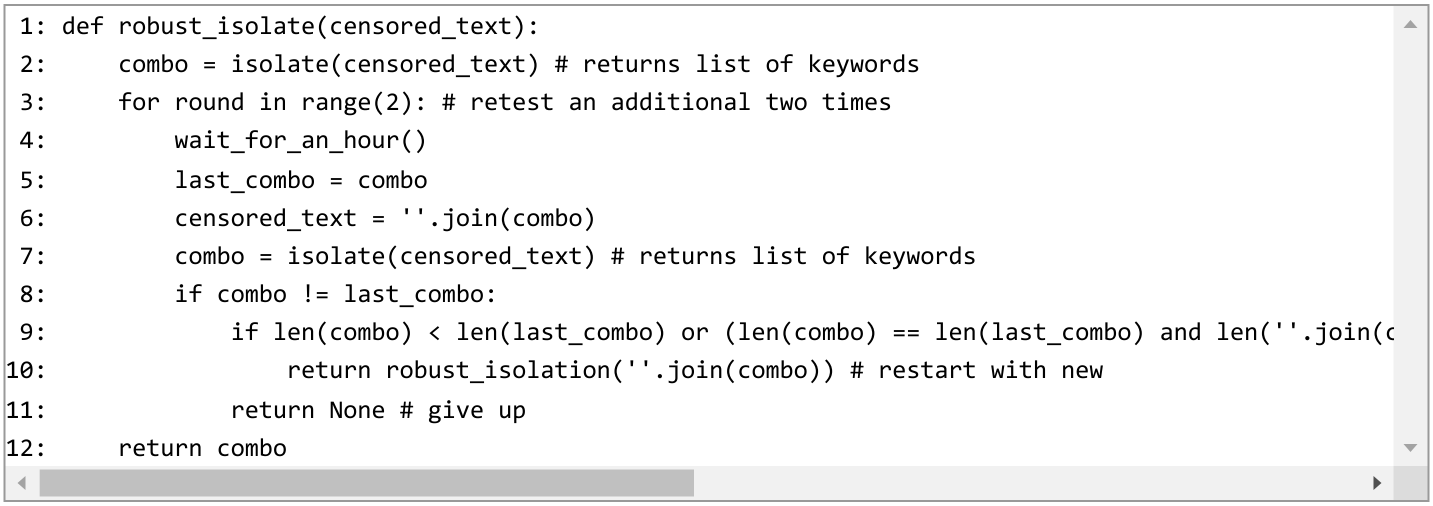
Website	Maximum query length	Encoding and unit
Baidu	76	GB18030 bytes
Baidu Zhidao	76	GBK bytes
Bilibili	33	Unicode characters
Bing	150	UTF-8 bytes
Douyin	202	UTF-16 bytes
Jingdong	80	Unicode characters
Sogou	80	GB18030 bytes
Weibo	40	GB18030 bytes

Table 8: For each search platform, the maximum query length we used in testing.

Our code was written to ensure that queries were never tested which exceeded a platform’s limits to ensure the reliability of our results.

Inconsistent search results

We observed inconsistencies in the search results with some search engines during our testing. When we searched for a truism for the first time, we found that some platforms would occasionally return no results for a truism, even if it is not censored. Testing it again would yield results. We hypothesize that the eccentric queries which we construct would sometimes overwhelm the search platform but, once it had sufficient time to be primed, it would then return results for subsequent searches using that query. For other platforms, we also observed cases in which it seemed that we would see a small number of censorship rules being applied inconsistently. We hypothesize that such inconsistent observations may have resulted from load balancing between servers with small differences between the censorship blocklists with which they had been deployed. In any case, to make our measurements robust to these and other inconsistencies, we apply the following algorithm, expressed below in Python-like pseudocode, which effectively retests a potential keyword combination an additional two times over the span of three hours before considering it a censored keyword combination:



```
def robust_isolate(censored_text):
    combo = isolate(censored_text) # returns list of keywords
    for round in range(2): # retest an additional two times
        wait_for_an_hour()
        last_combo = combo
        censored_text = ''.join(combo)
        combo = isolate(censored_text) # returns list of keywords
        if combo != last_combo:
            if len(combo) < len(last_combo) or (len(combo) == len(last_combo) and len(''.join(c
                return robust_isolation(''.join(combo)) # restart with new
            return None # give up
    return combo
```

In this code, in the event that we discover an inconsistent result, we do one of two things depending on how the new result compares to the previous one. If, compared to the previous result, the new result's keyword combination has either fewer constituent keywords or if it both has the same number of constituent keywords but the sum of the lengths of each of its constituent keywords is less than those of the previous result, then we restart the robust isolation process from scratch on the new keyword. Otherwise, we simply give up attempting to isolate the triggering keyword combination from the given censored string. We have this rule in place to ensure that the isolation of the keyword combination is making some measure of progress, in either having fewer keywords or in having the same number of keywords but shorter ones. This policy ensures that, in an environment where servers may be giving inconsistent results, the algorithm still terminates, either by eventually returning a reliable result or by failing. Although we did not collect data specifically pertaining to this matter, we believe from casual observation that such failures are exceedingly rare and occur only when nothing else could have been easily done to obtain a reliable result.

Experiments

In this work we perform three experiments using different sampling methodologies to address different research questions that we had. In our first two experiments, we test search platforms for the censorship of people's names and of known sensitive content, respectively. We also present a third, ongoing experiment from which we already have preliminary results, in which we test text for censorship from daily news sources. In the remainder of this section we set out the design of these three experiments in greater detail.

Experiment 1: Measuring censorship of people's names

In our first experiment we test people's names. Individuals or their names have the following desirable properties:

- Individuals can represent highly sensitive or controversial issues.
- Unlike more abstract concepts, a comprehensive sample of notable people and their names can be automatically curated and enumerated into a large test list.

- As opposed to a list of handpicked keywords or a list of sensitive keywords censored in other Chinese products, a list of people's names is not biased toward the sort or style of keywords censored in other Chinese products or toward a researcher's preconceptions.

To facilitate this experiment, we used a list of 18,863 notable people whose names which we had previously curated from Wikipedia in 2022. The manner in which we curated these is spelled out in a previous report (https://citizenlab.ca/2022/05/bada-bing-bada-boom-microsoft-bings-chinese-political-censorship-autosuggestions-north-america/#methodology), but, at a high level, these names were collected from Wikipedia by looking for people whose articles had a sufficiently high number of Wikipedia views and whose names had a sufficiently high amount of search volume on Microsoft Bing. While this list of notable names inevitably contained the names of famous Chinese politicians, political dissidents, and others whom we might expect to be the targets of censorship, the criteria through which we selected these names was designed to be unbiased and to also produce names for testing whose censorship we might not expect with the intention that we find surprising results.

In this experiment we test each person's name individually. For each name on this list, to generate a test string, we take the person's name as expressed in the Wikipedia article title and append, if different, the name in simplified Chinese characters and append, if different, the name in traditional Chinese characters, forming a final test string of between one and three variations of the name concatenated together. If in testing we find that the test string is censored, we then use our isolation algorithm to isolate a keyword combination triggering its censorship.

While isolating the triggering keyword combination may not seem necessary when individually testing keywords such as people's names, as it might seem apparent that sensitivity of that person's name must be responsible for triggering the censorship, we found it helpful in discovering cases where names were collaterally censored, either by accidentally containing another part of another censored name (e.g., "习" [Xi]), or by accidentally containing other sensitive characters triggering its censorship (e.g., "伍富橋" [Alvin Ng] censored due to containing the character "橋" [bridge] following the Sitong Bridge Protests).

During this experiment, for each platform tested, we record each censored name and the keyword combination triggering its censorship.

