China Cybersecurity: No Place to Hide

September 24, 2020

Authored by Steve Dickinson

I. Cybersecurity with Chinese Characteristics: The Party is the leader of everything.

Under the guidance of the Chinese Communist Party (CCP), the Chinese government is working to create a cybersecurity system with Chinese characteristics. This system is designed to make all networked information that crosses the Chinese border a) transparent to the Chinese government and b) closed to unauthorized access by foreign and domestic hackers and governments not affiliated with the CCP.

The primary goal is to use this system for surveillance and control. Surveillance means acquisition of information. As a result, the transparency of the system means all information that crosses the Chinese border should be available to the CCP and its agents. There are no secrets from the Party. As a result, from the standpoint of an individual or a business entity, whether domestic or foreign, this system is a cyber-insecurity system. As the system is implemented with progressively greater refinement and scope, there will be no place to hide from the eyes of the party.

All foreign entities operating within China are subject to this cyber-insecurity system. Since network systems and communication are central to the work of every modern company, understanding how the Chinese system operates is essential. The impact is not limited to foreign entities that establish foreign invested enterprises in China. It also applies to anyone who transmits information, personal or technical, into China via any network. It also applies to any person who transmits information into any country in which the Chinese digital authoritarianism system has been implemented through the Digital Silk Road project. It also applies to anyone who transmits information into any country or region (Hong Kong/Taiwan) that has become the target of Chinese based data gathering operations.

To understand the basis of this system, certain features of the current Chinese system of government must be understood. First, we must understand the role of the CCP. There are two key features:

One, the CCP has been recognized as the "leader on everything". Under Deng, Jiang and Hu, the goal was to remove the Party from the dominant leadership role so as to release the

economic and creative power of the people and non-party institutions. This plan worked so well that many in China began to question the role of the Party.

The primary goal of the Xi Jinping administration has been to reverse this trend. Through the efforts of Chairman Xi, the CCP is now the leader on everything. There is no limit on its role in directing all aspects of China. Accordingly, in 2018 the CCP constitution was revised to state:

> The leadership of the CCP is the primary characteristic of socialism with Chinese characteristics. The Party, government, military, civil and education, north, south, east, west and the center, the Party is the leader on everything.
>
> 中国共产党的领导是中国特色社会主义最本质的特征，是中国特色社会主义制度的最大优势。党政军民学，东西南北中，党是领导一切的。

This statement is a rejection of the policy of Deng, Jiang and Hu. It hearkens back to the position of Mao Zedong as stated in 1962. 1962 年 1 月 30 日，中国共产党中央委员会主席毛泽东在扩大的中央工作会议.

Though the CCP is the leader on everything, the primary goal of the Party is to lead in economic development. As stated in the Preamble to the CCP Constitution:

> In leading the cause of socialism, the Communist Party of China must continue its commitment to economic development as the central task, and all other work must take an ancillary role and serve this center. The Party shall implement the strategy for invigorating China through science and education, the strategy on developing a quality work force, the innovation-driven development strategy, the rural vitalization strategy, the coordinated regional development strategy, the sustainable development strategy, and the military-civilian integration strategy. It shall give full play to the role of science and technology as primary productive forces and the role of innovation as the primary force driving development, draw on advances in science and technology, improve the quality of the country's workforce, and ensure higher-quality and more efficient, equitable, and sustainable development of the economy.

In keeping with this broad role, the CCP has also greatly expanded the concept of national security. Under Xi Jinping's Comprehensive National Security Concept (总体国家安全观), the traditional military, protection of borders approach to national security is transformed. Under the new security concept, two features are critical. First, the primary goal is to preserve the absolute power of the CCP as ruler of China. Second, the focus is on these threats to CCP power:

-- Failure of the PRC to develop quickly into a high technology country.

-- Failure of the Party to control ideology and information.

The cybersecurity concerns of private persons and business entities do not enter into the analysis. It is the Party that must be protected, not the public. In particular, it is not possible for any member of the public to be in conflict with the Party. Any such conflict is anti-Party and therefore anti-China. This issue is not addressed in any way. All of this is explained in detail in the standard collection of Xi Jinping's speeches and writings on the comprehensive national security concept: 习近平关于总体国家安全观论述摘编，2018. A good summary in English can be found at Matthew D. Johnson, *Safeguarding Socialism: The origins, evolution and expansion of China's total security paradigm*,

In order to be the leader on everything, the Party has to know everything. In the cyber realm, the CCP and its agencies have responded to this need to know in two ways:

Domestically, the CCP has embraced digital technology to create a surveillance state within China. Through facial recognition, control of the Internet, mobile phone, WeChat and related sources of information monitored and controlled through AI and big data, the PRC has created a surveillance and control system that has been termed digital authoritarianism. See U.S. Senate Committee on Foreign Relations, *The New Big Brother: China and Digital Authoritarianism*.

Internationally, the Party and its agents, the Ministry of State Security (MSS) and the Ministry of Public Security (MPS), have become the primary cyber-hackers of technology and trade secrets. The role of the MSS in cyber-hacking is well documented. Recent criminal indictments and U.S. and foreign government responses can be found here for the United States and here for the United Kingdom.

What then is the CCP?

1. The CCP is the CEO of Chinese state owned and private businesses that direct compete with foreign entities.
2. The CCP is the director of the research centers charged with developing technology per the Made in China 2025 program and other high-speed high-tech development projects.
3. The CCP is commander in chief of the Chinese military, a military from which foreign persons are banned from dealing. Under the doctrine of civil/military fusion, the military has access to all information and technology obtained by the CCP.
4. The CCP is the manager of the worldwide cyber hacking system conducted by the MSS and the People's Liberation Army (PLA), along with the domestic cyber hacking system conducted by the MPS.

The Party is entirely in control of this system. The Party is the leader of everything: north, south, east, west and center. Any attempt to defeat this system is doomed to failure. All networks and digital data within the Chinese border will be made transparent to the CCP with no exceptions. There is no place to hide.

So, how does it work? That will be discussed below.

