上海国際问题研究院
SHANGHAI INSTITUTES FOR INTERNATIONAL STUDIES

Lies and Truth about Data Security

— Against the U.S. DHS's Data Security Business Advisory

Author

ZUO Xiaodong

April 2021

Lies and Truth about Data Security

— *Against the U.S. DHS's Data Security Business Advisory*

ZUO Xiaodong[1]

[1] Zuo Xiaodong is Vice President of the China Information Security Research Institute and Nonresident Senior Fellow at the Shanghai Institutes for International Studies.

Foreword

CHEN Dongxiao，*President of SIIS*

The SIIS Center for International Cyber Governance is committed to promoting China-U.S. cyber dialogue and providing a platform for debating competing views. Over the past few years, SIIS has conducted a number of joint research projects with the Carnegie Endowment for International Peace and the Computer Science and Artificial Intelligence Laboratory at the Massachusetts Institute of Technology. With our partners, we have also hosted a series of international seminars and conferences where Chinese and U.S. scholars and officials exchanged, debated, and spread their views in a rational and professional way. We believe that China-U.S. positive interaction in cyberspace should be underpinned by objectivity and rationality.

Cooperative competition has defined China-U.S. cyber relations over recent years. In September 2015, Beijing and Washington launched a high-level dialogue mechanism for combating cybercrime and reached a six-point consensus, setting an example of great power cooperation in cyberspace. Even as the two cyber powers began to build up mutual trust, the generally cooperative relationship was disrupted by U.S. unilateral actions, including continued indictments of Chinese citizens for their alleged role in threatening U.S. cybersecurity. The U.S. government has also released a number of high-profile reports that misunderstand and misrepresent China's cyber policy, further undermining the efforts to build a stable China-U.S. cyber relationship.

Dr. Zuo Xiaodong, a nonresident senior fellow at the Center for International Cyber Governance, is a veteran cybersecurity expert long involved in strategy formulation, law enactment, and standard setting regarding China's cybersecurity. This long cyber career has given him a unique perspective and

professional understanding, allowing him to refute and debunk the many claims, charges, and myths in the DHS's report. We consider scholarly perspectives and critiques to be essential to the current, complex China-U.S. cyber relationship for their role in reducing the many U.S. misunderstandings and misperceptions regarding Beijing's cyber intentions and capabilities, at this critical moment when Beijing and the Biden administration are designing the best way for China-U.S. engagement in cyberspace.

Content

Summary

The Sino-U.S. cyber relationship is the most important relationship in cyberspace. Its stability determines the overall stability of cyberspace and bilateral cooperation underpins the prosperity of cyberspace. Cybersecurity is also a new and complex issue in bilateral relations, requiring joint efforts by both sides to manage differences, promote cooperation, and maintain stability. China once proposed to make cybersecurity a new highlight of bilateral cooperation, and actively responded to the concerns of the United States by establishing a China-U.S. high-level dialogue mechanism against cybercrime. However, China's goodwill and cooperative attitude was given a cold shoulder. Worse still, the United States has taken unilateral prosecutions, sanctions, and suppression measures against the Chinese government and companies. In order to cooperate with the U.S. government's suppression measures, some cybersecurity companies and think tanks have published a large number of false, exaggerated, and fictitious cybersecurity incidents in order to incite anti-China sentiment.

During the Trump administration, the U.S. government changed its old ways of behind-the-scenes manipulation, resorted to overt containment policies, and released a large number of false research reports on China's Internet policy. These reports are easily regarded as "authoritative" by the outside world because they are stamped with the badge of the U.S. government. The reality is that these reports took advantage of the negative sentiment of the American public and society towards China, as well as the lack of cybersecurity knowledge, and produced a lot of false content through the production of fake news, thereby achieving the purpose of confusing the audience. The above-mentioned actions of the U.S. government have completely transcended cybersecurity issues and reduced it to a “fake news” and “war of public

opinion." The purpose is not to safeguard U.S. interests in cyberspace, but to hysterically suppress China.

On December 22, 2020, the U.S. Department of Homeland Security (hereinafter referred to as DHS) issued a report titled "Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China." This is a recent report, representing U.S. government's discrediting China's Internet policy. This report is extremely sinister in its tone. It directly targets China's cybersecurity laws and regulations, and misinterprets the National Intelligence Law, the Data Security Law (Draft), and the Cryptography Law with malicious extensions and subjective assumptions. It claims that "Chinese law forces all Chinese companies and entities to transfer data collected at home and abroad to the government"; "The National Intelligence Law may force Chinese companies to install backdoors and other security vulnerabilities in equipment and software sold abroad to facilitate the Chinese government's easy access to data not controlled by Chinese companies"; "Any encryption system that is 'approved' for use in China, or used by a company that processes Chinese data, must provide its encryption key to the Chinese government"; and "Enable the State Cryptography Administration to access commercial cryptographic systems, including access to data protected by these systems." As a result, the State Cryptography Administration can fully obtain decryption keys, passwords, and any other information needed to access data on commercial encryption servers. Therefore, American technology companies seeking to do business in China must surrender intellectual property and technology.

None of these alarmist conclusions are based on facts. China is one of the largest digital markets in the world, and major companies involved in the digital economy, including American companies, have invested and operated in China for a long time. If China's laws and regulations really include the

above-mentioned provision, it will inevitably have an impact on American companies. But the truth is that the U.S. government has not obtained any evidence that can support its judgment. Upon closer examination, it can be found that the shocking discoveries in the report are all based on assumptions.

The fact is that the United States has established the world's largest state-sponsored surveillance system, and has conducted long-term all-pervasive monitoring of the United Nations, allies, and other countries. Public records have shown that the legal system of the United States has facilitated the United States' global surveillance program. The "Snowden Incident" has already been publicly exposed, but the U.S. government has not taken this as a warning. On the contrary, it continues to expand the scale and capabilities of global monitoring. The actions of the United States have seriously endangered the global network security. Under such circumstances, the blatant accusations made by the United States against China are just a kind of thief shouting to catch the thief.

Contrary to the wrong accusations of China in the report, China's laws, regulations, and policy measures in the cyber field are basically the same as those of other countries, all aimed at maintaining cybersecurity and national security. These practices are usually in line with international practices and are common practices adopted by various countries when dealing with cybersecurity. Chinese law not only does not infringe on the intellectual property rights of foreign companies, but also provides legal protection for their lawful business operations in China. China also put forward a "Global Data Security Initiative," which is the first comprehensive data security blueprint for governments, international organizations, and other stakeholders.

Lies and Truth about Data Security

— Against the U.S. DHS's Data Security Business Advisory

ZUO Xiaodong

On December 22, 2020, the U.S. Department of Homeland Security (DHS) released a report entitled "Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China." Issued just weeks before a new administration was to be inaugurated, the report represented another attempt in a broader U.S smear campaign against China—an early indication that the incoming Biden team would carry on his predecessor's "tough on China" policy position. Addressing the "growing cyber threat" from China has been a strategic priority over recent years and protecting data security is nothing but a pretext to spread Sinophobia.

Beijing has always opposed the politicization of technical issues and asked the U.S. government to produce specific evidence, if any, of the so-called cyber threats emanating from China. But the U.S. government disdains to talk about technology and keeps pointing fingers at Beijing and misusing the elastic term of "national security." Washington does not have any firm evidence and believes there is no need for any. Just as U.S. officials held a model vial of anthrax—that looked pretty much like washing powder—to make the case for at the UN Security Council in March 2003, it may also interpret a news report on "Inheriting the Red Gene" on the anniversary of the PLA's founding as evidence of the Chinese military's effort to genetically modify its soldiers.

This time things look a bit different as the DHS seems to have laid out "detailed and reliable" evidence by citing profusely Chinese laws and regulations to bolster its assertion that Beijing is engaged in "organized" and "planned" data theft. I have been hoping that the U.S. government can provide solid evidence, but unfortunately, what we have heard over the years are such far-fetched old stories like "Communist cells are embedded in Chinese state-owed and private enterprises" and "retired military officers are *de facto* bosses of many private businesses." A closer examination can debunk these false assertions.

Dusting off the old playbook

The Data Security Business Advisory is issued to alert U.S. businesses to the growing “data-related risks” and recommend using "alternative data service providers and equipment." Since all network services and IT equipment involve data processing, the DHS actually intends to eliminate all Chinese elements from the IT field. This is a serious breach of WTO rules and an extreme form of unilateralism and protectionism.