Experiment 2: Measuring censorship of known sensitive content

In our second experiment we test from a compilation of known sensitive content. Previous work has shown that, to comply with Chinese censorship regulations, companies are generally responsible (https://www.usenix.org/conference/foci11/three-researchers-five-conjectures-empirical-analysis-tom-skype-censorship-and) for curating (https://firstmonday.org/ojs/index.php/fm/article/view/4628/3727) their own (https://www.usenix.org/conference/foci15/workshop-program/presentation/knockel) censorship lists (https://www.usenix.org/conference/foci17/workshop-program/presentation/knockel) and that lists used by any two companies will, on average, have little overlap (https://www.cs.unm.edu/~jeffk/publications/jeffs-dissertation.pdf). However, due to the onerous task of compiling these lists, which may contain tens of thousands of keywords or more, companies are often reluctant to invest the resources required to develop their own lists, instead opting to use whatever lists that might be most easily available. Software developers have been known to take censorship lists with them (https://www.usenix.org/conference/foci15/workshop-program/presentation/knockel) when leaving companies and to later use them in new products. Furthermore, when comparing a list across a database consisting of as many as thousands of other previously discovered Chinese censorship lists, it can be possible to find one or more lists (https://citizenlab.ca/2021/08/engrave-danger-an-analysis-of-apple-engraving-censorship-across-six-regions/#derivation-of-mainland-china-keyword-list) from which the list in question may have been derived (or lists which may have been derived from the list in question) due to an amount of overlap unexplainable by chance. Therefore, testing from a large sample of other products' lists can be an effective way to find what another product is censoring.

As such, in our second experiment, we sample tested by drawing from a database of thousands of Chinese censorship lists (https://github.com/citizenlab/chat-censorship) previously discovered on other platforms consisting in aggregate of 505,903 unique keywords. Instead of testing keywords individually, we treated the entire database as a large text by concatenating the unique keywords together ordered by frequency and secondarily lexicographically. By treating the database as a single, large text, we were able to test more content at once, limited only by each search platform's limitations on query length, decreasing the time required to test and increasing the chance of discovering keyword combinations consisting of more than one keyword. When we discover a censored string of text, we isolate its triggering keyword combination and record it. We then resumed testing at the character after the censored keyword combination's earliest character (i.e., after the keyword combination's earliest keyword's earliest character).

Experiment 3: Ongoing testing from news articles

In our third experiment, we test from news articles in a perpetual, ongoing fashion. Our motivation for choosing news articles is that they are easy to collect, contain words related to current events, and often cover politically sensitive topics. Furthermore, they may be directly the desired object of inquiry on a web search platform or the object of discussion on a social media network, as we found many titles of or long phrases in news articles censored on search platforms.

To facilitate this experiment, every 60 seconds, we check for and collect news articles from 16 different RSS (https://en.wikipedia.org/wiki/RSS) feeds spanning Mandarin, Cantonese, Tibetan, and Uyghur languages as well as editorial stances which range from expressly pro-Beijing to expressly critical of Beijing including those news sources with stances in between (see Table 9 for a complete list).

Source	Language
Botan (https://botanwang.com/rss.xml)	Mandarin
Boxun (https://boxun.com/feed)	Mandarin
China Digital Times (https://feeds.feedburner.com/chinadigitaltimes/IyPt)	Mandarin
Deutsche Welle Chinese (https://rss.dw.de/rdf/rss-chi-all)	Mandarin
Financial Times Chinese (https://www.ftchinese.com/rss/feed)	Mandarin
Mingpao (https://news.mingpao.com/rss/ins/all.xml)	Cantonese
New York Times Chinese (https://cn.nytimes.com/rss/)	Mandarin
People's Daily (https://www.people.com.cn/rss/politics.xml)	Mandarin
Radio France Internationale Chinese (http://cn.rfi.fr/general/rss/)	Mandarin

Radio Free Asia Cantonese (https://www.rfa.org/cantonese/rss2.xml)	Cantonese
Radio Free Asia Mandarin (https://www.rfa.org/mandarin/rss2.xml)	Mandarin
Radio Free Asia Tibet (https://www.rfa.org/tibetan/rss2.xml)	Tibetan
Radio Free Asia Uyghur (https://www.rfa.org/uyghur/rss2.xml)	Uyghur
Solidot (https://www.solidot.org/index.rss)	Mandarin
Voice of America Chinese (https://www.voachinese.com/rss/)	Mandarin
Voice of America Cantonese (https://www.voacantonese.com/api/)	Cantonese

Table 9: RSS news sources used in testing.

For the purposes of testing, we consider each article text a concatenation of its RSS title, description, and URL. On each search platform, we then test each article as much at a time as possible, as limited by the platform's maximum query length. As in Experiment 2, when we discover a censored string of text, we isolate its triggering keyword combination and record it, and we then resume testing at the character after the censored keyword combination's earliest character.

Experimental setup

We coded an implementation of our experiments in Python (https://www.python.org/) using the Selenium Web browser automation framework (https://www.selenium.dev/) and executed the code on Ubuntu Linux (https://ubuntu.com/) machines. We tested each search platform from a Toronto network except for Bing, which we tested from a Chinese vantage point using a popular VPN service. Experiment 1 was performed in October 2022. Experiment 2 was performed in February 2023. Experiment 3 began January 1, 2023, and is ongoing as of the time of this writing.

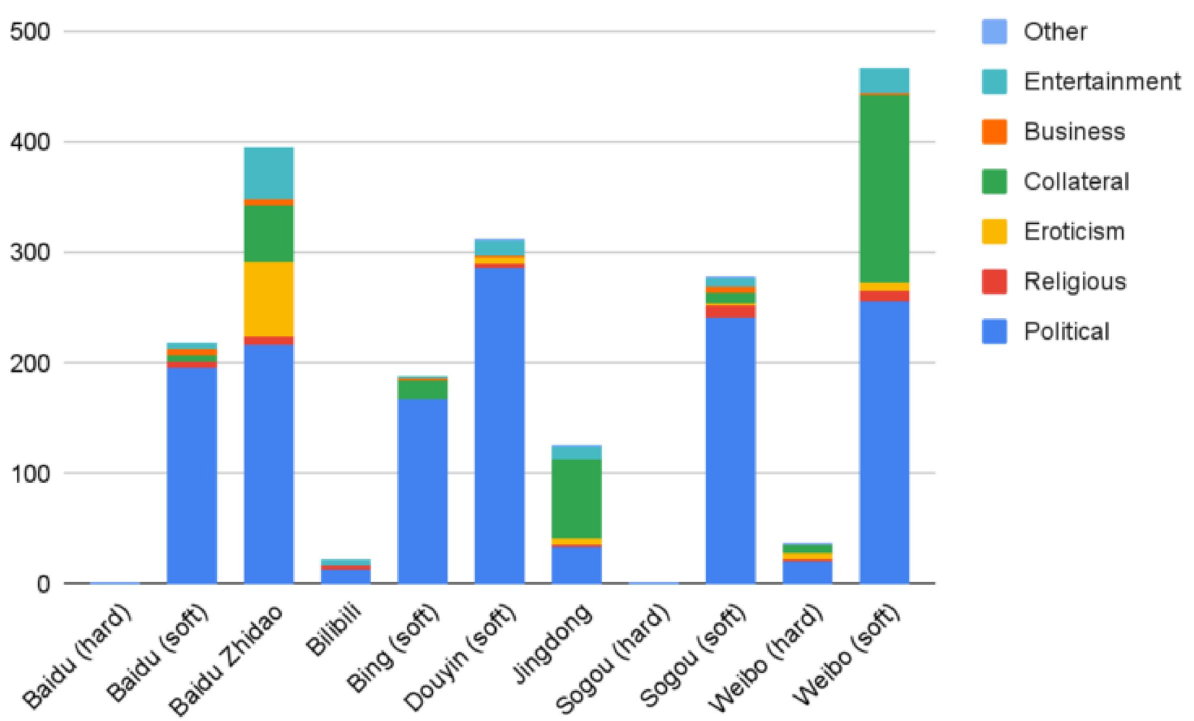
Results

In this section we detail the results of our first two experiments and present preliminary results from our third.

Experiment 1: Censorship of people's names

Among the 18,863 names tested from Wikipedia, we found a combined 1,054 unique names — over 1 in 18 — censored across the search platforms which we tested. Among the unique censored names, 605 were hard censored on at least one platform, and 449 were only ever observed to be soft censored. Among platforms which performed both hard and soft censorship, such platforms performed very little hard censorship, suggesting that they prefer to perform soft censorship when operators possess the capability. From the censors' perspective, soft censorship may be more desirable as the way in which it controls information is less obvious, but, from the platform operators' perspective, it may be also desirable, as it creates less friction during a user's interaction with the platform because a user, if receiving no results on one platform, may be tempted to try switching to another.