II. China's Comprehensive Network Security Program.

The Chinese government has been working for several years on a comprehensive Internet security/surveillance program. This program is based on the Cybersecurity Law adopted on 2016. The plan is vast and includes a number of subsidiary laws and regulations. On December 1, 2018, the Chinese Ministry of Public Security announced it will finally roll-out the full plan.

The core of the plan is for China's Ministry of Security to fully access the massive amounts of raw data transmitted across Chinese networks and housed on servers in China. Since raw data has little value, the key to the Ministry's success will be in processing that data. Seeing that this is the key issue, the Ministry has appointed Wang Yingwei as the new head of the Cybersecurity Bureau. Wang is a noted "big data" expert and he will be tasked with making sense of the raw data gathered under the new system.

The plan for the new system is ambitious and comprehensive. As explained by Guo Qiquan, the chief cheerleader for the plan, the main goal of the new system is to provide "full coverage". "It will cover every district, every ministry, *every business* and other institution, basically covering the whole society. It will also cover all targets that need [cybersecurity] protection, including all networks, information systems, cloud platforms, the internet of things, control systems, big data and mobile internet."

This system *will apply to foreign owned companies* in China on the same basis as to all Chinese persons, entities or individuals. No information contained on any server located within China will be exempted from this full coverage program. No communication from or to China will be exempted. There will be no secrets. No VPNs. No *private* or encrypted messages. No anonymous online accounts. No trade secrets. No confidential data. Any and all data will be available and open to the Chinese government. Since the Chinese government is the shareholder in all SOEs and is now exercising *de facto* control over China's major private companies as well, all of this information will then be available to those SOEs and Chinese companies. *See e.g.* China to place government officials inside 100 private companies, including Alibaba. All this information will be available to the Chinese military and military research institutes. The Chinese are very clear that this is their plan.

In the past, foreign owned companies in China were generally able to avoid the impact of this type of system in two ways. They did this primarily by establishing VPN internet servers in their own offices. These servers used VPN technologies to isolate data from the Chinese controlled networks, allowing for a company intranet to maintain the secrecy of emails and data stored on the company servers in China. As cloud computing has advanced, foreign owned companies typically use the same VPN technologies to isolate their cloud-based servers from the Chinese controlled system. Though the Chinese authorities often complained about these VPN systems, foreign companies were usually able to claim their special WFOE status exempted them from Chinese data controls.

However, with the roll-out of the new system, that will all change. First, the Cybersecurity Law and related laws and regulations are clear that they apply to *all* individuals and entities in China *without regard to ownership or nationality*. There are no exceptions. More important, the new Foreign Investment Law that went into effect on January 1, 2020 eliminates any special status associated with being a WFOE or other foreign invested enterprise. Foreign owned companies will be treated in exactly the same way as Chinese owned companies. See China's New Foreign Investment Law Benefits: Like Putting Lipstick on a Pig. This means the Cybersecurity Law will apply to foreign owned companies (WFOEs, joint ventures, and Representative Offices) in the exact same way it applies to Chinese owned companies and individuals. There will be no place for foreign owned companies to hide.

This means using intra-company VPN systems will no longer be authorized in China for anyone, including foreign companies. This in turn means all company email and data transfers will be required to use Chinese operated communication systems fully open to China's Cybersecurity Bureau. All data servers that make any use of Chinese based communications networks will also be required to be open to the Cybersecurity Bureau's surveillance and monitoring system.

It is important to fully understand what this means. Under the Cybersecurity Law, the Chinese government has the right to obtain from *any* person or entity in China *any* information the Chinese government deems has *any* impact on Chinese security. The Chinese government understands foreign companies and individuals will be reluctant to simply turn over their information to the Chinese government when asked. For that reason, the Chinese Cybersecurity Bureau does not plan to politely make a formal request for the information. The fundamental premise of the new cybersecurity systems is that the government will use its control of communications to simply take the information without discussing the matter with the user. All data will be open to the Chinese government.

This system of constant and pervasive access to and monitoring of data sets up a fundamental conflict for U.S. and many foreign companies operating in China because U.S. law in many cases mandates much information be kept secret. But Chinese law now

requires complete government access to those secrets if those secrets cross the Chinese border for any reason. This conflict puts many U.S. and foreign companies in an impossible legal bind. I include foreign companies because foreign companies with U.S. subsidiaries or even certain sorts of relationships with U.S. companies will also be bound or at least impacted by these U.S. secrecy laws.

First, as the scope of what the U.S. government designates as controlled information and technology begins to expand, the restrictions on what cannot be transmitted across the Chinese border increases. See this post on what will likely constitute a restricted "emerging technology" under U.S. law. U.S. companies used to take the position that their information in China is on a private server isolated from the Chinese government and if the Chinese government requests this information, "we will refuse to comply." This argument will no longer work because the Chinese government will no longer ask for the information; it will simply take it.

Second, much intellectual property is protected as a trade secret rather than because it is registered as a patent. In fact, the value of many U.S. patents lies in its supporting trade secret know-how. Trade secrets are a form of property protected under U.S. law. However, the general rule for being able to maintain something as a trade secret (under U.S. and China and EU law) is that the holder of the trade secret must take reasonable steps to maintain its secrecy. Once a trade secret has been intentionally or unreasonably revealed by its holder, its protection as trade secret property is terminated. This then leads to the conflict.

Under the new Chinese system, as a practical matter, trade secrets hidden from the CCP will no longer exist. This means U.S. and EU companies operating in China will now need to assume any “secret” they seek to maintain on a server or network in China will automatically become available to the Chinese government and then to all their Chinese government controlled competitors in China, including the Chinese military. This includes phone calls, emails, WeChat messages and any other form of electronic communication. Since no company can reasonably assume its trade secrets will remain secret once transmitted into China over a Chinese controlled network, they are at great risk of having their trade secret protections outside China evaporating as well.

The U.S. or EU company may have an enforceable agreement with the Chinese recipient of its confidential information that protects that information with respect to that authorized recipient. But if the secret is easily available to the Chinese government, there is no real trade secret protection.