The report believes that U.S. businesses expose themselves and their customers to heightened risks when they share sensitive data with Chinese firms or use equipment and software developed by Chinese firms. It claims that these risks result from direct actions of the Chinese authority and Chinese laws that coerce Chinese firms into providing data and relevant information to the Chinese government.

So, what kind of "Chinese actions" have the DHS found threatening? And what “Chinese laws” are coercive?

With scanty evidence, surmise...

The Advisory surmises growing data-related risks from China based on one sentence: "If oil is the core resource in the era of industrial economy, then data is the most important strategic resource in the era of digital economy" attributed to China’s National Information Center, dated March 10, 2020. In fact, this is the only official Chinese record with a specific source and original text

in the report. However, this statement is commonly used in China to show Beijing's focus on data as a new factor of production. It also demonstrates China's determination to develop the digital economy and foster new momentum of economic growth.

The DHS thinks it has found a valuable piece of evidence, jumping to the conclusion that Beijing is now seeing data as an essential "strategic resource," just as Washington has long viewed oil as a high-value asset over which it has fought several wars. Beijing is portrayed as a data thief to support its domestic and international agendas.

This sentence alone is certainly not enough; therefore, the DHS cites several other national development plans.

— "Made in China 2025" plan, "Digital Silk Road," and "Military Civil Fusion" efforts

— Shifting manufacturing from lower-value goods to higher value-added technical areas

— Efforts to replace foreign products

— Modernization of the People's Liberation

These development plans are cited to increase the credibility of the report. But how do these development plans relate to data? The DHS attributes China's decades of rapid economic growth to the theft of U.S. intellectual property and highlights that "the PRC has increased its efforts to collect foreign data, through both legal and illegal channels" to support the implementation of these plans.

The report devotes nearly two pages to outlining the actions taken by the U.S. government in response to "CCP data theft." Some of these actions are related to several executive orders issued by Donald Trump and sanctions against China in trade frictions. Others include U.S. Department of Justice's indictment of Chinese citizens for their alleged role in "cyber attacks" against the United States. Regarding cybersecurity, China's Foreign Ministry has repeatedly stated China's solemn stance and exhorted the U.S.—the real "Hacker Empire"—to stop the political show. I would like to propose a new perspective on this: How many cybercrime cases are there in the U.S. every year? Are the U.S. government the chief sponsor in each case?

Malicious Misrepresentation and Distortion of Chinese Laws

The second piece of so-called evidence cited in the Data Security Business Advisory is three specific Chinese laws, namely, the *National Intelligence Law*, *Data Security Law (Draft)*, and *Cryptography Law*. Perhaps because most Americans do not read Chinese, the DHS has played a few tricks that are easily identified.

First, quoting out of context. A major conclusion of the report is that China's National Intelligence Law "compels all PRC firms and entities to ... turn over data collected abroad and domestically to the PRC," as Article 7 it stipulates that "All organizations and citizens shall, in accordance with the law, support, cooperate with, and collaborate in national intelligence work, and guard the secrecy of national intelligence work they are aware of." In fact, this article is a principled statement of citizens' obligation to safeguard national security. In addition, Article 8 also stipulates that "The national intelligence work should be carried out according to law, respect and protect human rights, and

safeguard the legitimate rights and interests of individuals and organizations." However, the DHS deliberately ignored Article 8 and misinterpreted Article 7 to draw the shocking conclusion. The U.S. requirement for civil obligations can be seen in its naturalization oath: "that I will bear arms on behalf of the United States when required by the law; that I will perform noncombatant service in the Armed Forces of the United States when required by the law; that I will perform work of national importance under civilian direction when required by the law." Following the DHS logic, what can be inferred from this oath?

Second, fabricating evidence. The DHS claims that the National Intelligence Law may compel PRC firms to install backdoors and other security vulnerabilities in equipment and software sold abroad so that the PRC government can easily access data not controlled by PRC firms; the Data Security Law (Draft) represents an even greater shift in the CCP's attitude away from protecting Chinese data systems as a defensive mechanism toward collecting data as an offensive act; and the Cryptography Law stipulates that any encryption system that is "approved" for use in China, or by companies that handle Chinese data, is required to provide its encryption keys to the PRC government. These descriptions are completely fabricated by the DHS. No relevant text is available in any Chinese legal provisions, and it is impossible to deduce similar conclusions.

Third, draw a far-fetched conclusion. Every law stipulates penalties for violations and sometimes rewards for excellent behaviors. However, the DHS frames the reward and penalty clauses under the National Intelligence Law as a regime of offering economic incentives for conformists and punishment for defiers. It has been a practice in the U.S. for decades to improve joint response capabilities in handling cybersecurity incidents by enhancing information

sharing. However, the DHS interprets the related statement in the Data Security Law (Draft) as follows: "the PRC will establish a centralized process to monitor and assess risk, share data with relevant PRC bodies." Moreover, the DHS associates information sharing with national security review, which are irrelevant, to further mystify data security risk assessment as well as monitoring and warning mechanisms and intentionally induce readers to associate information sharing with the conspiracy theory. Article 31 of the Cryptography Law requires the establishment of an information platform for regulation and management of commercial cryptography. This platform is mainly used for the release and query regarding industrial information on regulation and management, but is described by the DHS as "allowing the SCA to request complete access to commercial cryptography systems, including to the data protected by such systems. The result is that the SCA has full access to decryption keys, passwords, and any other information needed to access data on a commercially encrypted server. Therefore, American technology companies must turn over intellectual and technological property if they seek to do business in China"—a scenario grim enough to scary away U.S. businesses which seek to expand their Chinese operations.

Fourth, confuse right and wrong. In order to counter trade discrimination, Article 24 of the Data Security Law (Draft) stipulates that "For any country or region that adopts discriminatory prohibitions, limitations or other such measures toward China with respect to investment or trade related to data, data development and use, or technology, China may, according to the actual circumstances, adopt corresponding measures toward that country or region." But it is interpreted by the DHS as "discriminatory" and further extended as "force foreign markets to remain open to Chinese data services providers." Why is it that the DHS allows the U.S. to ban Chinese firms but prohibits China from taking reciprocal countermeasures? Moreover, it is well known that the U.S.

has been implementing "long-arm jurisdiction" and "extraterritorial enforcement" and claims that data stored by U.S. businesses anywhere in the world should be provided to the U.S. government in compliance with U.S. domestic laws. In this context, various countries put forward requirements for the local storage of data. The DHS claims that "data localization requirements, for example, may force foreign businesses to make costly investments," showing its dissatisfaction. How can the U.S. justify the fact that it allows its government to have access to data stored around while prohibiting other countries from protecting their own data?

Fifth, misleading the public. In fact, the DHS does not only aim at China's laws, but also at China's major projects and important plans. The DHS believes that the detailed data reported by enterprises on China's National Credit Information Sharing Platform (NCISP) contains proprietary data or other sensitive information. Regarding the "Made in China 2025" plan, the DHS says that China attempts to "pursue global dominance in its next phase of data-driven technological growth" by leveraging its "asymmetrical advantages," including "the lack of privacy laws, intellectual property rights, and human rights protections." To show authenticity, the DHS also provides a link to the "Made in China 2025" plan, which actually redirects to the U.S. Congress's comments on this plan. However, there are no such "asymmetrical advantages" or similar statements in the U.S. Congress's report. The DHS, as an important agency of the U.S. government, is so full of lies.

Unprofessional Technical Fantasy

The third piece of evidence cited by the Data Security Business Advisory is that Chinese products are found to have technical flaws or covert data transmission

channels. The DHS is supposed to be much better at addressing technical issues than making comments on Chinese law. Unfortunately, the DHS's technical judgment has long lost its impartiality, and even common-sense errors have occurred again and again. The DHS should be capable of doing it well. It did not do so, but kept spreading reckless slanders just for political correctness as people believe those stupid slanders.

In addition to the repeated words that smear China's National Intelligence Law and Cryptography Law, and the "industrial subsidy" topic in the Sino-U.S. trade negotiation, the Data Security Business Advisory also mentions several specific risks associated with Chinese data services. Unfortunately, these risks are also fabricated.