Among the platforms analyzed, we found Weibo to target the highest number of names (474) for some type of censorship, and among the web search engines, we found similar levels of censorship, with Sogou targeting 282, Baidu targeting 219, and Bing targeting 189 with some type of censorship. Strictly concerning hard censorship, web search engines targeted very few names. Baidu hard censored “习明泽” [Xi Mingze], Xi Jinping’s daughter, and “徐晓冬” [Xu Xiaodong], a mixed martial artist with anti-China political views. Seemingly beyond coincidence, Sogou hard censored the same two names, although Sogou targeted Xi Mingze with a more broad rule: “习 + 明泽” [Xi + Mingze]. These similar findings are especially surprising as Xu Xiaodong, while a sensitive name, would not seem as sensitive or as well known a name as many others in Chinese politics. We did not find Bing to hard censor any names.



[(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/04/image1.png&nocache=1)](https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/04/image1.png&nocache=1)

Figure 5: For each platform, for hard and (if applicable) soft censorship, a breakdown by category of the number of names censored in that category.

To better understand the motivations behind search platforms’ censorship of people’s names, we developed a codebook to categorize each censored keyword according to a person’s significance, particularly in the context of Chinese political censorship. Following grounded theory, we first went through all censored names to discern broad categories and repeated themes. This iteration led to seven high-level themes for the codebook. We then reviewed all of the censored names again and applied an appropriate label to each keyword (see Figure 5).

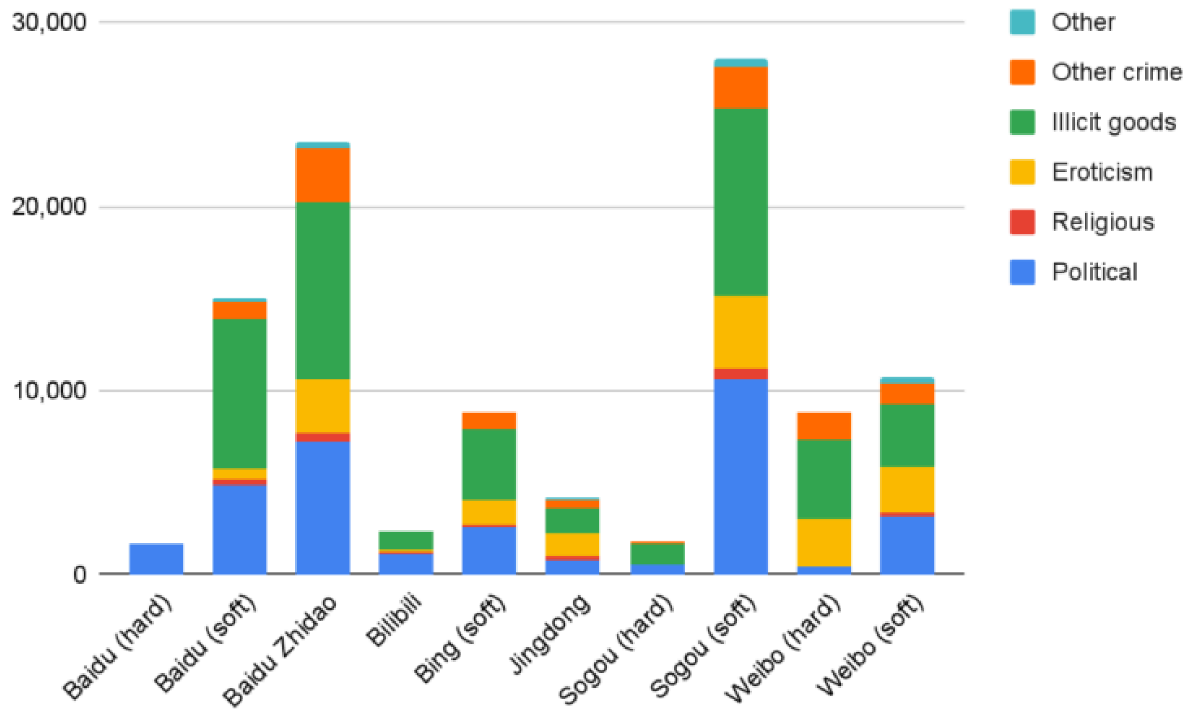
We categorized sensitive names into seven common themes: “Political” (e.g., political leaders and dissidents, major historical events, criticism of the Communist Party, or proscribed political ideas), “Religious” (e.g., banned religious faiths, spiritual leaders, and religious organizations), “Eroticism” (e.g., pornographic material, adult film actors, sex acts, adult websites, and paid sexual services), “Collateral” (names collaterally censored by a censorship rule targeting someone or something else), “Business” (businesspeople who do not have a clear political motivation for their censorship), “Entertainment” (celebrities, artists, singers and related figures in the entertainment and associated industries who do not have a clear political motivation for their censorship), and “Other” (a residual category that contains content which either does not fit within the other six categories and terms which have been censored for unclear reasons).

We found that most names that platforms censored were for political motivations, whether to shield leaders and other pro-Chinese-Communist-Party members from criticism or to silence dissidents. However, we also found that many names were collaterally censored by rules clearly targeting content other than that person or their name. As examples in English, Hong Kong musical artist “DoughBoy” was soft censored on Weibo for containing “ghB”, GHB being a drug illegal in China and broadly elsewhere, and Baidu Zhidao censored South Korean band “FLAVOR” for containing “AV”, an abbreviation for adult video. As examples in Chinese, Polish Violinist “亨里克维尼亚夫” [Henryk Wieniawski] was soft censored on Weibo for containing “维尼” [Winnie (the Pooh)], a common mocking reference (https://www.theguardian.com/world/2018/aug/07/china-bans-winnie-the-pooh-film-to-stop-comparisons-to-president-xi) to Xi Jinping, and Microsoft Bing soft censored Chinese actress “习雪” [Xi Xue] for containing “习” [Xi], Xi Jinping’s surname. Weibo’s soft censorship collaterally affected the largest number of names due to the platform’s use of broad censorship rules. In second and third are Jingdong and Baidu Zhidao, respectively. These examples of collateral censorship speak to the methodological importance of not just testing whether a string is censored but also of understanding the exact censorship rule targeting its censorship to avoid misattributing the censor’s motives.

Comparing the soft censorship of social networks Douyin and Weibo, we found that they censor a similar number of names under political motivation, with Douyin censoring slightly more. However, due to its use of broader rules, Weibo had much more names censored collaterally, whereas Douyin’s more specific rules were able to pinpoint political names without collaterally affecting any others in our measurements.

Experiment 2: Censorship of known sensitive content

Among our testing spanning 505,903 unique, previously discovered censored keywords, we found 60,774 unique keyword combinations censored across all search platforms which we investigated. Due to Douyin aggressively fingerprinting and banning our testing, we were unable to complete this experiment for Douyin. We also omit Bing hard censorship results from our discussion in this section as we only discovered four keyword combinations hard censored by Bing, and we believe that these keyword combinations were measurement artifacts of attempting to measure keyword combination censorship of a machine learning classifier trained to detect pornographic queries (we will discuss this more in the section “Evaluation of our model” later below).



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/04/image6.png&nocache=1)

Figure 6: For each platform, for hard and (if applicable) soft censorship, a breakdown by category of the estimated number of keyword combinations discovered in that category.

To understand the type of content censored on each platform, we randomly sampled 200 keyword combinations censored on each platform and categorized them as we did for the previous experiment into themes which resemble but are not all the same as the ones in the previous experiment: “Political” (e.g., political leaders and dissidents, major historical events, criticism of the Communist Party, or proscribed political ideas), “Religious” (e.g., banned religious faiths, spiritual leaders, and religious organizations), “Eroticism” (e.g., pornographic material, adult film actors, sex acts, adult websites, and paid sexual services), “Illicit Goods” (e.g., narcotics, weapons, and chemicals), “Other Crime” (e.g., gambling, fraud, extortion, counterfeiting, and private surveillance), and “Other” (a residual category that contains content which either does not fit within the other five categories and terms which have been censored for unclear reasons). For each platform, based on the proportion of keyword combinations that we found in each category in our random sample, we then estimated the total number of keyword combinations in each category for each platform.

We based our criteria for these six categories on what we found through examining censored content on the eight platforms listed in Table 3. Our six categories also roughly match the categories of prohibited content listed in Chinese government legislation (Figure 1), the targets of internet purification special operations (Figure 2), official announcements on reports of undesirable or harmful online information (Figure 2), and the nine categories of illegal, undesirable, or harmful information listed on the Cyberspace Administration of China’s Reporting Center (Figure 3). Below we describe our findings from each of these categories in more detail.