By giving the Chinese government and its cronies full access to its data, the U.S. or EU company may very well be deemed to have illegally exported technology to China, and it could face millions of dollars in fines and even prison sentences for some of its officers and

directors. There is an inherent conflict between foreign laws mandating a company *not* transfer its technology to China and China's laws which effectively mandate that transfer.

III. China's Regulatory System: The Multi-Level Protection Scheme (MLPS 2.0).

A core concept in the CCP system of control is that China must be ruled by law. The law is the expression of the will of the Party. That expression of will must be clear and inflexible. In keeping with that basic policy, the cybersecurity system that will be rolling out over the next decade is documented in detail as the Cybersecurity Multi-level Protection Scheme ("MLPS 2.0"), which is came into effect on December 1, 2019. This scheme sets out the technical and organizational controls *all* companies and individuals in China must follow to comply with MLPS-related Internet security obligations mandated by China's Cybersecurity Law. All companies and individuals must abide by the following three standards:

1. GB/T 22239 – 2019 Information Security Technology – Baseline for Multi-level Protection Scheme

2. GB/T 25070 – 2019 Information Security Technology – Technical Requirements of Security Design for Multi-level Protection Scheme.

3. GB/T 28448 – 2019 Information Security Technology – Evaluation Requirements for Multi-level Protection Scheme.

The Chinese language versions of these standards can be found here; I am not aware of any English language translations of these standards.

My personal file on the laws and regulations relating to the MLPS 2.0 system consists of 800+ pages of very technical Chinese. But even this vast documentation is not sufficient to fully understand the function of the system. To fully understand all this, one must also consider the objectives of other key Chinese government planning documents, such as the national artificial intelligence program, the Internet+ program, the social credit system for individuals and businesses (See China's New Company Tracking System: Comply, Comply, Comply), and various other network/Internet/data gathering and surveillance programs being implemented in China.

When one examines these various different programs together, it becomes apparent the MLPS 2.0 system is the "hardware" component of a comprehensive data gathering, surveillance and control program. China's plan is to create a system that covers *every* form of network activity in China: Internet, mobile phone, WeChat type social networks, cloud systems, domestic and international email. China's goal is *not* to create a commercial system

where individual players can participate and make money. Its goals are surveillance and control by the PRC government and the CCP.

To achieve those goals China is creating a system to achieve two ultimately contradictory objectives: the system will be closed against intrusion by "bad actors" (foreigners and internal dissidents), but completely transparent to the Ministry of Public Security and other internet security agencies of the PRC government and the CCP. Transparency to the Ministry of Public Security means what it says: No technology that blocks access by the Ministry of Public Security is permitted. No VPN, no encryption, no private servers. If the Ministry of Public Security is required to install back doors or other message/data interception devices or systems to achieve full access, then China Telecom and Chinese based ISPs are r*equired* to comply. But because providing open access to the Ministry of Public Security directly conflicts with the goal of hardened security from intrusion, how to mediate between these conflicting goals is the chief reason for the length and complexity of the MLPS 2.0 standards.

The legal basis for allowing China's Ministry of Public Security to access networks and data comes from a regulation not included within the MLPS 2.0 standards. As I noted above, full understanding requires pulling together all the applicable regulations. This is just one example of this. The written regulations that give the Ministry of Public Security the right to just "take it" are the Regulation on Internet Security Supervision and Inspection by Public Security Organs (公安机关互联网安全监督检查规定). This regulation was promulgated on September 15, 2018 and came into effect on November 1, 2018. My references to this regulation below are to the articles of the Chinese language version published by the Chinese government. It is important to base comments on the Regulation on what was actually adopted, not to earlier discussion drafts containing provisions that were not adopted.

As a preliminary issue, a key matter confirmed by the Regulation on Internet Security Supervision and Inspection by Public Security Organs is that the Ministry of Public Security has lead authority to take on the front-line enforcement duties related to the Internet and to network security in China. This means MIIT (China Telecom), CAC, CNNIC and the alphabet soup of other Chinese agencies that sought a role in cybersecurity administration have been pushed aside in favor of the Ministry of Public Security. This means enforcement will be handled by the police rather than by local bureaucrats. This decision on enforcement has real meaning for foreign companies doing business in China and for its foreign employees who live and work there. When a Chinese bureaucrat shows up at your door asking for information, you can perhaps send that bureaucrat on his or her way. But when two or more uniformed police officer show up at your door, you have no option but to comply.

The Regulation on Internet Security Supervision and Inspection by Public Security Organs provides for two levels of inspection of networked servers: on-site inspection and offline, remote access. *See* Article 13. When an on-site inspection is conducted, a minimum of two

local police officers must be present. *See* Article 14. The police officers will be accompanied by local government agency staff charged with Internet security. If local government agency staff are not sufficient, the Ministry of Public Security may employ independent contractors to do the work.

The inspection team has complete access to the network system. Inspection can cover both the technical aspects of the network system *and the data/information maintained on the servers*. *See* Article 10.

The inspectors can fully access the system and copy any data they find. *See* Article 15. The only restriction on the inspectors copying the data in your company's system is that they must provide you with a receipt. Though Article 10 "restricts" access to matters involving national security, the definition of national security in China is so broad there is no real limitation on what can be accessed, copied and removed.

In cases where the Ministry of Public Security determines there is an Internet security issue, it has the right to perform a remote access inspection. the scope of which is set out in Article 10. Prior notice of remote access is required. There are two issues related to such notice: First, the purpose of the notice is *not* to protect the rights of the party being inspected. Rather, the purpose of the notice is to ensure that the server has been completely opened to access by the Ministry of Public Security. Second, for servers maintained by a cloud provider, it is not clear whether notice goes only to the cloud provider or to both the cloud provider and its customer(s). It is therefore not clear whether the cloud customer will ever receive notice that its server and data were viewed and copied by China’s Ministry of Public Security. Time will tell on this, but my guess is the cloud customer will never know unless its cloud provider tells them, which is unlikely.