First, use of Huawei equipment in Papua New Guinea. According to the DHS, the data center built by Huawei for the National Cyber Security Centre of Papua New Guinea has four major problems: (1) Data flows on the equipment in use could be easily intercepted by entities familiar with the equipment's flaws; (2) The data center uses an decrypted algorithm for encryption; (3) The data center relies on outdated firewalls; (4) Huawei has undercut its international competitors to secure 4G/5G infrastructure contracts around the world but changed terms of service during the implementation phrase. This is obviously ridiculous. In today's world, no large international companies would provide customers with outdated security products or use compromised cryptographic algorithms. Regarding the first problem, what are the "flaws"? Who are the "entities"? And what are "intercepted"? The DHS uses such ambiguous language to sell the "conspiracy theory" again. Can the DHS answer the following questions: Shall a firewall intercept communication streams when it is running? Shall intrusion detection equipment intercept

communication streams when it is running? Shall a situational awareness system intercept communication streams when it is running? The DHS may have forgotten that Europe and the U.S. have proposed systematic requirements on "lawful interception" interfaces for communication equipment and prohibited market access of equipment that does not meet their "lawful interception" requirements. What is the relationship between these "interceptions"? There is no need to say much about the fourth problem because the U.S. should not blame others for their loss of advantages in technology and cost and U.S. business has long been known for their predatory practices in the Third World.

Second, Telikom PNG's accusations against Huawei. Telikom PNG is a telecommunications operator in Papua New Guinea. According to the DHS, Telikom PNG can not see 20-30% of the network traffic, and all changes need to be vetted by a Huawei employee. Moreover, technology outside of Huawei's ownership is denied access to its network infrastructure, and the operational language of manuals is Mandarin Chinese. The DHS considers this as monopolization. This example is even more ridiculous. What does 20-30% of the network traffic mean to Telikom PNG, a backbone network operator? Would Telikom PNG remain indifferent to such a large amount of covert communication? As far as I know, when the U.S. conducts global interception, it transfers only a small amount of critical data through U.S. equipment to prevent its interception behavior from being detected. Will anyone do this manifestly? As for equipment change and technology use, I suggest that the DHS relearn the basic concepts of "system integration" and "system O&M." If I buy a piece of U.S. software and ask the original vendor to open its source code for my secondary development independent of the original vendor, will the U.S. enterprise agree? I cannot help but ask again, is the DHS serious about writing this report? Will anyone believe that a highly internationalized

company provides operational manuals to foreign customers only in Mandarin Chinese?

Third, analysis of the new concept of "bug door." To smear Chinese firms, the U.S. government often claims that vulnerabilities are discovered in a Chinese product and have adverse consequences. However, this no longer works over time. Even junior middle school students who have studied programming know that bugs often exist in programs, and there is another word "debug," which means "detecting and removing bugs." Defects, including bugs, that lead to the compromise of the system by attackers are called vulnerabilities. Vulnerabilities are inevitable in any software or hardware, and therefore IT companies often release "patches" to fix vulnerabilities. In fact, all users in the world are familiar with the regular patching of U.S. products such as the Windows operating system. The Common Vulnerabilities and Exposures (CVE), the most authoritative vulnerability database in the world, is maintained exactly by a DHS-funded agency. In this context, using vulnerabilities as an excuse is implausible and ridiculous. Therefore, the DHS creates the word "bug door" and defines it as a camouflaged "backdoor." Then, what are the technical standards for a "bug door"? What is the technical difference between a "bug door" and a bug? Is the DHS trying to say that the bugs found in U.S. products are bugs and those found in Chinese products are backdoors? This concept is not created from the technical perspective but to tarnish China's reputation.

Fourth, legally acquired data augmenting illicitly acquired data. The DHS envisages that China, after illicitly acquiring data, can purchase legitimate data from intermediaries through agents to facilitate big data mining. For example, it envisages that China can restore some sensitive data by associating

anonymized data sets and adding other data. Of course, this is technically feasible, but is the DHS writing a novel? It seems that "China" can be replaced by "the U.S." or any other country in this context. However, the U.S. does not need to do so because global data is already in its possession. We will find out how later in this article.

Fifth, software and mobile device applications. According to the DHS, "Data collected through software and mobile applications owned or operated by PRC firms is also accessible to the PRC government." The DHS claims that the U.S. government has provided evidence that the Chinese app TikTok could covertly track a device's unique MAC address and discover information stored by the user in the clipboard function. If I remember correctly, the U.S. did not ban the use of WeChat and TikTok after its president that "provided evidence" announced the ban. This president's account was shut down by U.S. high-tech companies before he left office, but TikTok retained his account. More examples are available. After the General Data Protection Regulation (GDPR) came into force in the EU, a large number of huge fines have been imposed, many of which are related to U.S. enterprises, with illegal acquisition of user data accounting for the majority. Few cases involve Chinese companies.

Sixth, fitness trackers and other wearables. According to the DHS, "Even where the identity of the wearer is kept anonymous by the device itself, the combination of location data over a certain time interval can identify where each user lives, works, or otherwise spends time. Location data of this sort would not only provide travel patterns of wearers, but—in combination with property tax records—could be further leveraged to identify names and family members." Thank the DHS for providing us with technical principles, but so what? Does this indicate a data security risk from China? Aren't there more

wearables produced in the U.S.? The DHS describes much about the basic principles of data collection in the "Risks of Procuring Data Services From, or Partnering with PRC" chapter in the Data Security Business Advisory. This is because it believes that the Chinese government may compel Chinese companies to turn over data under China's National Intelligence Law and if it can technically prove that Chinese companies are able to collect data, this will be an indirect indicator for the Chinese government's collection of global data. This is the DHS's logic and also the truth of all the so-called "evidence" provided in the Data Security Business Advisory.

Inside the Empire of Surveillance

The U.S. intelligence community remained unapologetic and unabashed about its wide-ranging surveillance programs at home and abroad even after the PRISM scandal expose by Edward Snowden, a former CIA contractor and has carried on its smear campaign against its adversaries, China and Russia, accusing them of stealing U.S. government and private-sector data. The U.S. acts like a thief crying "stop the thief." How come it has got its courage to do so? It comes from a set of flawed, long-running theories that classifies cyber attacks as legal and legitimate ones and illegal ones. What the U.S. does is totally legal, so it can launch cyber attacks and obtain data from all over the world. But how about the other countries? If the U.S. says you've done it, then you've done it, illegally.

As Americans see it, since every country has armies and every country has intelligence operations, why can't there be armies and intelligence operations on the Internet? What's legal in the real world should also be legal on the Internet. That is to say, as long as cyber attacks are launched for military, national security, counter-terrorism, and intelligence purposes, they are legal and should be recognized by international law. There is only one type of act that is illegal in the real world — theft of trade secrets— so it is not allowed on the Internet either. This is exactly why the U.S. government turned a blind eye to external accusations of its cyber attacks, and also why it always accused China and other countries of theft of trade secrets and other misconducts in the commercial field.

That theory seems plausible but does not stand up to closer scrutiny. At the end of 2018, the *New York Times* reported that the NSA had infiltrated servers in Huawei's headquarters in Shenzhen, monitoring the communications of Huawei's top executives. The NSA's attack on Huawei, a private company, was launched for national security reasons, because it wanted to obtain evidence of Huawei's links with the Chinese government and military. To advance U.S. national security interests, no action would be deemed inappropriate. If the U.S. assertions unfortunately become the international law, it will be completely free from the constraints of rules and do whatever it likes in cyberspace. If that ever happens, there won't be any international peace or security.

So, before we go deep into this empire of surveillance, let's uncover its tricks.

Unquenchable Thirst for Control

In 1949, George Orwell, an English novelist, published his novel *Nineteen Eighty-Four*, depicting a world where the "Big Brother is watching you" and nothing can escape government scrutiny. Since then, this slogan has been popular around the world for describing any surveillance operations that infringe on privacy. The U.S. is then labeled "Big Brother."

The U.S. truly lives up to this label.