Political

We found that a large proportion of censored names of political leaders refer to Xi Jinping's name "习近平" or his family. Examples include his current wife "彭丽媛" [Peng Liyuan], his former wife "柯玲玲" [Ke Lingling], his sister "齐桥桥" [Qi Qiaoqiao], and his daughter "习明泽" [Xi Mingze] (see Table 10 for a breakdown per platform).

Baidu (hard)	Baidu (soft)	Baidu Zhidao	Bilibili	Bing (Soft)	Jingdong	Sogou (hard)	Sogou (soft)	Weibo (hard)	W
1,332	390	510	282	64	53	91	1,754	0	33

Table 10: For each platform, a breakdown of the estimated number of keyword combinations discovered related to Xi Jinping or his family based on sample testing.

Censored terms referring to Xi Jinping included the hard censoring of numerous homoglyphs (e.g., "刁斤干" on Baidu) of Xi's name, as well as hard censoring of terms like "xi + 包子" [xi + bun] on Bilibili, a reference to earlier propaganda campaigns which painted Xi as an avuncular figure (https://www.theguardian.com/world/2016/mar/30/xi-jinping-chorus-of-chinese-pop-songs-celebrate-president) with simple tastes (https://www.theguardian.com/world/2013/dec/29/chinese-president-xi-lunch-bun-shop). Other references to Xi are soft censored, including some homonyms (e.g., "吸精瓶") and the term "三连任" [three consecutive terms] on Bing, a reference to Xi's third term (https://www.nytimes.com/2023/03/09/world/asia/xi-economy-us-rivalry.html) as China's paramount leader. References to Xi's personal life are also widely censored. These include terms like "离婚 + 习近" [divorce + Xi Jin], possibly referring to Xi's first marriage to Ke Lingling (https://www.scmp.com/news/hong-kong/article/2180598/chinese-president-xi-jinpings-former-father-law-diplomat-ke-hua-dies). References to Xi Jinping's daughter Xi Mingze, such as "明泽 + 公主" [Mingze + princess] on Sogou, are hard censored. Little information is publicly available about Xi Mingze, but she is believed to have enrolled in Harvard University (https://www.newyorker.com/news/news-desk/what-did-chinas-first-daughter-find-in-america) in 2010 under a pseudonym. Terms related to other Xi family members are also censored, including references to rumors that Xi Jinping's elder sister Qi Qiaoqiao has Canadian citizenship (e.g., "加拿大籍 + 习近平 + 大姐" [Canadian nationality + Xi Jinping + eldest sister]) which are hard censored on Baidu.

While references to Xi Jinping are the most widely censored among all of China's political leaders, references to other past and current political figures are also censored. Some references to former premier "温家宝" [Wen Jiabao], including homonyms of his name (e.g., "温加煲" on Bilibili), are soft censored, as are phrases like "温 + 贪污" [Wen + corruption] on Weibo, the latter referring to accounts of alleged Wen family corruption covered in an investigative report by The New York Times (https://www.nytimes.com/2012/10/26/business/global/family-of-wen-jiabao-holds-a-hidden-fortune-in-china.html).

Terms indicating criticism of the Communist Party were also subjected to censorship. These include homonyms for Communist Party (e.g., "共抢党", soft censored on Weibo), as well as calls for the Communist Party to step down (e.g., "GCD + 下台" [GCD + step down] on Baidu). Some hard-censored slogans, like "洗脑班" [brainwashing class] on Jingdong and "共产党灭亡" [death of the Communist Party] on Bilibili, are associated with material produced by the Falun Gong spiritual movement. For example, the term "退党保平安" [quit the Party to stay safe and peaceful], hard censored on Bilibili, refers to a campaign (https://www.tuidang.org/) launched by the Falun Gong to encourage Chinese citizens to quit the Communist Party, Communist Youth League, and the Young Pioneers. Other censored terms refer to the 1989 Tiananmen Square protests and subsequent massacre (e.g., “TAM学生” [TAM students], soft censored on Bing) and notable dissidents (e.g., “晓波刘” [Xiaobo Liu], soft censored on Bing) and “吾尔开希” [Wu’er Kaixi], hard censored on Bilibili).

Religious

Much of the censored content concerning religion refers to banned spiritual groups, in particular the Falun Gong. These include homonyms for Falun Gong (e.g., “法仑功”) and references to the persecution of Falun Gong devotees (e.g., “弟子 + 迫害 + 洗脑” [disciple + persecution + brainwash]), both soft censored on Baidu. References to other banned spiritual groups are also soft censored, like “觀音法門” [Guanyin Famen, in traditional characters] on Sogou and “观音法门” [Guanyin Famen, in simplified characters] on Bing and “狄玉明” [Di Yuming], the spiritual leader of Bodhi Gong.

Not all censored religious terms refer to banned spiritual groups. The title of Tibet’s exiled spiritual leader, “达賴喇嘛” [Dalai Lama], is hard censored on Jingdong. Terms related to Christianity are also hard censored, though for reasons which are not immediately clear. “耶稣 + 少儿” [Jesus + children], “青少年 + 上帝” [youths + God], and “青少年 + 基督教夏令营” [youths + Christian summer camp] are all hard censored on Jingdong. While authorities have not banned Catholicism and Protestantism, Christian religious activities are strictly monitored (https://www.cfr.org/backgrounder/christianity-china) throughout China. Authorities also routinely surveil, harass, and detain (https://freedomhouse.org/sites/default/files/FH_ChinasSprit2016_FULL_FINAL_140pages_compressed.pdf) practitioners of underground house churches and Christian-influenced banned faiths like Church of Almighty God (“全能神教会”). The hard censoring of references to youths and Christianity may also be in response to reported state efforts to prevent those under the age of 18 (https://foreignpolicy.com/2021/07/01/chinese-communist-party-scared-of-christianity-religion/) from participating in religious education.

Eroticism

Censored terms in these categories refer to various kinds of pornographic material, acts or body parts, and paid sexual services. This includes terms like “色情无码” [uncensored pornography], soft censored on Bing, Japanese adult film actor “唯川纯” [Jun Yuikawa], hard censored on Baidu Zhidao, and sex acts like “舔嫩逼” [lick tender pussy], hard censored on Bilibili. Other censored terms refer to soliciting sex workers, such as “包夜 + 按摩” [overnight + massage], soft censored on Baidu, or “婊子上门” [visiting prostitutes], hard censored on Baidu Zhidao, or specific body parts, like “大屌” [big dick], soft censored on Sogou.

Illicit Goods

Many censored terms concerning illicit goods refer to drugs. Some refer to selling drugs like “卖 + 咖啡因” [sell + heroin] or “售 + 摇头丸” [sale + ecstasy], both hard censored on Bilibili, or “售 + 地西泮” [sale + diazepam], soft censored on Baidu. Others terms concern manufacturing drugs such as “制作 + 毒药” [crafting + poison], soft censored on Sogou, or “提炼 + 三甲氧基安非他明” [refining + Trimethoxyamphetamine], hard censored on Bilibili.

Censored terms also refer to weapons, including euphemistic references to particular weapons (e.g., “气狗” [air dog] or air gun, hard censored on Jingdong), their sale (e.g., “批发 + 弓弩” [wholesale + bow and crossbow], hard censored on Weibo), or their manufacturing (e.g., “制作 + 枪” [crafting + gun], hard censored on Weibo).

Chemicals also feature as censored terms, such as “光气 + 提供” [carbonyl chloride + supply], soft censored on Baidu, and references to buying particular kinds of insecticide (e.g., “敌杀磷 + 购买” [Dioxathion + buy], soft censored on Sogou). It is unclear why references to particular chemicals have been censored, though in some cases censorship may be related to the potential use of some chemicals in the manufacturing of narcotics or the production of explosives.

Gambling terms also make up a large number of censored terms related to illicit goods. These gambling-related terms include the names of particular websites (e.g., “金沙sands线上娱乐场” [Golden Sand sands online resort], a reference to Sands Casino in Macao, hard censored on Sogou), particular kinds of gambling (e.g., “赌马 + 开户” [horse betting + open account], and even “online casinos” in general (“网上赌场”, soft censored on Weibo).

Other Crime

This category of prohibited content contains references to a range of illicit or criminal activity. Some refer to various forms of fraud or forgery, including selling high quality counterfeit identity cards (“卖高仿身份证”, soft censored on Bing) or searches for police uniforms (“警服”, hard censored on Jingdong).