This off-site access rule is awkward to manage. The structure of the MLPS 2.0 standards suggest the Ministry of Public Security plans to work with cloud providers and Managed Service Providers to get them to install systems that will allow the Ministry of Public Security easy off-site access at any time, without need to go through an incident by incident prior notice then access procedure. However, this type of constant access system is not contemplated by the Regulation. Even if the Regulation on Internet Security Supervision and Inspection by Public Security Organs is strictly followed, there is no getting around the fact that it provides for China's Ministry of Public Security to have essentially unfettered access to all servers and data. Referring to this as "cybersecurity" is fundamentally misleading. As the Regulation itself states, this is a regime for inspecting and controlling by the Chinese government. It has nothing to do with cybersecurity as normally considered in the open Internet world.

The key issue then becomes what happens to the data collected by China's Ministry of Public Security --your company's data, for instance. The Ministry is permitted to copy and remove virtually any information or data it finds on the servers it inspects. What about the

confidentiality of that information? Article 5 of the Regulation on Internet Security Supervision and Inspection by Public Security Organs addresses this issue : "The personal information, privacy, trade secrets and state secrets that the public security organs and their staff members are aware of in the fulfillment of the duties of Internet security supervision and inspection shall be strictly kept confidential and shall not be disclosed, sold or illegally provided for others." This provision must be read carefully because it provides for "confidentiality with Chinese characteristics".

The key point is that the term "others" does *not* include any agency of the Chinese government or of the CCP. In other words, it does *not* include universities and other research centers operated or controlled by the Chinese government. It also does *not* include the Chinese military or Chinese arms manufacturers. It also does not include China's State-Owned Entities (SOEs). Though not clear, the term "others" also probably does *not* include nominally private entities controlled by the CCP. *See e.g.,* Huawei.

So again, what does this confidentiality provision mean? As applied in China, the confidentiality rule of Article 5 is intended to prevent Ministry of Public Security officers from doing two things: selling data to Chinese or foreign companies for personal profit and two, disclosing data to foreign agents (spies). This rule is *not* intended to prevent the Ministry from sharing the data it collects with the insiders described above. In fact, such sharing is mandated as part of the data needs of the entire Chinese government and the CCP. The Ministry of Public Security is not permitted to hoard the data; it is required to spread it around within China's Party- controlled system.

This result then leads to the key issue. Confidential information housed on any server located in China is subject to being viewed and copied by China's Ministry of Public Security and that information then becomes open to access by the entire PRC government system. But the PRC government is the shareholder of the State-Owned Entities (SOEs) which are the key industries in China. The PRC government also essentially controls the key private companies in China, such as Huawei and ZTE, and more recently, Alibaba and Tencent and many others. See China is sending government officials into companies like Alibaba and Geely and China to place government officials inside 100 private companies, including Alibaba. The PRC government also either owns or controls China's entire arms industry.

Simply put, the data the Ministry of Public Security obtains from foreign companies will be available to the key competitors of foreign businesses, to the Chinese government controlled and private R&D system, and to the Chinese arms industry and military.

The negative consequences of this should be obvious. But the critical issue is that the consequences go far beyond just the commercial impact. China's new systems will become a matter of national security for the U.S. and other governments. This then sets up a conflict private companies will not be able to avoid. Do they make their data available to China's Ministry of Public Security as required by Chinese law or do they keep that data from the

Ministry (and in turn the Chinese Military) as required under the laws of their home country? In other words, do they simply stop using or providing data to their China operations?

The final result will be that as far as China is concerned, "free trade" in the critical areas of technology will end up being severely curtailed. Welcome to the New Normal.

IV. Cryptography is not a solution.

The PRC National People's Congress enacted the long-awaited Encryption Law (密码法），which came into effect on January 1, 2020. The official text of the law can be found here and an English language summary can be found here.

Cryptography is a key technology that will be used to achieve the goals of the comprehensive cybersecurity program. Normally, cryptography is used to protect the confidentiality of information transmitted and stored on networks. But its use presents the Party with a dilemma: the same cryptography that hides information from the general public can also be used to hide information from the government itself. In this case, the Chinese government is presented with the issue of how it can require cryptography while still maintaining its open access to the network system.

The Law divides encryption into three categories: core, common and commercial. Core and common are intended for systems that transmit and store PRC state secrets. Commercial encryption is intended for business and private use. Foreign encryption systems can be sold in China, if approved and certified through a certification system that has not yet been described. Use of encryption will be subject to the provisions of the Cybersecurity Law and the associated MLPS 2.0 regulations. Article 26. The State Cryptography Administration (SCA), an office of the CCP, will have authority to monitor and inspect implementation and use of the cryptography system. Article 31.

This three-class system ignores the way cryptography is normally implemented. The most important cryptography systems are not commercial systems. Most systems are based on the Gnu Privacy Guard system. This is a completely open system. The source code is generally available to the public. You can download the source code here. It is not conceivable that the organizations that offer PGP systems will cooperate with the PRC government in obtaining review and certification of their product when the focus of these PGP systems is to allow companies and individuals to hide their information from the government. Cooperation with any government would be contrary to that principle.

This then leads to the first question under the new Law. Most cryptography systems are freely downloadable as open source systems. The PRC government is free to examine the source code used to implement the PGP and related open source systems. The real issue is whether the PRC government will allow companies and persons who operate in China to use PGP and related systems, given that that these systems will NEVER be submitted to the PRC government for review and approval. If the answer is no, then the entire set of provisions for foreign encryption systems is meaningless. If the answer is yes, then the designation "commercial" has no meaning.

This then leads to the most important issue. Cryptography techniques are not secret. The most important algorithms are public and available to anyone to use. Governments know exactly how the algorithms work because governments have been the inventors of most of these algorithms. The Cybersecurity Law 's focus on cryptography products is nothing more than a head fake. What is critical in cryptography is *not* protection of the cryptography algorithm; what is critical is protection of the key that allows decryption of the encrypted message or data.

The Cryptography Law is silent on the issue of decryption and it is also silent on protection of passwords and other keys that prevent decryption. Its ultimate plan is to break all forms of end to end encryption by putting all passwords and decryption keys into the hands of the PRC government and the CCP. In other words, opaque to the public but transparent to the government.