First, the U.S. has established a huge intelligence community through executive orders. The U.S. intelligence community was established under Executive Order 12333 signed in 1981. The Executive Order established an intelligence community composed of 16 agencies, including, most prominently, the NSA, CIA, and FBI, and ordered that one of the most important tasks of intelligence agencies was to engage in broad surveillance (including the

collection of intelligence information concerning corporations and other commercial organizations) and highlighted the aim of strengthening collection techniques feasible abroad. Executive Order 12333 authorized the NSA to collect and retain data transmitted through the transatlantic submarine fiber-optical cables before it arrives at the U.S., and ordered that the activities carried out by the NSA under the Order would not be governed by statutory law. On July 16, 2020, the Court of Justice of the European Union invalidated the EU-U.S. Privacy Shield for cross-border data transfer due to concerns that there is no privacy guarantee for EU citizens under surveillance because U.S. intelligence agencies can access EU data under Executive Order 12333.

Second, the U.S. has established a legal system for surveillance through the *Foreign Intelligence Surveillance Act* (FISA 1978), *Electronic Communications Privacy Act* (ECPA 1986), and *Communications Assistance for Law Enforcement Act* (CALEA 1994). For the first time, the FISA separates national security surveillance operations from the scope of criminal procedure and provides independent legislation for intelligence surveillance, covering secret investigation means such as electronic surveillance, physical searches, pen registers and trap & trace devices, and access to certain business records. To facilitate smooth implementation of the FISA, the U.S. federal judiciary has created a special court, the Foreign Intelligence Surveillance Court (FISC). Compared with other courts in the U.S., the FISC has a distinctive particularity that it has unilateral procedures, and the targets of surveillance have no opportunity to defend themselves in court. Most surveillance orders are signed by one judge, and the judgment is not made public. The ECPA protects wire, oral, and electronic communications, while the CALEA further clarifies telecom carriers' duty to assist in law enforcement, achieving all-round surveillance in the legal system. After the September 11 terrorist attacks in 2001, the U.S. quickly enacted the *Provide Appropriate Tools Required to Intercept and*

Obstruct Terrorism Act (PATRIOT Act), which grants the NSA, FBI, and other agencies three privileges of surveillance for counter-terrorism: Intercept and store citizens' communication data for a long time, monitor through the use of roaming wiretaps, and track lone-wolf terrorist suspects. Under the PATRIOT Act, Title II "Enhancing Surveillance Procedures" greatly expands the governmental authority and scope of intelligence surveillance. Section 215 grants U.S. law enforcement agencies the authority to investigate any information related to terrorist activities, serving as a legal basis for the NSA's large-scale collection of citizens' call data. This section resulted in hash criticism and expired after June 1, 2015.

Third, U.S. legislation gives the green light to overseas surveillance operations. The FISA operates in a discriminatory manner regarding Americans and non-Americans. When Americans are involved, the FISA requires intelligence agencies to exercise caution in using technical investigative techniques, follow the strict principle to determine the target of surveillance, develop and use minimization procedures, apply to the FISC for a warrant, and accept supervision. However, the conditions and procedures for the surveillance of non-Americans are fairly simple, even without prior authorization of the justice warrants. Under Section 702 of the FISA, the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to one year from the effective date of the authorization, the NSA's targeting of persons reasonably believed to be located outside the U.S. to acquire foreign intelligence information, without the need to apply for a FISC order. The NSA's PRISM surveillance program implemented since 2007 was authorized pursuant to Section 702 (PRISM will be detailed in subsequent sections). Section 206 of the PATRIOT Act authorizes law enforcement agencies to conduct interception on individuals in foreign intelligence investigations

with mobility, shifting the interception from specified lines to specified persons. This increases the flexibility and mobility of intelligence interception.

Fourth, the U.S. has strengthened extraterritorial enforcement to counter Internet data protection requirements of other countries. In 2013, the U.S. District Court for the Southern District of New York issued a search warrant, requesting Microsoft to turn over all emails and information associated with an account to the FBI to assist in a case investigation. Because the emails of the account were stored on a Microsoft server in Dublin, Ireland, Microsoft argued that it could not provide data to the FBI under the EU and Irish data protection requirements, and moved to vacate the warrant. Later, the U.S. DOJ filed a lawsuit against Microsoft. After five years of litigation, the case was made moot due to the passage of the *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) in March 2018. The U.S. DOJ agreed that the CLOUD Act resolved the core legal issues of the Microsoft case, and further proceedings would be meaningless. So why is that? The CLOUD Act amended the 1986 *Stored Communications Act* by authorizing U.S. law enforcement agencies to issue subpoenas or seek warrants forcing cloud service providers subject to U.S. long-arm jurisdiction to provide data located outside the U.S., including the email content, chat records, names, address, metadata, service duration, and call fee records. To further reduce the technical barrier to obtaining foreign data, the U.S. government has long been opposed to the data storage localization requirements of other countries. This is one of the criticisms against China in the DHS's Data Security Business Advisory.

Fifth, U.S. intelligence agencies were born to serve commercial interests. On January 22, 2019, the U.S. released the 2019 National Intelligence Strategy, which specifies seven mission objectives: strategic intelligence, anticipatory

intelligence, current operations intelligence, cyber threat intelligence, counter-terrorism, counter-proliferation, and counterintelligence and security. But in fact, since their inception, U.S. intelligence agencies have had the function of serving commercial interests, especially when it comes to bidding for the military-industrial complex (MIC), such as Lockheed Martin, Boeing, Raytheon, and so on. It is not surprising that these companies are supported by intelligence agencies because they have exerted a huge influence on U.S. politics to maintain their huge profits. In November 2020, Denmark's Public Broadcaster, the DR, published revelations that the U.S. NSA spied on Denmark's financial and foreign ministries in order to obtain information on the country's fighter acquisition program and subsequently gained an advantage in selling the Lockheed Martin F-35s. The documents of the PRISM surveillance program leaked by Snowden show that the NSA's mass surveillance operations not only target overseas government leaders but also international organizations and business leaders. The German weekly *Der Spiegel* reported that financial transactions, especially credit card deals, were among the targets of NSA surveillance programs. Visa and the international payments system SWIFT were both monitored. Surely, the U.S. government would say that they've done this in order to track terrorist fund-raising activities, but what's behind the curtain?

Unparalleled Surveillance Capability

The U.S. has become the world's only "empire of surveillance," largely owning to its capabilities. The U.S. is the birthplace of a series of major IT technologies, and almost all the other countries in the world are heavily reliant on its technologies and services. This gives the U.S. additional leverage to get things

from others, see what others cannot see, and understand what others cannot understand.

First, the U.S. has the power to allocate basic Internet resources. There are 13 Internet DNS root servers in the world, with 1 primary root server and 12 secondary root servers. The primary root server is located in the U.S.; 9 of the 12 secondary root servers are located in the U.S., and the rest in the UK, Sweden, and Japan. These root servers are managed by the Internet Corporation for Assigned Names and Numbers (ICANN) authorized by the U.S. government. Although ICANN claims to be a not-for-profit organization, it is actually controlled by the U.S. With ICANN allocating Internet domain names and addresses, the U.S. government is actually managing and controlling the running of the global Internet. If the U.S. wants to suppress any other country, it can stop the resolution of the country's top-level domain names, disconnecting the country from the Internet, and thereby making the country disappear from the Internet world. For example, during the Iraq War, the U.S. terminated the application and resolution of .iq domain (Internet country code top-level domain for Iraq), "destroying" Iraq in the Internet world. In addition, the U.S. once handed over .ly domain (Internet country code top-level domain for Libya) to the opposition forces in Libya, directly interfering in the Libyan internal affairs. The U.S. super-monopoly over the Internet has caused strong concerns of other countries. In recent years, the internationalization of ICANN has been continuously advancing, but will the U.S. give up the control?

Second, the U.S. is leading the deployment of various types of network infrastructure and the generation of network content. The U.S. controls the Internet communications backbone. In December 1988, the first transatlantic submarine fiber-optical cable (TAT-8) entered into commercial service. From then on until 2008, European and U.S. companies monopolized the global fiber-optical cable market, and the submarine fiber-optical cables that they deployed

were generally originated from or traversed hub stations in the developed countries in Europe and the U.S. Since 2008, such companies have shifted their investments to areas with weak network infrastructure, such as Africa, but European and U.S. companies retain their monopoly over submarine fiber-optical cables. Currently, submarine fiber-optical cables in cyberspace are connected through code nodes in the U.S. Data transferred from one country to another almost inevitably passes through the U.S. The NSA documents leaked by Edward Snowden showed that the NSA maintains "corporate partnerships" with particular U.S. technology and telecom companies that allow the agency to "gain access to high-capacity international fiber-optic cables, switches and/or routers throughout the world," enabling the U.S. to carry out mass surveillance at will. The U.S. also controls the information sources of the Internet. The U.S. has the world's largest number of visits to websites; it has the world's most popular search engine Google, the largest video website YouTube, and the most influential social networking sites Facebook and Twitter. With a complex intelligence legal system in place, the data collected and stored on these websites undoubtedly falls into the hands of U.S. intelligence agencies.