Other censored terms include references to adopting babies (“收养 + 宝宝” [adoption + baby], soft censored on Sogou) to selling organs (“售 + 肝臟” [sell + liver], soft censored on Weibo), potentially censored due to police efforts to deal with child trafficking and kidnapping (https://www.cnn.com/2014/02/28/world/asia/china-online-baby-trafficking-crackdown/index.html) and illegal organ harvesting (https://www.bbc.com/news/world-asia-china-55097424), respectively. References to other illicit activities like live broadcasting suicide (“自杀 + 直播” [suicide + live], soft censored on Sogou), hiring kidnapping services (“替人绑架” [kidnap for someone], hard censored on Weibo), or selling diplomas (“卖 + 文凭” [sell + diploma], soft censored on Baidu) are also censored, as are terms related to buying commercial surveillance devices (e.g., “供应 + 卧底窃听软件” [sale + undercover eavesdropping software], soft censored on Baidu).

Other

This residual category included censored terms which did not clearly fit within the other five categories. Some of these were profanity, both in Chinese (e.g., “艹你妈” [fuck your mom], hard censored on Jingdong) and English (e.g., “Fucker”, soft censored on Weibo). Others referred to news websites blocked in China, like Radio Free Asia (https://www.reuters.com/article/uk-google-china-mobile-idUKTRE62T21J20100330) (“自由亚洲电台”, hard censored on Bilibili) and the Taiwanese newspaper Liberty Times (https://archive.ph/jCfo) (“自由时报”, soft censored on Sogou).

References to censorship itself and how to circumvent content management controls were also censored. This includes references to the Great Firewall (“防火长城”, soft censored on Sogou), “翻墙” [leaping over the wall], soft censored on Weibo, and “网络发言防和谐” [online speech anti-censorship], soft censored on Baidu. In other cases, censorship reflected the corporate concerns of a specific platform. Jingdong hard censored the term “狗东” [Dog East or “gou dong”], a satirical play on words referring both to the companies name Jingdong and the use of a cartoon dog as the company’s mascot.

Impact of censorship across platforms

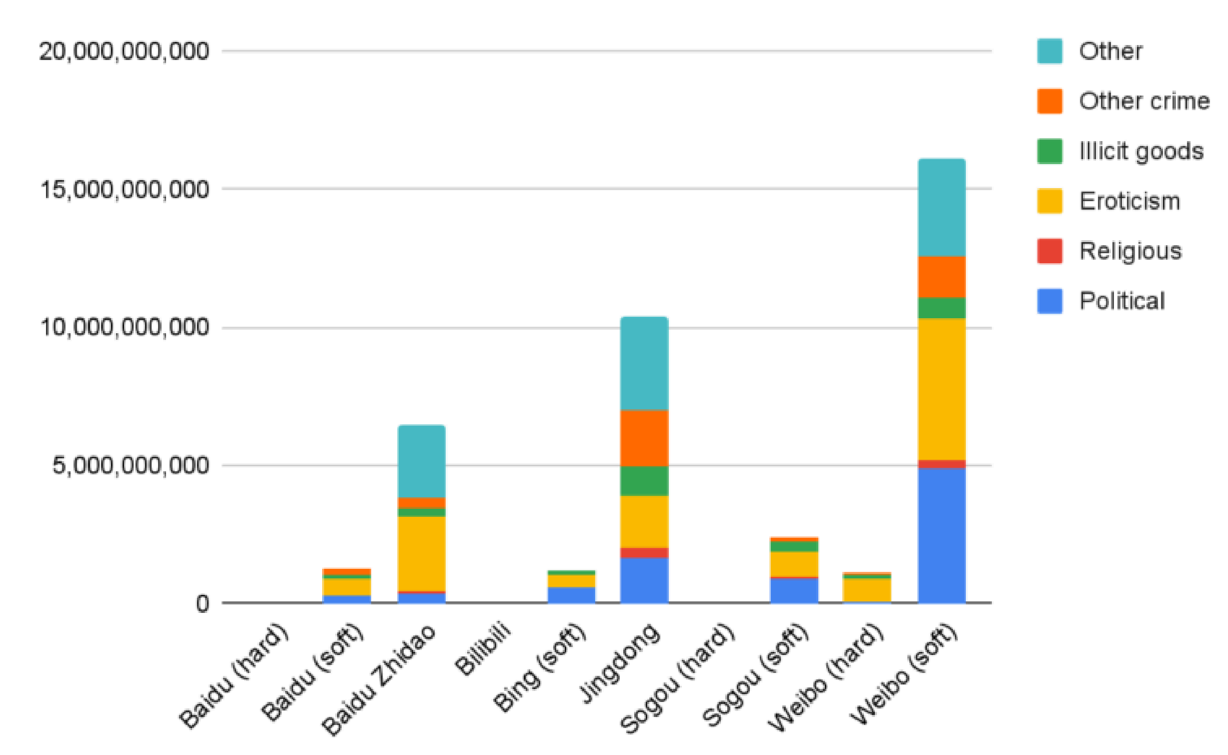
Although measuring the number of censorship rules targeting a type of content may be a valuable measure of the amount of attention or resources that a platform has invested into censoring that content, it may be a misleading measure of the actual impact of that censorship. For instance, when looking at Baidu’s soft censorship rules, we found 559 keyboard combinations containing the character “习” [Xi]. Many of these are homonyms of Xi Jinping’s name (e.g., “习进瓶”) or derogatory references (e.g., “习baozi”). Although Baidu uses a large number of rules containing “习”, Bing has only has one such soft censorship rule containing “习”, but it is to simply censor all queries containing the character “习” without any additional specificity. From this, a naive analysis might conclude that Baidu’s censorship of Xi is 559 times broader than Bing’s since it has 559 times as many rules, but yet Bing’s single, broad rule censors more Xi-related queries than Baidu’s long list of specific queries.

To attempt to measure which search platforms had the broadest censorship, we devised a new metric. At first, as an attempt to approximate the number of queries a keyword combination is censoring, we considered using search engine trends data, but such data appeared to have two major issues: first, trends data appeared to have data for only the most common of queries, and, second, trends data for a query were only for queries which exactly matched as opposed to performing a substring match. For example, trends data for “习近” [Xi Jin] would show fewer results than for “习近平” [Xi Jinping], despite “习近” being a substring of “习近平”. Thus, to approximate how many queries were censored by a rule censoring all queries containing “习近”, we would have to anticipate all such queries that one might make which contain “习近” and then add up the trends data for each.

Instead, we adopted a different metric, which we call the *impact score*, which was devised to approximate the number of web pages censored by a keyword combination. To determine the impact score for a keyword combination rule, we created a query where each keyword in that keyword combination was surrounded by quotation marks. For instance, for the keyword combination “习 + 二婚”, we recorded the number of results for the following search query:

```
"习" "二婚"
```

This query requests all pages containing both the exact phrase “习” and the exact phrase “二婚”, which mirrors the corresponding keyword combination censorship rule which censors any query containing those exact phrases. For this testing, to obtain the number of web pages impacted by a keyword combination, we measured using Bing as accessed from the Canadian region, as, to the best of our knowledge, Bing has not implemented Chinese political censorship of search results in this region. Note that we apply this metric even to search platforms which are not web search engines, even though these platforms are not searching web pages but rather other items such as store products, microblog posts, or social media videos, as we suspect that this metric can still approximate the impact of the censorship on these platforms as well.