Article 31 of the Cryptography Law provides for a government inspection and control system implemented by the SCA and its local agencies. This system gives the SCA and its local agencies complete access to the cryptography system and to the data protected by that system. The systems are also subject to the MPS supervision and control system that is being implemented under the Cybersecurity Law and the MLPS 2.0 system described here and here. So both the SCA (a CCP office) and the MPS (working with the MSS) will have full access to encrypted servers, including full access to the decryption keys and the passwords. Once this access is achieved, end to end encryption disappears. For a description of how this works, see this.

In the end, inviting foreign providers and users of cryptography is just a trap for the unwary. Once data crosses the Chinese border on a network, 100% of that data will be 100% available to the Chinese government and the CCP. Cryptography may prevent access by the public, but all this data will be an open book to the PRC government.

This then raises major issues for U.S. and other country entities that rely on end to end encryption in China as an exception to U.S. export control rules. Under China's new system, end to end encryption will no longer exist in China and so this exemption from U.S. export

controls will no longer be effective. As the U.S. expands the scope of technology subject to export controls, the risks for foreign companies will become progressively more significant.

Many U.S. entities look at cryptography as their escape from China's Cybersecurity Law, but that will not work because the PRC government will not let it work. The Chinese government knows exactly what it is doing. The Chinese government has set up a system that will allow it to achieve a fully transparent system.

V. A Concrete Example: The Golden Tax Malware Program

The ultimate goal of the Chinese system is for the Party to install malware on computer systems that allows the Party and its agents full access to the system. This malware is normally some form of a remote access trojan (RAT), a malware technology in which the Chinese are world leaders. The Golden Tax malware program provides a concrete example of how this can be done.

The Chinese government and its state-controlled banks have worked hard over the last decade to "digitize" financial reporting and procedures. These days, a business operating in China virtually never needs to visit a Chinese government agency office or a bank. Transactions and reporting are done online.

For normal daily operations, this means the following are done through the Internet:

1. Day to day banking
2. Monthly tax reports
3. Monthly tax and social insurance payments
4. Issuance of VAT tax receipts
5. Periodic reports to government agencies
6. For importers/exporters, reporting to customs

If you try to do this kind of work by visiting Chinese government offices, you will be turned away.

All this appears to be modern and efficient, but this extensive use of the Internet conceals a hidden danger. In all these transactions, Chinese government agencies and the banks require the business make use of software provided by the agency or the bank. No independent software is allowed. This software is usually a package that includes connection software and anti-virus protection. In my experience, these packages are poorly

written, buggy, slow and difficult to use. When this software is installed on a business's central computer, it slows operations to the point of being unusable.

But the real issue runs deeper. As discussed above, the goal of the Chinese government is to make information networks in China closed to outsiders but completely open to the Chinese government. Once on the Internet, the goal of the system is to ensure all information can be accessed by the Chinese government. To state things more bluntly, the Chinese government has become the most active information hacker in China. The software the business is required to install on its systems is being provided to it by a hacker – the CCP. The risks are obvious.

The reality of the risk has recently been exposed by Trustwave, a U.S. based cybersecurity consultant, in its report on a case where malware was included in software required by a Chinese bank for tax payments. See The Golden Tax Department and the Emergence of Golden Spy Malware, subtitled, Trustwave SpiderLabs has discovered a new malware family, dubbed Golden Spy, embedded in tax payment software a Chinese bank *requires* corporations install to conduct business operations in China. The basic story is typical of China. The bank requires installation of its mandated software created by a private "big data" Chinese company working under contract with the Chinese national tax department. In other words, the mandate requiring use of this spyware comes straight from China's national government in Beijing.

The software contains a backdoor that takes two actions. First, all data submitted to the bank and all other data on the host computer is transmitted to a server owned by a private Chinese company connected with China's national tax department. This server is housed on the Alibaba cloud. Second, the software allows the operator of the backdoor *complete access to the entire host computer system*. Trustwave provides standard advice on best practices for dealing with this type of infection. Their advice to remove the software is, however, simply not practical, since companies are *required* to use this spyware to do business in China. Their alternative is to install the software on a dedicated laptop insulated from the main company computer system. This approach prevents infection of the main company network system. However, it does not prevent the private data transmitted to the local tax authority from being transmitted to the malware server to be used for undisclosed purposes. It also is not clear how the Chinese government will treat a foreign company that isolates its exposed data to a sole, non-networked computer.

So now we know why all this Chinese government mandated software works so badly. The software is so filled with malware, backdoors and surveillance protocols that normal operation is slowed to the point of making many systems unusable. Those of us who work in China have always assumed this and now the Trustwave report provides a concrete example.

The larger issue is that this forced installation of backdoor malware is a constant issue in China. It is not just the case of one piece of software from one bank. As this case shows, the national government works with government-controlled banks, local governments, private software/big data companies and Chinese based cloud service providers to implement a system that allows total access to all information available on the networks located in China.

It might be possible to implement protections against one single piece of malware, as Trustwave advises. But as a practical matter, it is impossible to implement protection against the constant and pervasive measures the Chinese government takes to access private company data. There are too many points of access. For example, government mandated inspection of company networks allows for installation of similar backdoor malware as part of the inspection process.

The issue is not simply the compromise of the China based system of foreign investors. Once the China system is compromised, the hacker (Chinese government) can almost always then gain access to the entire international network linked to the hacked system. The infection spreads from China around the world. Informatization, big data and full spectrum dominance is the Chinese government's highest priority. This has important implications for companies operating in China and this reality must be carefully assessed.

The standard response to the tax malware risk from cybersecurity consultants is to claim Western-style cyber security measures can be successfully used to defend against government lead hacking in China. These proposals will not work, and the suggestion they will work creates a false sense of security that actually increases risk. To put it starkly, in China, the government itself is the hacker and it will not allow foreign or domestic technicians to provide services that will defeat the hacker's ultimate goals.

Let me explain why the normal cybersecurity techniques will not work.

Cybersecurity consultants usually start by explaining how setting up banking operations on a separate laptop can seal the compromised site from the safely protected main site. The use of a dedicated laptop for banking purposes is standard practice in China. I did that in China myself when I had to step in to help run a company there. The reason a separate laptop is required reveals where the problems lie. The Chinese bank software is written so it will only run on a Chinese version of the Windows operating system.