Third, the U.S. controls every key link along the IT industrial chain. The U.S. is the largest supplier of global information and communications equipment, dominating every key link in the industry chain. U.S. manufacturers monopolize the R&D and production of the core parts of hardware and software of global IT products, from network infrastructure (Cisco and Juniper), cloud (Amazon), database (Oracle), operating systems (Microsoft Windows, Android, and iOS), chip design (Intel and Qualcomm), and content services (Facebook, Twitter, and Google), to software and terminals (Apple). These products are deployed worldwide, penetrating almost every link of the global network. Moreover, in order to maintain its absolute dominance over the industry chain, the U.S. continues to pursue mergers and acquisitions to control

the core technologies of other countries, either directly or indirectly. In addition, the U.S. has adopted national security review measures to prevent foreign investors from accessing key technologies. In August 2018, the U.S. released the *Foreign Investment Risk Review Modernization Act* (FIRRMA), extending the scope of "critical technologies" from "technologies that are essential to U.S. national security" to include "emerging and foundational technologies." Almost all foreign investments in these areas have been vetoed by the U.S. through national security review, defending its monopoly on core technologies.

Fourth, the U.S. has taken moves to suppress dissidents in the supply chain on the grounds of cybersecurity and Clean Network initiative, aiming to maintain its capabilities to intercept global networks. With its dominance in key links in the industry chain, the U.S. has gained an absolute advantage in surveillance in cyberspace. However, the rise of Chinese communications companies in recent years has challenged its interests. The U.S. will never give the green light to those non-U.S. companies, such as Huawei, ZTE, TikTok, and WeChat, which it considers dissidents in the industry chain. If the NSA wants to modify routers or switches in order to eavesdrop, a Chinese company will be unlikely to cooperate, which significantly increases the difficulty for the U.S. to disrupt and penetrate into target networks. Clearly, the more gear from Huawei and other Chinese companies is installed in the world's telecommunications networks, the harder it becomes for the U.S. to "collect it all." Every time such a gear is deployed, the U.S. is taking a step backward in its surveillance landscape. Ironically, the U.S. Clean Network campaign claims to promote privacy and data security by excluding untrusted Chinese suppliers. Obviously, there is no such thing as a secure network under the control of the U.S., as it can penetrate into whatever network it wants. The real reason the U.S. is making every effort to purge Chinese companies has nothing to do with

security, but everything to do with its desire to maintain its capabilities to intercept global networks.

Unscrupulous Online Actions

The U.S. uses three major technical means to conduct network surveillance: (1) Getting direct access to Internet companies' servers and databases to retrieve data; (2) An NSA special unit proactively obtaining information secretly and remotely by hacking; and (3) Obtaining data worldwide through fiber-optic cables. In this context, no communication means can ever escape from the NSA's mass surveillance, for example, Internet user data, optical cable communication, metadata of phone calls or emails, voice or SMS messages, and faxes; nor can any country, individual, or organization get away from U.S. surveillance because the U.S. FISC allows the NSA to spy on all countries around the world, even U.S. allies and intelligence partners, in specific scenarios to serve its best national interests.

Under the support of a variety of technical means, the U.S. has conducted several types of operations.

First, the U.S. has established different surveillance enforcement departments to carry out their respective duties and collaborate with each other. U.S. intelligence agencies started their modern surveillance technologies with the deciphering of military communications during World War II, and since then they have expanded their surveillance into cyberspace. The NSA is the main surveillance agency, and the Office of Tailored Access Operations (TAO), Special Source Operations (SSO), and Global Access Operations (GAO)

are its three branches. TAO is usually responsible for researching and developing cyber attack technologies, launching cyber attacks, and invading foreign computers for cyber espionage activities; SSO is primarily responsible for collecting, processing, and monitoring Internet metadata; GAO takes charge in intercepting intelligence from satellites and other international intelligence platforms. Under this system, the NSA has planted backdoor software in around 100,000 computers worldwide since 2008, giving it the capability to monitor them around the clock, as well as launch attacks. The NSA once secretly broke into the main communication links that connect Yahoo and Google's respective data centers around the world, and collected data from hundreds of millions of user accounts by tapping these links. The NSA gathers around 5 billion records each day on the whereabouts of smartphones and collects about 2 billion smartphone text messages each day from around the world by breaking into global mobile networks. Smartphone operating systems such as iOS and Android are described as the "gold nugget of data resources" in an internal NSA document. The NSA targets smartphone apps to fish for users' personal data, and once increased the budget from US$204 million to US$767 million. The apps under surveillance include the popular game Angry Birds, Google Maps, Facebook, Twitter, and the photo-sharing site Flickr.

Second, the U.S. has set up dedicated network surveillance programs. The NSA has set up a number of programs that are directly linked to network surveillance, covering both the Internet and telecommunications networks. One of the most well-known programs is PRISM leaked by Edward Snowden. In June 2013, Edward Snowden handed over two top-secret documents to the *Guardian* and *Washington Post*, making the secret surveillance program PRISM public. According to the leaked documents, PRISM requested at least nine major Internet companies in the U.S., including Microsoft, Google, Facebook, Yahoo, Apple, PalTalk, AOL, Skype, and YouTube, to provide data for the NSA,

including emails, instant messages, videos, photos, stored data, voice chat, file transfers, video conferences, login time, social network profiles, and other communication information of Internet users. These companies normally delivered data to the government electronically. Some companies established independent security access to make it easier for government agencies to extract intelligence. In addition, the NSA has been monitoring 122 world leaders since 2009, and built a secret database on world leaders, which contains 300 reports on German Chancellor Angela Merkel. The documents leaked to the *Washington Post* described PRISM as the most prolific contributor to the President's Daily Brief. The Snowden leak caused a global uproar over the range and depth of U.S. surveillance. Some EU countries attempted to build the EU Internet to get rid of U.S. surveillance.

Third, the U.S. has been cooperating with allies to establish a global surveillance network. In 1948, after the end of World War II, the U.S., together with the UK, Canada, Australia, and New Zealand, signed the United Kingdom – United States of America Agreement (UKUSA) for intelligence sharing and joint interception of foreign intelligence. In addition to assigning a level of classification to intelligence products (e.g., SECRET), dissemination at any level can be further restricted by use of a caveat that defines which "eyes" may see the material. For example, a Top Secret document intended only for Canadian officials would be stamped as, "TOP SECRET – CANADIAN EYES ONLY." Over time, intelligence officials from the five countries began to adopt the term "Five Eyes" as a form of verbal shorthand. This is how the term "Five Eyes" came about. The Five Eyes' surveillance system, known as the ECHELON, has its core ground stations deployed in Sugar Grove in West Virginia and Yakima in the Washington, D.C. of the U.S. and two airbases in the UK. The ground stations have large and small radio dish antennas for intercepting signals from international communications satellites, via which signals of telephones,

telegraphs and computer communications from 134 countries around the world are transmitted. The revelation about ECHELON caused great concern of the international community, and many countries severely reprimanded this serious violation of human rights and even international conventions. Some European countries were worried that modern communications are insecure, and they were more angry at the violation of their right to privacy. Therefore, the EU conducted a comprehensive investigation into this program. The investigation focused on checking whether the ECHELON surveillance system was involved in mass espionage activities against EU commercial trade, and whether the political and economic decision-making organizations of the EU headquarters were under comprehensive surveillance.

Undoubtedly, the U.S. has become the biggest security threat to in cyberspace, compromising the fundamental human rights of global citizens and national security of countries around the world. For a long time, the reliance of countries on U.S. equipment and technologies has made the world "unidirectionally transparent" to the U.S. The U.S. can intercept global networks by tapping its technical advantages, such as the root servers deployed on its soil, monitors installed in equipment, and backdoors planted in software. Even countries that it claimed to be allies are no exception. This helps maximize its military, political, and economic interests.