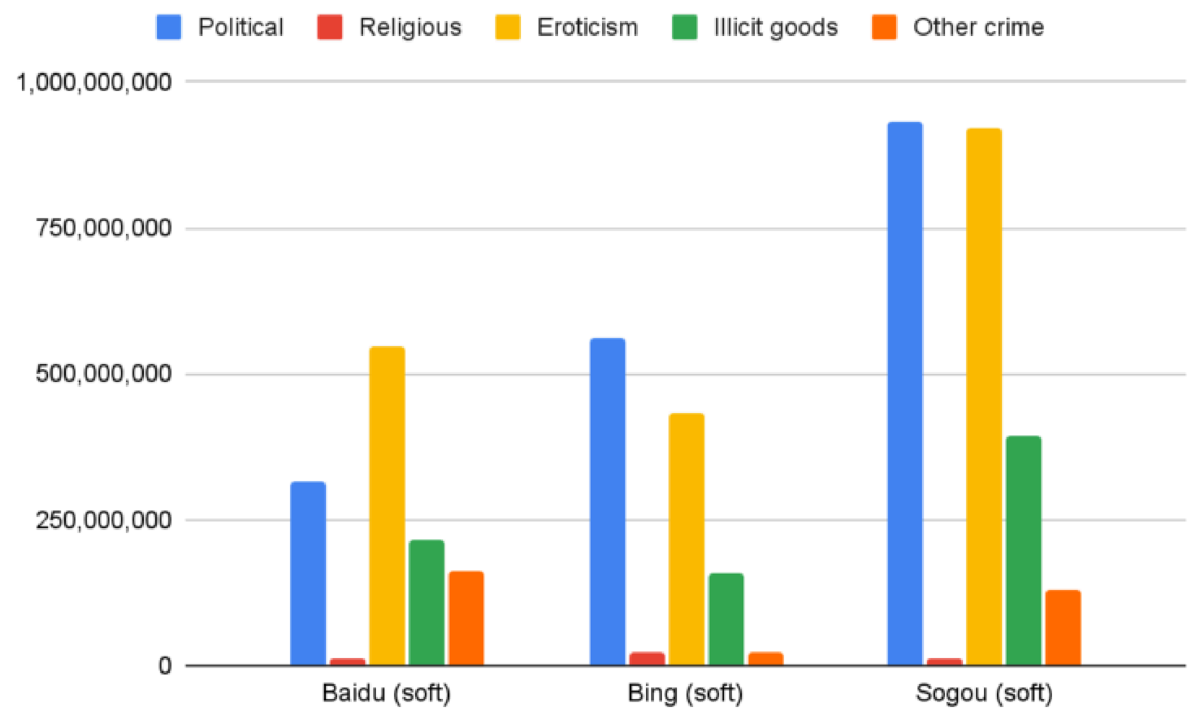


(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/04/image8.png&nocache=1)

Figure 7: For each platform, for hard and (if applicable) soft censorship, a breakdown by category of the estimated sum of the impact scores of each keyword combination in that category.

To understand the type of content most likely to be censored on each platform, we randomly sampled 200 keyword combinations from each platform by performing a weighted uniform sampling, with replacement, weighted by the impact score of each keyword combination. We then categorized these keyword combinations using the same codebook as before. These results are characteristically different than before, with Weibo now demonstrating the highest level of total censorship among the search platforms we analyzed (see Figure 7).

Analyzing by category, we find that Jingdong has the highest level of censorship of illicit goods. This finding is not unexpected given that Jingdong is the only e-commerce platform that we analyzed and thus could be expected to have broader filtering of illegal goods.



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/04/image3.png&nocache=1)

Figure 8: Among web search engines, a breakdown by category of the estimated sum of the impact scores of each soft-censored keyword combination in that category.

Turning our focus to the three web search engines, we find that Sogou has the highest level of overall censorship. Compared to Baidu, Bing has slightly less overall censorship than Baidu. However, breaking down by category, Bing's level of censorship of political and religious topics exceeds Baidu's, with Baidu's filtering of content related to eroticism, illicit goods, and other crimes exceeding Bing's. This finding suggests that Bing is not a suitable alternative to Baidu for users attempting to freely access political or religious content and that to access such content Baidu may be a better choice despite it being operated by a Chinese company.

Experiment 3: Ongoing testing from news articles

In this section we briefly discuss preliminary results from our ongoing experiment measuring censorship rules by testing news articles.

Baidu	Baidu Zhidao	Bilibili	Bing	Jingdong	Sogou	Weibo
1,493	1,426	165	115	329	4,438	908

Table 11: For each platform, as of April 2, the number of new censored keyword combinations which we discovered outside of the previous two experiments.

As of April 2, 2023, since our testing which began January 1, 2023, we have discovered between 155 and 4,438 new keyword combinations on each platform analyzed. Unfortunately we have limited ability to know if a newly discovered keyword combination was recently added or if it had merely been recently discovered. However, while many of the newly discovered censorship rules could not be shown to be recently added, many others referenced events that occurred since January 1, 2023, seemingly requiring them to have been introduced since then.

As examples, Weibo soft-censored “中国间谍气球” [Chinese spy balloon], referring to a Chinese balloon shot down (https://www.nytimes.com/2023/02/04/us/politics/chinese-spy-balloon-shot-down.html) on February 4, 2023, over the United States which the United States and Canada accused of being used for surveillance, as well as “阮晓寰” [Ruan Xiaohuan], an online dissident who was recently convicted (https://cpj.org/2023/03/chinese-blogger-ruan-xiaohuan-sentenced-to-7-years-in-prison/) of inciting subversion to state power. Baidu hard censored “逮捕令 + 普京 + 习近平” [Arrest Warrant + Putin + Xi Jinping], referring to an arrest warrant issued (https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and) on March 17, 2023, by the International Criminal Court for Vladimir Putin. In the days following the issuance, Xi Jinping would visit Putin (https://www.npr.org/2023/03/20/1160415730/latest-on-ukraine-xi-jinping-visits-moscow-to-meet-putin-march-20) in Russia. Sogou’s soft censorship of the Ukraine crisis used a large number of very specific keyword combinations, many of them referencing 2023 developments:

- 乌克兰 + 王吉贤 [Ukraine + Jixian Wang]
- 博明驳斥美国 + 台湾乌克兰化谬论 [Bo Ming refutes the US + fallacy of Ukrainization of Taiwan]
- 入侵乌克兰一年后 + 俄罗斯依赖中国 [A Year After Invading Ukraine + Russia Depends on China]
- 成为下一个乌克兰 + 台湾 [Be the next Ukraine + Taiwan]
- 王吉贤 + 乌克兰 [Jixian Wang + Ukraine]
- 抗议 + 俄罗斯 + 乌克兰战争 [Protests + Russia + Ukraine War]
- 大疆 + 无人机 + 乌克兰 [DJI + Drones + Ukraine]
- 马斯克 + 乌克兰 + 星链 [Musk + Ukraine + Starlink]
- 俄罗斯 + 入侵 + 乌克兰 + 一年 [Russia + invasion + Ukraine + year]

As we have previously mentioned, our isolation algorithm generalizes effortlessly to all languages. For example, we found that many platforms censored keyword combinations containing Uyghur script. Here are two examples of Bing targeting Uyghur users referring to issues of Xinjiang independence:

- ئەركىنلىك [Freedom]
- ۋەتىنىمىز [Our homeland]

This experiment has only recently begun, and we intend to continue performing this ongoing experiment, measuring how censorship unfolds across these platforms in realtime in response to world events.

Evaluation of our Model

We now reflect on how well our modeling of search platforms’ censorship rules as a “list of ordered sequences” fits with their censorship behavior in practice. In general, we found our results to be highly internally consistent using our model. However, both Jingdong and Bing showed inconsistencies which should not be strictly possible in our model. For instance, on Jingdong, we found that both the strings “枪” and “射网枪” are censored even though the string “网枪”, which contains “枪”, is not. On Bing, we found that both the strings “89天安门” and “1989天安门” are soft censored, even though the string “989天安门”, which contains “89天安门”, is not. On these platforms, characters surrounding censored keywords can sometimes seemingly play a role in determining whether to censor a string, behavior which is currently not captured by our model, and thus the number of censored keyword combinations may be underreported on these platforms.

While these were minor departures from our model, a more extreme case would be all four keyword combinations which our algorithm found to be hard censored on Bing:

- 台湾 + 小穴 + 护士做爱 + 台湾 [Taiwan + pussy + nurse sex + Taiwan]
- 片BT下载BANNED骚逼 [Piece BitTorrent Download BANNED Pussy]
- 你 + 你 + 你 + 你的屄 [you + you + you + your cunt]
- 你 + 你 + 你的屄 + 你 [you + you + your cunt + you]

Unlike our results for other platforms, including those of Bing’s soft censorship, the results for Bing’s hard censorship are, while seemingly related to eroticism, mostly nonsensical to human interpretation. The results pages for each of these four queries showed an explicit notification that results were blocked due to a mandatory “safe search” filter being applied to the mainland Chinese region, and we suspect that we were triggering a machine learning classification system trained to detect search queries related to eroticism. While machine learning algorithms struggle to censor according to subtle, broad, and rapidly evolving political criteria, they are more effective at detecting relatively narrower, more well-defined, and more slowly changing criteria such as whether a query is related to pornography. As such, these results may be an interesting glimpse into what would happen if we applied our isolation algorithm against a censorship system applying a machine learning classifier intending to politically censor content.