Moreover, it will only run on an outdated, unpatched, unsupported version of Windows -- usually an outdated version of Windows 7. The reason is that the malware hidden in the software depends on exploiting various flaws that are endemic in unpatched Windows operating systems. For this reason, anyone using a dual language, patched, supported version of Windows 10 simply cannot make use of the bank provided software. Use of the separate laptop is therefore forced.

In the daily life of a normal business in China, this use of a separate laptop becomes completely impractical. It is important to understand that under the new system I described, the entire financial and regulatory life of a business in China is done over the Internet. For full protection, then, we would need multiple separate laptops: one for each bank, one for the tax department, one for VAT receipts, one for the local government, one for the national government, one for freight forwarders, one for customs, one for the (government controlled) accountant, one for the bookkeeper, and one for the employee benefits service. The list becomes endless. There is thus pressure to combine all these software systems onto one single laptop. This laptop is then used throughout the entire working day. It is not linked to the receiver (let's say the one bank) and then immediately shut down. It remains linked to someone on the Internet for virtually the entire day.

But wait, it gets worse. Now all of the business's important data is located on one or more dedicated laptops sealed off from the company's main system. But to do business, the company needs the data from its laptops to go to its main system. Imagine for just a minute if all your company's bank information were on one laptop in one office and not a part of your main system. So data from the laptops has to be regularly transmitted to the main system.

Not only must data from the laptop go to the main system at some point for the company to function at all smoothly, but it is also necessary for data from the main system go to the laptop for use of the various systems located on the laptops. Again, just imagine how you will smoothly move only certain financial data from your main system to your laptop every day.

As a practical matter, it is not possible to keep the systems separate and during these required data transfers, your door is opened for malware infection. In the most primitive way, malware is transferred when a thumb drive is used for data transfer. However, many businesses just do the data transfer through some form of Ethernet or wireless link between the various systems. In some cases, companies just give up and shift all their important financial operations to the dedicated laptop, or even to a Chinese Windows desktop.

This is what actually happens on the ground in China, and there is no way to prevent it. Foreign owned companies in China will often install a system based on advice from a foreign cybersecurity expert. They will use patched, updated operating systems, the most modern anti-virus protections, the best cryptography and a sophisticated VPN. This work is all in vain because when a network connection is required, China Telecom or some other Chinese government agency will install the network system. And they will say it is fine for you to use these systems for your personal purposes, but you cannot use these systems for any operations that make use of the Internet in China because China's rules require the following:

1. China approved virus software.

2. China approved cryptography.

3. A China approved ISP.

4. A China approved cloud provider.

5. China approved connection software.

6. A China approved version of Chinese language Windows that we will provide to you.

7. Support service provided only by a China approved (and controlled) network consultant.

To top it all off, as discussed above, China's local authorities have the right to inspect your networked system at any time without notice and this inspection is done without the participation of company staff. During that inspection, your data will be removed using a thumb drive. If the government inspectors want to do it, they can then install the malware through the use of that same thumb drive. Most large network connections in China are done through use of a cloud system. Chinese government authorities have the same rights to inspect the cloud system. In accordance with the rules, the client of the cloud provider will not even know its system has been inspected.

Network systems are provided to businesses in China exclusively through the Chinese government and/or by Chinese government agencies and/or by IT consultants approved and controlled by the government. The Chinese government is the primary hacker in China, with your cyber security being performed by the hacker itself. This goes beyond a simple network connection. The Chinese government provides the landline phone system and the cell phone system. The Chinese government provides the Internet connection. The Chinese government provides the email server. Many Chinese government agencies will not use email; they instead *require* all contacts be through WeChat, a completely insecure platform constantly monitored by the Chinese government. By using the extreme efforts suggested by the best cybersecurity advisors, a foreign company doing business in China might be able to avoid one of these assaults on its data. But when the attacks come from every direction and are organized by the Chinese government itself and backed up by threat of imprisonment, any defense will ultimately fail.

VI. How Companies are Pushed into an Insecure Network System.

As we have seen, the goal of the CCP and its agents is to push all businesses, foreign and domestic, into an insecure network system that allows CCP surveillance, control and full access to all data stored or transmitted over networks within the PRC. So: how do they do it?

A. The CCP Makes Use of Non-governmental Agents

The first step is that the CCP makes use of its agents to implement its hacking system. These agents include the companies and consultants that are controlled by the CCP and that are charged with development of the key components of the networked and informationized system. This use of agents is illustrated by the Golden Spy/Golden Helper malware program discussed earlier. Trustwave reports the Golden Spy software was written by Aisino Corporation: (Aerospace Information Joint Stock LLC. - 航天信息股份有限公司) Listed IT company specializing in information security. Their website states they are owned by the state company CASIC (China Aerospace Science & Industry Corporation Limited - 中国航天科工集团公司). See Golden Spy Chapter 4: Golden Helper Malware Embedded in Official Golden Tax Software.

CASIC is the PRC's leading manufacturer of missiles and related aerospace devices. It sells missile systems to North Korea and it works closely with the Russian military. As a weapons provider, it is an SOE directly under the control of the PRC government and the CCP. In other words, it is the government. Recently, as part of the PRC plan to promote indigenous development of network operations and cloud computing, CASIC entered into the commercial network business via Aisino, its subsidiary that had been active in payment processing and other accounting systems. Aisino's drafting of the Golden Shield tax software and implementation of the related system is part of that process.

B. The Golden Spy/Golden Helper Malware

Aisino's drafting the Golden Spy malware means the PRC government drafted this malware. Simply stated, the PRC government is the hacker and this hacker is shielded from any liability arising from its hacking activity. This is why Aisino employed a crude and easy to identify trojan horse system for this malware. It is at no risk of getting caught or getting punished or getting taken down.

Some have commented to us and to security professionals that such an obvious intrusion somehow shows the PRC government cannot be behind the malware program. ArsTechnica responded to this type of comment in clear terms:

> **Comment from reader:** "Use of a trojan downloader is not subtle."