Disastrous Consequences of Surveillance

The wrongdoings of the U.S. in cyberspace blatantly undermine the principles of international relations and seriously threaten the peaceful development of the world, which produce a series of negative consequences and also have a serious impact on itself.

First, undermining cybersecurity. According to Reuters, the NSA reached a US$10 million deal with RSA, an encryption technology company, to insert a backdoor in RSA's cryptographic algorithm in order to undermine software encryption standards and make it easier for the NSA to launch mass surveillance. According to an intelligence budget document leaked by Snowden, the NSA spends US$250 million each year on the SIGINT Enable Project to undermine security standards and practices. The U.S. has repeatedly undermined the supply chain of IT products (such as high-end routers) manufactured in the U.S. by planting backdoors in the products before they are delivered to customers, facilitating intrusion by U.S. intelligence agencies. Everyone knows that we should keep a close eye on the vulnerabilities in IT products and install patches as quickly as possible. However, users are not notified of the vulnerabilities immediately after they are discovered. Instead, they are provided to the U.S. intelligence agencies, greatly facilitating their online exploitative operations before users are aware of the vulnerabilities. Some vulnerabilities will never be disclosed to users; instead, they are used by the U.S. to develop targeted cyber weapons. These U.S. moves make the security line of defense of the target systems vulnerable, rendering these systems unable to defend against the interception by the U.S. government and prone to be exploited by hackers, cyber criminal groups, or other cyber attackers.

Second, violating human rights. U.S. intelligence agencies' indiscriminate, all-round, and multi-level mass surveillance around the world seriously violate fundamental human rights, including the right to privacy, right to freedom of information and expression, right to a fair trial, and right to freedom of religion. In particular, the U.S. retains a large amount of communication data, which fundamentally violates the rule of law, compromises personal privacy, and is a direct infringement of personal data protection laws, in which the EU GDPR

is a typical one. People under surveillance are afraid to express their opinions or communicate with the outside world on sensitive topics, which not only affects their freedom of speech, but also undermines others' freedom of information. Even U.S. allies believe that such indiscriminate behavior could pose a destructive threat to the foundations of the democratic system if intelligence agencies could bypass democratic political and legal channels to intercept massive private calls.

Third, affecting the image and commercial interests of U.S. companies. On July 16, 2020, the Court of Justice of the European Union invalidated the EU-U.S. Privacy Shield for cross-border data transfer. This is the second EU-U.S. cross-border data transfer mechanism abolished by the Court of Justice of the European Union since the EU-U.S. Safe Harbor Framework was invalidated in 2015. The Court held that the Privacy Shield cannot be trusted because it cannot protect EU citizens from mass surveillance programs operated by U.S. intelligence agencies. The two draft recommendations released by the European Data Protection Board (EDPB) on November 10, 2020 basically deny the legality of transferring data of EU citizens to the U.S. by stating that "If the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society, then the EDPB is incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights." Clearly, U.S. companies have lost the most convenient conditions for conducting cross-border transactions in Europe due to the dishonest surveillance operations of U.S. intelligence agencies, which brings great uncertainty to the future development of U.S. companies in Europe. In addition, the active or passive cooperation of U.S. companies with U.S. intelligence agencies in a series of surveillance operations has shaken people's basic trust in U.S. companies. What's worse, the U.S. government is on guard against the few

Chinese companies that have entered the U.S. market, while a large number of U.S. companies have already been doing business in China for decades. Is China completely transparent to the U.S.? How shall China deal with these U.S. companies?

Fourth, compromising the well-being of U.S. citizens. The development of new network technologies continuously drives human civilization to new heights, brings profound impacts on social transformation, greatly unleashes potential productivity, and makes human life better. 5G technology is a most typical one. The emergence of 5G is of great significance, similar to what papermaking, steam engine, and Internet have brought to the human society, and is bound to have a bright future. However, the U.S. has launched a smear campaign against China's 5G on the grounds of data security risks. It not only bans China's 5G on the U.S. soil, but also forces other countries not to use it through diplomatic, trade, and other means. The U.S., once a great power in technological innovation, has now staged a big show of anti-intellectualism, acting in the opposite direction of civilization and history out of its own selfishness. Strangely enough, the DHS was complacent in this regard and claimed in the recent Strategic Action Plan against China that "recent actions have mitigated the PRC's attempts to dominate global 5G market share." So, let me ask one question, what can the U.S. government get by rejecting the world's most secure and cost-effective 5G technology? Is secure and reliable 5G technology available to American citizens? When will it become available? Given the performance of the U.S. government in responding to the COVID-19 pandemic, can a government that puts its people's lives at risk take their economic and other welfare into consideration?

Fifth, undermining international mutual trust. In the shadow of the U.S. indiscriminate global surveillance, even other western countries with the same ideology as the U.S. have shown their distrust of the U.S. without the slightest hesitance, which has significantly changed the landscape of international cooperation in cyberspace. Especially, concerns have grown in EU countries about losing control over data, data law enforcement, and the capacity for innovation of local companies. As stated by Margrethe Vestager, executive vice president of the European Commission, EU citizens want to trust technology when they use it and not begin in a new era of surveillance. U.S. technology companies are collecting massive amounts of personal data in the EU, and their business model is based on the collection and exploitation of online users' data to generate advertising revenue. The Cambridge Analytica scandal illustrated how online platforms are also able to extract personal data for political profiling purposes. These trends are referred to as surveillance capitalism by the EU. In terms of data law enforcement, EU member states have become highly concerned about the expansive extra-territorial powers granted to U.S. law enforcement agencies to obtain foreigners' personal data under the U.S. CLOUD Act, and that U.S.-based large online platforms will dominate entire sectors of the EU economy and deprive EU Member States of their sovereignty in areas such as copyright, data protection, taxation, and transportation. In terms of technological innovation of local companies in the EU, experts warn that high-tech economy is increasingly based on intangible assets (i.e., data and intellectual property), and major gaps will rise between first-mover U.S. companies and EU companies in this regard. In 2020, the EU released a series of strategy documents, including Shaping Europe's Digital Future, A European Strategy for Data, and European Data Sovereignty to counter the U.S. data hegemony. As Margrethe Vestager put it, "We've come to a point where we have to take action. A point where the power of digital businesses – especially the biggest gatekeepers – threatens our freedoms, our opportunities, even our

democracy. So for the world's biggest gatekeepers, things are going to have to change."

China's Proposal to Address Data Security

Building a peaceful, secure, open, cooperative, and orderly cyberspace is what the Chinese government aspires for global cyberspace security, China's strategic goal for cyberspace security, the direction of China's actions, and also China's greatest goodwill for the world. However, the U.S. government has been taking moves against China over data security in an effort to contain China.

— In May 2019, the U.S. gathered representatives from 32 countries and regions for a two-day Prague 5G Security Conference in Prague, discussing 5G security standards. This circle formulated the Prague Proposals at the conference, which suggests proposals in four distinct categories for 5G security risks. Three categories are related to data security, targeting Chinese 5G technology suppliers such as Huawei. In particular, the Prague Proposals suggest taking into account the overall risk of influence on a supplier by its country, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection. These deliberately selected security assessment factors cannot be objectively measured or assessed, and will be used subjectively in the absence of a fair procedure. The Prague Proposals attempt to directly designate China as a high-risk source and block all Chinese companies from the global market. Ironically, while the U.S. took the lead in developing the Prague Proposals, it never thought that the EU-U.S. Privacy Shield would be invalidated just one year later.

— In August 2020, then U.S. President Donald Trump signed two Executive Orders to ban WeChat and TikTok on the grounds that they were suspected of obtaining data of U.S. citizens. According to the Executive Orders, no U.S. citizen is allowed to use the two apps originated from China, no U.S. company is allowed to have any transactions with Chinese companies Tencent and ByteDance or even their associated companies. This was too absurd that the Executive Orders were not executed in the end.