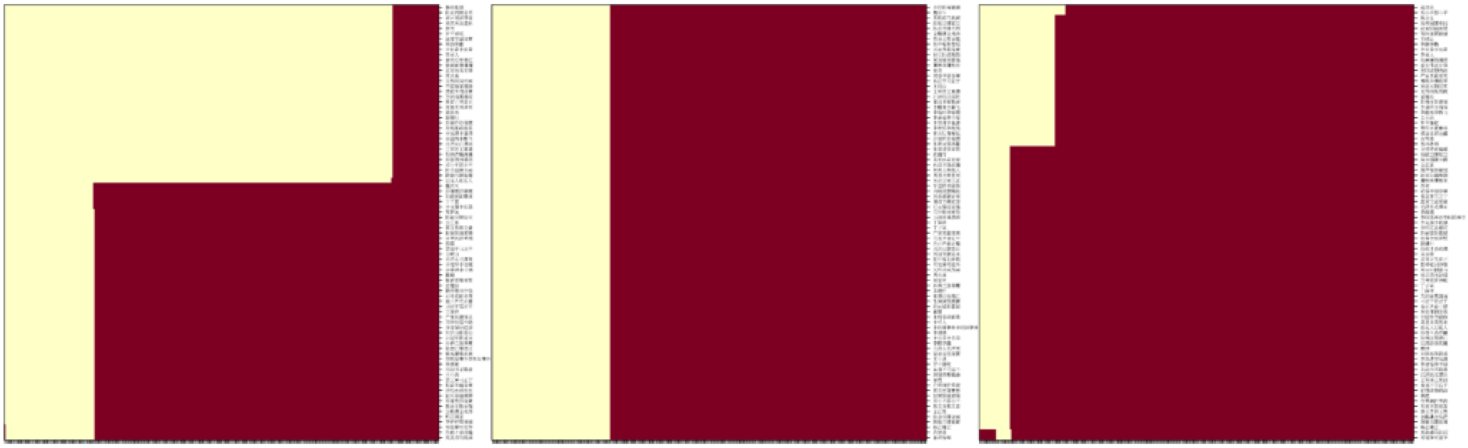
Authorized domain lists

All three web search engines which we analyzed performed soft censorship, a censorship scheme in which if a query contained a soft-censored combination of keywords, then results would only be returned from a list of authorized domains. In this section, we explore whether different search engines authorized different domains and whether different domains are authorized for different keyword combinations.

To investigate these questions, first we developed a method to measure whether a domain was authorized to be displayed in results for a given string. Our method is a simple modification of the one which we used to determine whether a string is soft censored in general: we replace “site:microsoft.com”, which was a domain which we presumed would not be authorized for any soft-censored string, with “site:IsThisAuthorized.com”, where IsThisAuthorized.com is a domain which we wish to test to see if it is authorized for that soft-censored string. Using this method, we tested across a set of domains *D* and a set of strings *S*.

To choose *S*, we selected those name test strings which we found soft censored on all three web search engines in Experiment 1. To determine *D*, for each of those strings, on each platform, we then searched for these strings, recording all domains which we observed in the first 100 search results. *D* then is the set of all domains which we observed during this procedure. In our experiment, *S* consisted of 83 strings, and *D* consisted of 326 domains.

In October 2022, on each web search engine, for each domain in *D* and string in *S*, we tested whether that domain was authorized for that string on that search engine. We then collected the results into a two dimensional matrix. To draw out the general shape of the lists, we hierarchically clustered (https://en.wikipedia.org/wiki/Hierarchical_clustering) both dimensions of the matrix according to the UPGMA (https://docs.scipy.org/doc/scipy/reference/generated/scipy.cluster.hierarchy.linkage.html#scipy-cluster-hierarchy-linkage) method.



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/04/all-o.png&nocache=1)

Figure 9: The "shape" of the authorized domains lists for Baidu (left), Bing (center), and Sogou (right): for each domain (x axis) and string (y axis), whether the domain is authorized for that string (light yellow) or not (dark red).

We found disparate authorization lists across web search engines (see Figure 9). We found that, in our experiment, Sogou authorized, on average, the fewest domains for each string, followed by Bing, with Baidu authorizing the most. Bing used the same authorization list for each string which we tested, whereas Baidu appeared to use approximately two different lists, although some strings used lists with small additions or subtractions from these two. Sogou appeared to mostly use two lists, with a third and fourth list being applied to some tested strings. In comparing Baidu and Bing, Baidu had a more complicated set of authorizations, whereas Bing broadly applied the same list to each string and thus authorizes fewer domains overall. While one might hypothesize that more sensitive keyword combinations are associated with shorter lists of authorized domains, we surprisingly did not notice any correlation between sensitivity and authorized domain list length.

To better understand the domains authorized by these search engines, we categorized them into three categories (see Table 12). The majority of sites on each list were Chinese state-approved news sites. Examples include xinhua.org (http://www.xinhua.org/) (Xinhua News Agency), people.cn (https://www.people.cn) (People's Daily), and qq.com (https://www.qq.com/) (QQ News). Sites from this category professed varying degrees of loyalty to the Chinese Communist Party (CCP), ranging from presenting the necessary regulatory license to practice journalism to statements such as these from huyangnet.cn (http://www.huyangnet.cn/node_50449.html) (Authoritative information release platform of Xinjiang production and Construction Corps) indicating Party sponsorship (translated): “Bingtuan Huyang.com is a key news portal website of Bingtuan, which is approved by the Information Office of the State Council and sponsored by the Propaganda Department of the Party Committee of Xinjiang Production and Construction Corps.”

List	News	Party-state	Other	Total
D	241 (73.9%)	77 (22.8%)	8 (2.45%)	326
Baidu (short)	45 (64.3%)	24 (34.3%)	1 (1.43%)	70
Baidu (long)	221 (73.4%)	76 (25.2%)	4 (1.33%)	301
Bing	82 (89.1%)	8 (8.70%)	2 (2.17%)	92
Sogou (shortest)	11 (84.6%)	2 (15.4%)	0 (0.00%)	13
Sogou (shorter)	22 (91.7%)	2 (8.33%)	0 (0.00%)	24
Sogou (longer)	50 (84.7%)	8 (13.6%)	1 (1.69%)	59
Sogou (longest)	51 (76.1%)	13 (19.4%)	3 (4.48%)	67

Table 12: Breakdown of authorized domain lists by category.

Other sites were more directly operated by either the Chinese Communist Party or the Chinese state. Many of these were official government websites of different jurisdictions, such as xinjiang.gov.cn (https://www.xinjiang.gov.cn/), the official web page of the People’s Government of Xinjiang Uyghur Autonomous Region, and gqt.org.cn (https://www.gqt.org.cn/), the official website of the Chinese Communist Youth League.

Finally, we have a small residual category, which contains miscellaneous sites such as search engines, those providing health information, etc.

One behavior which we were interested in understanding was how search engines behaved when two different soft-censored strings with different authorization lists occurred in the same query. Depending on how the systems are implemented, search engines may prefer the first observed keyword combination (such as if all censorship rules were implemented using a single deterministic finite-state automaton (https://en.wikipedia.org/wiki/Deterministic_finite_automaton)) or they might take the set intersection of all of the authorization lists for each occurring keyword combination. We found, however, that, when testing two different censored strings with different authorization lists, the list of one is preferred over the other regardless of their positions with respect to each other in the query (see Tables 13 and 14). This finding is consistent with a system which iterates over a list of blocked keyword combinations, testing for their presence in a query, and where, as soon as one is found present, the corresponding action for that keyword combination is taken, aborting the rest of the search.