> **Response from ArsTechnica**: As for it being less subtle... malware like this isn't subtle period by the standards you're applying here, so that's a bizarre argument. It's also a bit odd that you think the Chinese government cares about subtlety when we're talking about software that's distributed by government mandate within their country. Like... what, are the Chinese authorities going to do? Crack down on them?

As Arstechnica makes clear, when the malware or illicit gathering of data is done by the government itself, there is no remedy and no escape. The Chinese government and its related group of hackers do not need to be subtle or hide their tracks when they are operating within the borders of the PRC.

C. The Standard Techniques

What are some of the techniques used to push companies into an insecure network?

1. Forced use of government software that contains malware. The Golden Spy/Golden Helper malware included in the tax payment software required by the PRC government is an example of this method. Trustwave has issued a series of reports on this malware and on Aisino's response in dealing with the public revelations regarding this software. See Golden Spy: Chapter Two – The Uninstaller, Golden Spy Chapter 3: New and Improved Uninstaller, and Golden Spy Chapter 4: Golden Helper Malware Embedded in Official Golden Tax Software. These Trustwave reports should be required reading for any foreign company planning to operate in China.

Trustwave's follow up reports reveal the following three key things;

First, Aisino used the auto-update system in the Golden Spy software to propagate an uninstaller that removed the malware and any files or other traces of its existence. Their software uses a standard update procedure that can then be used to download malware or other unauthorized software at any time. A clean system today can be infected tomorrow. This means this software *is a constant source of risk.*

Second, Trustwave discovered a related but separate malware program concealed in the Golden Tax software. This malware, dubbed Golden Helper, was active in 2018 and 2019. From this, Trustwave reasonably concludes that the tax software malware program is not a recent event but has been going on for several years at least.

Third, Trustwave confirmed my earlier description of the technique used by the Chinese banks for delivering the Golden Tax software and its malware payload:

> During our investigation, we have been informed that the Golden Tax software may be deployed in your environment as a stand-alone system provided by the bank. Several individuals report receiving an actual Windows 7 computer (Home edition) with this Golden Tax software (and Golden Helper) preinstalled and ready to use. This deployment mechanism is an interesting physical manifestation of a trojan horse.

See Golden Spy Chapter 4: Golden Helper Malware Embedded in Official Golden Tax Software.

When I previously wrote of this prevalent and unstoppable CCP hacking, we received comments that none of this could be correct because it would mean the proliferation of compromised computer systems. It seems odd to people who don't work in the PRC that the PRC government would require companies use an insecure computer system. But this is not odd when you consider the government's goals. A compromised system is easy to hack. The government is the hacker, so they make it easy on themselves. The banks may be unaware of the details of the malware and the compromised system; the bank staff is just following orders.

2. Use of network hardware with backdoors installed. It has long been assumed PRC manufactured network hardware is filled with backdoors that allow unauthorized intrusion by the Chinese government and a recent report confirms this assumption. As reported by ZDNet, a research group has found seven separate instances of malware/backdoors in critical network fiber optic cable connection devises. See Backdoor accounts discovered in 29 FTTH devices from Chinese vendor C-Data.

ZDNet describes these intentional backdoors as follows:

> Two security researchers said this week that they found severe vulnerabilities and what appears to be intentional backdoors in the firmware of 29 FTTH OLT devices from popular vendor C-Data. FTTH stands for Fiber-To-The-Home, while OLT stands for Optical Line Termination. The term FTTH OLT refers to networking equipment that allows internet service providers to bring fiber optics cables as close to the end-users as possible.
>
> As their name hints, these devices are the termination on a fiber optics network, converting data from an optical line into a classic Ethernet cable connection that's then plugged in a consumer's home, data centers, or business centers. These devices are located all over an ISP's network, and due to their crucial role, they are also one of today's most widespread types of networking devices, as they need to sit in millions of network termination endpoints all over the globe.

> The simple evaluation of this malware is that it is as bad as it gets.
>
> C-Data, the vendor identified here, is a major source for this type of hardware within the PRC. The takeaway here has to be that if this company feels free to include this backdoor system in products it sells *outside* the PRC, it undoubtedly is unconstrained in doing the same thing within China. This then means any foreign company operating in China should assume that its Internet connection is completely compromised by this type of malware/backdoor in its entire network system. If it is not included in its office system, it is almost certainly included at the ISP or cloud provider level.

This system is installed by telecom providers owned or controlled by the PRC government. Once again, it is the hacker — the Chinese government — setting up the system and it is the hacker that enters company network systems through these back doors.

3. Use of PRC mandated antivirus software. One of the core directives under the new PRC Cybersecurity Law regime is the requirement networked users use antivirus software provided by the PRC government. Think about this for a minute: the Chinese government *requires* companies use only the "antivirus" software it provides. This antivirus software provides both a convenient platform for Chinese government hackers to enter the user's computer network and it is also no doubt programmed *not* to reveal Chinese government malware.

The risks in hacked antivirus software are well known in cybersecurity circles. In Former U.S. spies say antivirus software makes for a perfect espionage platform, Cyberscoop discusses how antivirus software is great for espionage:

> Because most antivirus vendors have designed their products to autonomously search for computer viruses on users' systems by directly scanning files and then sending that data back to a server for analysis, the software is highly intrusive by nature.
>
> Aside from the remote risks, antivirus can extend the attack surface of a host," said Blake Darche, a former computer network exploitation analyst with the NSA. "If an attacker can gain access to the central antivirus server within an organizations network, that central server can be used for malware distribution."
>
> Software updates, which can help patch bugs or other issues in a product, adds another attack vector because it provides a trusted avenue for the remote introduction of code into computers around the world.

Chinese hackers are well acquainted with using antivirus software for this purpose. See: Research claims CCLeaner attack carried out by Chinese-linked group.

Within the PRC, use of mandated PRC antivirus software takes Chinese government hacking risks to an even higher level. Within the PRC, there is no need for a remote hack. The hacker itself (the Chinese government) provides companies with an essentially pre-hacked system.