— In August 2020, the U.S. Department of State launched its Clean Network initiative as part of its effort to prevent China from stealing data. The initiative includes Clean Carrier (to ensure that untrusted Chinese carriers should not provide international telecommunications services to the U.S. and other countries), Clean Store (to remove untrusted apps from U.S. mobile app stores), Clean Apps (to prevent untrusted Huawei and other Chinese smartphone manufacturers from pre-installing—or otherwise making available for download—trusted apps on their apps store), Clean Cloud (to prevent U.S. citizens' most sensitive personal information and businesses' most valuable intellectual property from being obtained by cloud-based systems built or operated by Chinese vendors, such as Alibaba, Baidu, and Tencent), and Clean Cable (to ensure that information transmitted through the undersea cables connecting the U.S. to the global Internet is not compromised or leaked). The U.S. made such a big move in a nominal attempt to achieve the Clean Network free from Chinese elements, but was actually trying to maintain the global surveillance network under its control. This move was building unclean networks indeed.

— In December 2020, the Federal Communications Commission (FCC) refused to remove Huawei from its national security threat list. The FCC previously

said it formally listed China's Huawei and ZTE on the so-called "threat list." The move meant that U.S. companies would not be allowed to buy equipment from these Chinese companies through a US$8.3 billion government fund. It dates back to May 2019, when Trump signed an Executive Order prohibiting U.S. companies from using "telecommunications equipment made by companies posing national security risks," and added Huawei to its trade blacklist.

— In January 2021, Trump signed an Executive Order "Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies," to address the threat posed by applications and other software developed or controlled by Chinese companies, prohibiting any transaction by any person subject to the jurisdiction of the U.S. with persons that develop or control the eight Chinese apps or with their subsidiaries: Alipay, CamScanner, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat Pay, and WPS Office. This is on the ground that these apps can obtain Americans' personal and proprietary information—which would permit the Chinese government to track the locations of Federal employees and contractors, and build dossiers of personal information.

A series of events shows that data security has been put at the forefront of great power rivalry, and is used as the main pretext for the hegemonic country to stigmatize China. Technological, capital, talent, and material flows are all driven by information flow. Data security is essentially related to global topics such as politics, economy, culture, and military affairs. In recent years, international rules and bilateral or multilateral agreements in international trade and security are also deeply related to data security. As the focus of

international governance, data security is having a far-reaching impact on global political and economic development.

To this end, China will demonstrate its role as a responsible major country and inevitably respond to U.S. surveillance.

Global Initiative on Data Security

Cyberspace is a new domain of human activity and a new field for governance. Problems such as unbalanced development, inadequate rules, and inequitable order in cyberspace have become more prominent, increasingly exploited by certain countries to openly exercise data hegemony at will. The world calls for rules, and justice delayed is justice denied. On September 8, 2020, Chinese State Councilor and Foreign Minister Wang Yi delivered a keynote speech entitled "Upholding Multilateralism, Fairness and Justice and Promoting Mutually Beneficial Cooperation" at the high-level session of an international seminar under the theme "Seizing Digital Opportunities for Cooperation and Development." Wang Yi pointed out that China has taken a constructive part in multilateral discussions on data security including at the UN, G20, BRICS and, the ASEAN Regional Forum, contributing China's input to global digital governance. In view of the new issues and challenges emerging in this field, China would like to propose a Global Initiative on Data Security, and looks forward to the active participation of all parties.

The initiative will set a blueprint for international rules on data security and mark the start of a global process in this area. China believes that to effectively

address the risks and challenges to data security, the following principles must be observed:

First, upholding multilateralism. Pursuing extensive consultation and joint contribution for shared benefits is the right way forward for addressing the deficit in global digital governance. It is important to develop a set of international rules on data security that reflect the will and respect the interests of all countries through broad-based participation. Bent on unilateral acts, a certain country keeps making groundless accusations against others in the name of "clean" network and used security as a pretext to prey on enterprises of other countries who have a competitive edge. Such blatant acts of bullying must be opposed and rejected.

Second, balancing security and development. Protecting data security is essential for the sound growth of digital economy. Countries have the right to protect data security according to law. That said, they are also duty-bound to provide an open, fair, and non-discriminatory environment for all businesses. Protectionism in the digital domain runs counter to the laws of economic development and the trend of globalization. Protectionist practices undermine the right of global consumers to equally access digital services and will eventually hold back the country's own development.

Third, ensuring fairness and justice. Protection of digital security should be based on facts and the law. Politicization of security issues, double standards and slandering others violate the basic norms governing international relations, and seriously disrupt and hamper global digital cooperation and development.

Data security topics are very inclusive and closely related to supply chain, intelligence interception, cyberattacks, law enforcement and forensics, cross-border trade, IT product security design, and industry monopoly. Almost all of these fields are covered during the U.S. practices of exploiting global data, as well as its moves against China. Previously, there was a lack of global data security rules, let alone any comprehensive solutions to addressing difficulties in data governance. Protection of data security is not the responsibility of any single party; instead, it is related to both governments and enterprises. The Global Initiative on Data Security proposes comprehensive commitments on data security to national governments, international organizations and all other stakeholders, and calls on states to support the commitments laid out in the Initiative through bilateral or regional agreements.

First, approach data security with an objective and rational attitude, and maintain an open, secure, and stable global supply chain.

Second, oppose using ICT activities to impair other states' critical infrastructure or steal important data.

Third, take actions to prevent and put an end to activities that infringe upon personal information, oppose abusing ICT to conduct mass surveillance against other states or engage in unauthorized collection of personal information of other states.

Fourth, ask companies to respect the laws of host countries, desist from coercing domestic companies into storing data generated and obtained overseas in one's own territory.

Fifth, respect the sovereignty, jurisdiction, and governance of data of other states, avoid asking companies or individuals to provide data located in other states without the latter's permission.

Sixth, meet law enforcement needs for overseas data through judicial assistance or other appropriate channels.

Seventh, ICT products and services providers should not install backdoors in their products and services to illegally obtain user data.

Eighth, ICT companies should not seek illegitimate interests by taking advantage of users' dependence on their products.

In November 2020, Chinese President Xi Jinping addressed the 15th G20 Leaders' Summit and stated, "To address countries' concerns on data security, the digital divide, personal privacy and ethics, we should adopt people-centered and facts-based policies to encourage innovation and build trust. We should support the UN's leadership role in this field, and work together to foster an open, fair, just and nondiscriminatory environment for building the digital economy. Recently, China launched the Global Initiative on Data Security. We may work on that basis and join other parties for discussing and formulating rules on global digital governance.

Building the Capability to Maintain National Cybersecurity in an Open Environment

Warlike will perish; forgetting war will be dangerous. In the face of the aggressive posture of the U.S. in cyberspace, a country should have basic tools in place to maintain its own security. However, cyberspace has become a global village where countries are bound together by intertwined interests. Any attempt to achieve security by isolating networks and excluding specific products only by the country of origin is contrary to the openness nature of cyberspace and will not achieve real security.

How to build the capability to maintain national cyberspace security in an open environment and how to ensure supply chain security while being subject to others have become a challenge for all non-U.S. countries around the world. China has always emphasized the importance of addressing the relationship between security and development, and between openness and autonomy in its cyber practices.

China will not reject any new technologies as they are products of the development of human civilization. Independent innovation in China is not about making cars behind closed doors, not fighting alone, rejecting advancements, or being isolated from the outside world. China treats foreign technologies and products equally, and does not discriminate by the country of origin. To ensure supply chain security, China has established a cybersecurity review system. In April 2020, the Cyberspace Administration of China and other 11 ministries jointly released the Cybersecurity Review Measures, and officially started cybersecurity reviews thereafter.

China's cybersecurity review system is implemented for the only purpose of maintaining national security. Article 59 of the National Security Law of the People's Republic of China requires that the state establishes a system and

mechanism for national security review and regulation, and conduct national security review on network information technology products and services that affect or may affect national security as well as other major affairs and activities. The article makes it clear that cybersecurity review is a "national security review." Article 35 of the Cybersecurity Law of the People's Republic of China stipulates that critical information infrastructure (CII) operators purchasing network products and services that might influence national security shall undergo national security review organized by the national network information department and relevant departments of the State Council. This article emphasizes again that cybersecurity review is oriented to national security. After the release of the cybersecurity review system, especially under the hyping up of distortions by some foreign media outlets, foreign companies were extremely worried about its impact. However, it has been proved that there is not any slightest impact on both Chinese and foreign companies that operate legitimately.