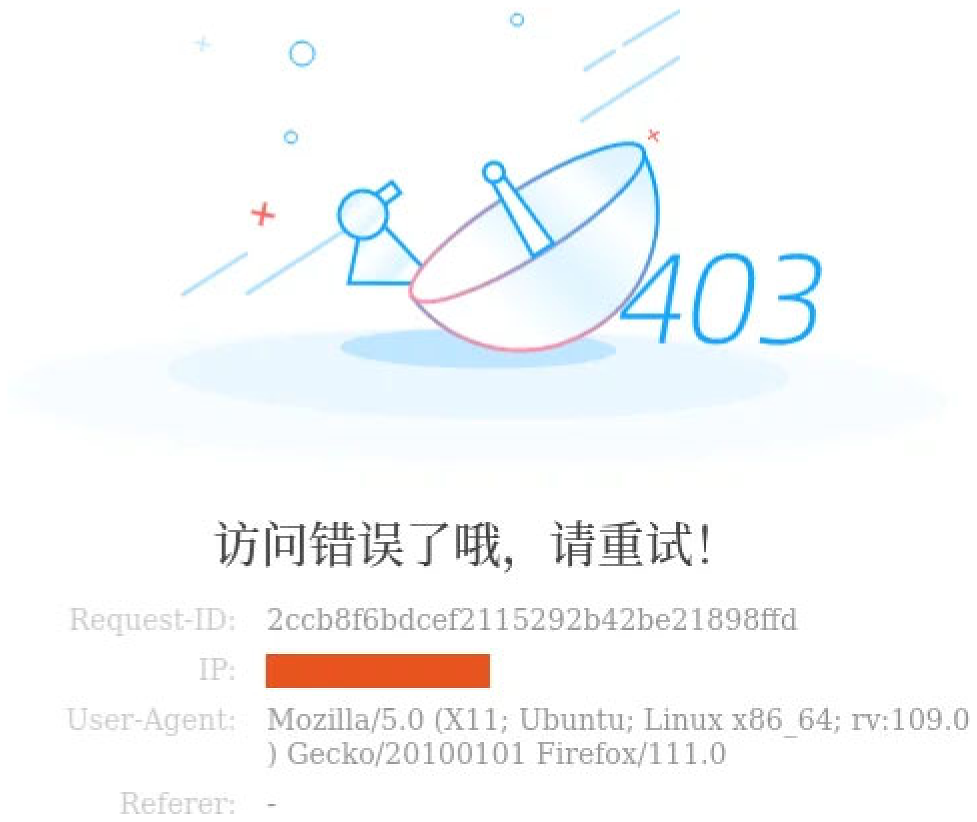
	baidu.com	mofcom.gov.cn
李克强李剋強	Authorized	Unauthorized
司徒華司徒华	Unauthorized	Authorized
李克强李剋強司徒華司徒华	Authorized	Unauthorized
司徒華司徒华李克强李剋強	Authorized	Unauthorized

Table 13: On Baidu, when both “李克强李剋強” [Li Keqiang, in both simplified characters and traditional characters] and “司徒華司徒华” [Situ Hua, in both traditional and simplified characters] are present, the authorized domains list for “李克强李剋強” is used.

	tibet.cn	baidu.com
韩正韓正	Authorized	Unauthorized
馬凱碩马凯硕	Unauthorized	Authorized
韩正韓正馬凱碩马凯硕	Authorized	Unauthorized
馬凱碩马凯硕韩正韓正	Authorized	Unauthorized

Table 14: On Sogou, when both “韩正韓正” [Han Zheng, in both simplified and traditional characters] and “馬凱碩马凯硕” [Ma Kaishuo, in both traditional characters and simplified characters] are present, the authorized domains list for “韩正韓正” is used.

While this may seem like a mundane finding, it suggests that the original order of keyword combinations discovered on the list can be reconstructed, at least partially (https://en.wikipedia.org/wiki/Partially_ordered_set), as the order of two keyword combinations with the same authorization lists cannot be directly compared using this method. Such an information side channel (https://en.wikipedia.org/wiki/Side-channel_attack) could be useful in measuring when a keyword combination was added to the list, where otherwise we would only know when it was first discovered on the list. Furthermore, not just knowing which keyword combinations are censored but also their order on a blocklist can be helpful (https://citizenlab.ca/2021/08/engrave-danger-an-analysis-of-apple-engraving-censorship-across-six-regions/#derivation-of-mainland-china-keyword-list) for inferring how such lists of censorship rules are shared among companies, developers, and other actors, as two lists might have many censorship rules in common by coincidence but, as the number of common censorship rules grows, it becomes super-exponentially (https://en.wikipedia.org/w/index.php?title=Factorial&oldid=1141925857#Growth_and_approximation) unlikely that both lists would have those censorship rules in the same order purely by coincidence.



访问错误了哦，请重试！

Request-ID: 2ccb8f6bdcef2115292b42be21898ffd

IP: [redacted]

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0

Referer: -

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/04/image7.png&nocache=1)

Figure 10: An example geoblocking block page for a popular Chinese news site.

Finally, when we were categorizing the domains, we noticed that a surprisingly large number of sites were inaccessible from outside of China. We found that, among the 338 domains in *D*, when accessed from a Toronto network, 59 (17.5%) failed to return an HTTP 200 status for either that domain or for that domain preceded by "www.". Some sites appeared to block connections on an IP or TCP layer, whereas others presented application layer block pages (see Figure 10). While the motivation for Chinese censors blocking non-Chinese sites from Chinese access is well understood, it is less understood why Chinese sites are in turn blocking access to non-Chinese users. Future research is required to understand this troubling progression of the balkanization (https://en.wikipedia.org/wiki/Splinternet) of the Internet.

Limitations

Our study analyzes automated censorship of search queries across a variety of platforms. However, there exist other layers of censorship which might also be affecting search results. For instance, on social media platforms, posts may be automatically or manually deleted or shadow-banned (https://en.wikipedia.org/wiki/Shadow_banning) if they contain sensitive content. In fact, the rules for automatically censoring posts may often match the rules for censoring search queries (see Appendix A). Users may also self-censor under the fear of reprisal for posting sensitive content. However, our work analyzes the rules used by platforms to automatically censor search results but not any of the other factors which might be skewing those results.

Some search platforms may have some censorship rules which censor not according to whether a query contains certain keywords but whether the query exactly equals a certain keyword. While this may seem like an inflexible manner to censor queries, we have observed such a case on Weibo, specifically when searching by hashtag (https://en.wikipedia.org/wiki/Hashtag), when we observed one hashtag which was censored (e.g., #hashtag) but superstrings of that hashtag which were not (e.g., #hashtagXYZ). Our method will often fail to detect censorship rules such as these which require exact matches, as our isolation algorithm requires that any query containing the censored content be censored in order to isolate the content triggering censorship.

Discussion

As North American technology companies such as Google (https://theintercept.com/2018/09/21/google-suppresses-memo-revealing-plans-to-closely-track-search-users-in-china/) mull over whether to expand search or other services to the Chinese market, a popular argument (https://www.scmp.com/comment/insight-opinion/united-states/article/2168337/china-even-censored-google-search-engine-would) has been that, although infringing on users' political and religious rights is inherently wrong, perhaps a North American company could better resist Chinese censorship demands and provide a less-infringing service than a Chinese company. However, even if the ends are to justify the means, then, for this argument to have any validity, the service provided by the North American company must be less infringing.

Unfortunately, our study provides a dismal data point concerning this argument. It suggests that whatever longstanding human rights issues pervade in China, they will not be magically addressed by North American technology companies pursuing business in the Chinese market. To the contrary, our report shows that users using Microsoft Bing are subject to broader levels of political and religious censorship than if they had used the service of Bing's chief Chinese competitor. In fact, rather than North American companies having a positive influence on the Chinese market, the Chinese market may be having a negative influence on these companies, as previous work has shown how the Chinese censorship systems designed by Microsoft (https://citizenlab.ca/2022/05/bada-bing-bada-boom-microsoft-bings-chinese-political-censorship-autosuggestions-north-america/) and (https://www.vice.com/en/article/qj8v9m/bing-censors-tank-man) Apple (https://citizenlab.ca/2021/08/engrave-danger-an-analysis-of-apple-engraving-censorship-across-six-regions/) have (https://citizenlab.ca/2022/03/engrave-condition-apples-political-censorship-leaves-taiwan-remains-in-hong-kong/) affected users outside of China.

The methods introduced in our work facilitate future, ongoing censorship measurement. In light of our third experiment, we presented preliminary results from an ongoing experiment discovering search platform censorship by sampling text from news articles. We intend to continue running this experiment for the indefinite future, tracking changes to search platform censorship over time as events around the world unfold.

The challenges in moderating search queries are similar to those moderating queries to machine-learning-powered chat bots such as ChatGPT (https://openai.com/blog/chatgpt) in that, just as with search platforms, when compared to the understanding of the actual query evaluator, the censorship system may have an inconsistent understanding of a query which can be exploited to measure for the presence of censorship. As one possible example, AI researcher Gary Marcus found (https://www.nytimes.com/2023/01/06/podcasts/transcript-ezra-klein-interviews-gary-marcus.html) through experimentation that ChatGPT responded to the query, "What religion