This pre-hacked system will not screen against malware created by the PRC government and this system also serves as the vector for inserting a continuous stream of malware provided by the PRC government and its partners.

Consider the parallel situation in the U.S. Imagine a scenario where the NSA and the FBI are the only vendors of antivirus software. This software might be effective at screening malware from criminals and foreign actors. But nobody would expect that software would protect users from NSA or FBI intrusion. That would be silly. It is sillier still to believe this about the PRC and its government mandated antivirus software.

4. Shift from email to WeChat. After the Chinese government banned Gmail in China, Chinese government agencies began pushing foreign companies to communicate using PRC approved email services. These services do not work well and are widely known to be insecure. Most foreign companies therefore continued to use alternative U.S. and European based email providers. These services are relatively secure from message interception by the Chinese. Proton mail and other systems with end-to-end encryption are quite secure in China.

The Chinese government could have taken a next step by blocking access to all foreign based email providers. But the Chinese agencies have taken a more creative approach. Now that the Chinese government has assumed essentially complete control over WeChat, Chinese agencies force all communications onto the WeChat application. If you send an email to your bank, your bank will not respond. If you send an email to your local tax office, it will not respond. If you send an email to the local police department concerning your visa status, it will not respond. The same holds true for Chinese courts, which typically respond to us simply by requesting we communicate with them using WeChat. This is even true when documents are submitted. Chinese government agencies almost invariably require submissions as a WeChat attachment rather than as an email attachment.

This then means a shift from adequate security to no security at all. This can be seen by the recent Amnesty International rating of instant messaging applications. Amnesty International rated the 11 top messaging applications on encryption and user privacy on a scale of 0 to 100. Facebook received the highest rating of 73. WeChat received *a zero* rating. In other words, Amnesty International concluded WeChat provides literally no protection at

all from hacking. None. Nada. Zero. Zilch. 没有. See FOR YOUR EYES ONLY? Ranking 11 technology companies on encryption and human rights.

This forced move to a completely insecure communication platform was done in a typical CCP way. There is no law or regulation prohibiting foreign based email. There is no law or regulation mandating WeChat. The "rule" is imposed in practice. If you send an email, it will not be returned. If you call or visit a government agency to complain, the response is: "Use WeChat. Everyone else does. You should too." And so the rule is imposed, with no obligation on the part of the Chinese authorities to formalize or publish the rule.

5. Forced use of an insecure version of Windows Explorer. Many services provided by the PRC government are now provided online. For example, many forms and applications will only be accepted by Chinese government agencies through an online system: paper applications are not accepted. In the same way, information from the government is primarily provided online. Here then is the catch. Virtually all PRC government online systems will only operate on an insecure, outdated, unpatched version of Windows Explorer, usually Explorer 8. If you try to use these systems with Chrome, Firefox, Safari or Opera, the systems do not work. There is no explanation, they just don't work. Access to these systems is not optional: doing business in China requires Internet access to these government websites. So without comment and without formal regulation, the user is forced into an insecure system.

VII. Cross border and International Implications.

The PRC cyber-insecurity system extends beyond the Chinese border, making it impossible to avoid it even by not setting up operations in China. Consider the following:

1. Any transfer of data into China is at risk of being accessed by the Party and its agents. All Chinese companies and organizations are subject to the cyber-insecurity regime. Assume you are working with a Chinese entity and assume that entity for its own benefit wants to keep secret the information you have provided. The sectors where transfers of highly confidential data go into China are numerous: contract manufacturing, joint R&D, technology licensing. The Chinese entity with which you are working is exposed to the same disclosure and access risks described above. As a result, any foreign entity must assume all data transmitted to China is at risk.

2. Under the Digital Silk Road program, the Chinese government is working to extend the Chinese cyber-insecurity program to all countries that allow Chinese entities to build out their network systems. This allows China to export its Internet based surveillance

and control system around the world. See *Will China control the global internet via its Digital Silk Road?* and *Exporting digital authoritarianism*

This concern is generally expressed as a human rights issue. From our perspective, however, the concern is the creation of the PRC cyber-insecurity model around the world. Through the Digital Silk Road system, the PRC government is teaching foreign governments how to create the information transparent system created in China. The added twist is that Chinese companies are setting up the system so the Chinese government has full access to the local system. This is then creating a system where foreign technical data will be acquired at two levels: by the local government and by the Chinese government.

3. Many non-Chinese industry sectors have been pre-hacked by the CCP and its agents. To transfer data into such hacked systems is to transfer data to the CCP and its agents. The Taiwan semiconductor industry is an example. Taiwan semiconductor manufacturers have been thoroughly hacked by the PRC. See *Chinese Hackers Have Pillaged Taiwan's Semiconductor Industry*. High level employees of Taiwan chipmakers have been hired away to work in China. See *China hires over 100 TSMC engineers in push for chip leadership: Emerging chipmakers offer lavish pay packages to snap up talent*. This means it is almost certain confidential chip designs and technology are being leaked to the PRC.

VIII. Conclusion

My goal with this report on cybersecurity in China is to describe the on the ground cybersecurity realities for foreign companies operating in China. As you have seen, the Chinese government is the hacker so it can have full access to all information about the foreign entities that operate in its midst — from critical information concerning protected technologies down to the most mundane facts about the daily activities of the foreign company *and* its employees. In our digitized world, that information is available on computer systems and networked communications of the foreign owned entity.

The Chinese government obtains the information it wants by using the techniques I described. In fact, I have outlined only a subset of the various techniques it uses to gain access to information.

Of course, the Chinese government encourages foreign owned entities to protect themselves from criminal hackers and from intrusions conducted by their non-state-owned business competitors. Under the new cyber regulations, this form of self-protection is legally required for enterprises operating in critical sectors.

But the flip side to this requirement is that the Chinese government allows for no protection against its own acquisition of that same information. Attempts to block access by the Chinese government are futile. One attack vector may be blocked in one case of infection.

But as a practical matter, it is not possible to defend against attacks by a PRC government that uses a full set of penetration techniques. The only question is whether the Chinese government is interested or not. If they are interested, they will succeed.

There is no place to hide.