China's cybersecurity review system focuses on assessing the potential risks to national security brought by CII operators' purchase of network products and services. Risk assessment mainly considers the following factors: (1) The risk that the use of products and services could bring about the illegal control of, interference with, or destruction of CII, as well as the risk of theft, leakage, or damage of important data; (2) The harm of product and service supply disruptions to CII business continuity; (3) The security, openness, transparency, and diversity of sources of products and services, the reliability of supply channels, as well as the risk of supply disruptions caused by political, diplomatic, and trade factors; and (4) Product and service providers' compliance with applicable Chinese national laws, administrative regulations, and department rules.

China's cybersecurity review system does not restrict or discriminate against foreign products or services; instead, it fully protects enterprises' trade secrets and intellectual property rights. Cybersecurity review targets both Chinese and foreign products, and does not consider the country of origin for assessing risks. Cybersecurity review fully respects and strictly protects enterprises' intellectual property rights. Relevant agencies and personnel involved in a cybersecurity review shall strictly protect enterprises' trade secrets and intellectual property rights, and shall undertake confidentiality obligations for undisclosed materials received, and other undisclosed information learned during the review.

China does not conduct cybersecurity review on a routine basis; instead, it is more like a deterrent. Network products and services used by CII within the territory of China are subject to review if they threaten or may threaten the national security of China. If a review procedure is initiated, product and service providers may face high costs of reputational damage, or lose market opportunities, with serious consequences. Products that have exposed national security risks and enterprises that have actively cooperated with U.S. intelligence agencies should be added to the review list. In particular, some multinational corporations were busy cooperating with the Trump administration and playing the U.S. pawn role to contain China. They cut off supplies to China on the grounds of the so-called extra-territorial application of laws of their local country. Such enterprises should also be covered in the review.

China's Data Security Protection Initiatives Contribute to Global Data Governance

When the EU GDPR went into effect in 2018, it shocked the whole world by ushering in a new era of data protection. Many U.S. agencies and companies criticized that the effect of the GDPR seems to take them "back to the middle ages." Rather, Chinese officials, research institutes, and industry associations all hold a positive attitude toward the GDPR. In particular, Chinese companies that have entered international markets proactively enhance their compliance with the GDPR.

China has been actively exploring new ideas and approaches for protecting data security, contributing to global data security protection.

China has made continuous efforts to improve its legal system for data protection. Since 2000, the Chinese government has continuously built a solid foundation for its legal system for personal information protection by enacting a series of laws and regulations, such as the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection, Cybersecurity Law, E-Commerce Law, Regulations on Network Protection of Children's Personal Information, Provisions on Protection of Personal Information of Telecommunications and Internet Users, Personality Rights in the Civil Code, and Criminal Law provisions against violations related to personal information. Chinese State Councilor and Foreign Minister Wang Yi emphasized that China has clear legal provisions for protecting the legitimate rights and interests of citizens and organizations, covering data security and personal information. The Chinese government has acted in strict compliance with data security principles. We have not and will not ask Chinese companies to transfer data overseas to the government in breach of other countries' laws. In addition, the National People's Congress's enactment of the Data Security Law and Personal Information Protection Law

is under way, and the first round of public consultation was completed in 2020. Both laws aim to protect, standardize, and promote. The Personal Information Protection Law provides a section "Special Provisions on the Processing of Personal Information by State Organs" under the chapter "Rules for Processing Personal Information" to restrict state organs in processing personal information and prevent the abuse of personal information.

China is establishing a data security standards system. In addition to adopting international standards, China's National Information Security Standardization Technical Committee has developed a number of national standards for key technologies, typical scenarios, and important links in protecting personal information, many of which are the first to develop internationally. Standards and specifications already released include: GB/T 35273-2020 Personal information security specification, GB/T 37964-2019 Guide for de-identifying personal information, GB/T 37988-2019 Data security capability maturity model, GB/T 39335-2020 Guidance for personal information security impact assessment, and GB/T 39725-2020 Guide for health data security. Standards and specifications under development include: Personal Information Security Engineering Guide, Guidelines for Personal Information Notice and Consent, Basic Specifications for Personal Information Collection by Mobile Internet Apps, Security Specifications for Network Data Processing, Guideline for Security Assessment on Cross-border Data Transfer, Specifications for Grading and Evaluating Personal Information De-identification Effect, Security Assessment Specifications for Personal Information in Mobile Internet Apps, and Mobile Internet App SDK Security Guide. It should be noted that a significant proportion of foreign enterprises have participated in drafting these standards and specifications, and the drafting process is open to the public.

China has learned from and expanded the GDPR. The GDPR is welcomed and treated with courtesy wherever it is in China. This shows China's respect for international rules and foreign best practices. To closely align China's personal information protection with the international community, China makes full use of the GDPR and developed GB/T 35273-2020 Personal information security specification based on specific practices in China's Internet governance. This standard is the foundation of a series of personal information security specifications of China. In this regard, China's requirements for personal information protection are consistent with those of the GDPR.

China has proposed the concept of important data and planned to establish a comprehensive data protection system. So far, data protection practices in Europe and the U.S. have focused on personal information. However, there is another category of data between state secrets and personal information, such as genetic data and geographic information with certain precision. Such data is also related to national security and should be protected. In response, China's Draft Data Security Law stipulates that the state shall implement data protection at different grades and classifications, and each region and department shall determine a regional, departmental, and sectoral important data protection catalog and undertake special protection for that listed in the catalog. A comprehensive protection system can be established only when different categories of data are classified, which constitutes true accountability for the people and state. However, there is also doubt that the concept of important data proposed by China is not an international practice and is suspected of expanding the appropriate scope of protection. Then, we will have to ask, are intellectual properties categorized as data to be protected? It is forbidden to take photos at security checkpoints at airports, customs control zones, banks, and other sensitive areas. Are photos taken in such areas

categorized as data to be protected? I think China's exploration in this area is of great significance to the improvement of global data protection practices. With regard to the doubt, such people must be looking forward to loopholes and weaknesses in China's data protection.

China has creatively developed new data protection policies for the governance of mobile Internet apps. The whole world is making tremendous efforts to refine the rules for personal information protection. China's experience in market oversight, however, shows that no matter how refined the rules are, there are always cases where loopholes are exploited to circumvent the rules. To this end, China has developed the Measures for Identification of Illegal Collection and Use of Personal Information by Apps and implemented special governance actions. In the mobile Internet era, it is prevalent to integrate various functions to apps to seize the Internet traffic entrance and increase user loyalty. In this case, bundled consent and collection of personal information beyond the authorized scope prevail for apps. To address these issues, China has enacted the Scope of Necessary Personal Information Required for Common Types of Mobile Internet Apps, specifying 38 common types of apps, such as map navigation, online car-hailing, and instant messaging, as well as the core functions, minimum permissions, and scope of necessary personal information that these apps may collect and use. In May 2018, a criminal offense occurred in Zhengzhou, Henan Province, China. An online car-hailing driver, who indulged in the dating function of the online car-hailing app, killed a flight attendant. This shows the importance of standardizing the main functions of apps.

Conclusions

Currently, the mounting risks of data security have put national security, public interests and personal rights at stake, and posed new challenges to global digital governance. The constant and massive cross-border data flow puts to the test the governance capacity of national governments in terms of governance philosophy, legislative framework and regulatory mechanism. The divergence of data laws and regulations in different countries has pushed up the compliance costs for global businesses. Countries, although varied in national conditions, development stage of Internet and challenges, hold the same desire for promoting digital economy, same interests in tackling cybersecurity challenges and same expectations for strengthened cyberspace governance. Countries face a pressing need to step up communication and coordination, build up mutual trust, and deepen cooperation with one another.

However, the anti-China camp led by U.S. politicians has been deliberately slandering China for a long time and imposing worldwide bans on China's 5G on so-called date security grounds. Under the political manipulation of the U.S., politicians in some countries have become subordinates to the U.S. They are politicizing technical matters, violating the constitutions and laws of their countries and the principle of fair market competition, and excluding China's 5G on fabricated charges. They not only abandon the use of new technologies to the detriment of their people, but also put their country into the new landscape of U.S. surveillance in the 5G era.

What's wrong with the world? What can we do now?

Let's hope everything will return to reason and rationality.

195-15 Tianlin Road, Xuhui,Shanghai, PR.China

021-54614900|www.siis.org.cn