CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

## Statement before the House Oversight and Reform Subcommittee on Cybersecurity, Information Technology, and Government Innovation

# *“Safeguarding the Federal Software Supply Chain”*

A Testimony by:

**James Andrew Lewis**

Senior Vice President; Pritzker Chair; and Director, Strategic Technologies Program, CSIS

**November 29, 2023**

**2247 Rayburn House Office Building**

Chairwoman Mace, Ranking Member Connolly, distinguished Members of the Subcommittee, I'd like to thank the Committee for the opportunity to testify on this important topic. CSIS does not take policy positions, so the views represented in this testimony are my own and not those of my employer.

The United States faces a major challenge in securing digital technology. Over the last 35 years, it constructed a series of deeply interconnected industrial and technology supply chains with China, based on the assumption that China would become a trustworthy partner, making it safe to take advantage of the business opportunities China presented. At the time, there was some truth to this and companies in the United States and its allies made immense amounts of money, but ultimately it was a mistake. The United States and its allies have now learned that when it comes to cybersecurity and software supply chains, China is not trustworthy.

The reasons for this have to do with China's priorities and intentions. China's leaders are determined to do anything to keep the Chinese Communist Party in sole power and their intention, under President Xi, is to assert China's dominant role in international affairs, and this requires displacing the United States. Information technology is central to achieving these ends.

Before 1979, under Mao, China had been kind of a hermit kingdom that stood apart from the rest of the world. When Deng Xiaoping replaced Mao as China's leader, he found an impoverished, backward nation whose economy and technology lagged decades behind the West. Deng set about to change this by opening China to Western investment. Deng also began a program of technology acquisition using both lawful and unlawful methods, such as encouraging companies to invest and build in China while at the same time stealing their intellectual property.

Deng's policies paid off and China has become the second largest economy in the world. Some speculate that it may have reached its peak. China's economic growth created political forces that challenged the rule of the Communist Party. Deng's opening to the West meant that the Party's carefully constructed narrative on why it's one party rule was essential was challenged by outside sources. China's leaders decided to end this challenge. Xi Jinping, China's current leader, was gripped with the collapse of the Soviet Union, studied it carefully, and determined that China's Communist Party would not follow the USSR into the dustbin of history. This creates an unavoidable tension – the Party needs economic growth to survive, but economic growth challenges its survival.

This is not good news for cybersecurity. Cyber espionage has been one of the keys to China's growth. The United States has been the primary target, but it is not alone in being targeted. As China's growth slows, it may increase its already high level of spying and it will use any tool, including, including exploiting opportunities created by transnational supply chains for software, telecommunications, and internet applications.

Much of what Xi has done reflects themes in Chinese policy that had existed for years. There were those in China who wanted to move in the direction of becoming more like other developed economies and adopt global norms for trade and commerce, but there was always a powerful undercurrent of nationalism that was hostile to the West. Nationalism and control of the narrative are important parts of Xi's policies, but he is building on policies that were already present. What has changed is that Xi has worked to minimize what he sees as threats to Party control.

Even before Xi took office, China had built the world's largest surveillance system by 2010. Information technology is at the heart of this system. Cyber espionage was always part of Chinese policy, both against its own people and against other countries, particularly the United States. Theft of technology is as crucial for China's growth as foreign investment, and China feels justified in stealing as reimbursement for what they call the 'Century of Humiliation," when European powers occupied China.

American, European and Japanese companies felt they could manage the risk of espionage and intellectual property theft in ways that would allow them to participate in China's economy. This was a mistake, the result of a gamble that China would eventually adopt international norms, stop spying and end the theft of intellectual property. By 2015, when the Office of Personnel Management was hacked as part of a larger espionage campaign to collect personal information of Americans, two years after Xi took power, it was clear this was a mistake.

The United States, Japan and even the Europeans now realize that trade with China comes at the cost of massive espionage and creates the risk of hollowing out their economies. China's predatory trade policies, using a blend of illicit subsidies, restrictions on foreign competitors, and espionage, led to situation where the world was on the cusp of finding itself dependent on Chinese technology. Huawei and the 5G telecom story is the best example of this, but it is not the only one. By supporting Huawei financially and through commercial espionage, the Chinese government built a powerful global company, gained access to other countries' telecommunications infrastructure in ways that provided intelligence benefits, and was able to drive out Western competitors to dominate this strategic market, what China would call a "win-win."

The United States faces other opponents, but none are as deeply intertwined with the American tech sector and none of them have the scope or wealth of China. The Democratic People's Republic of Korea (DPRK) has a software industry of sorts, but it is small and limited. Iran has a limited software industry and some private hackers who work with the government, but not much of a presence in global markets. Russia had a strong software industry, but it, like Iran and North Korea, it is now under sanctions and its presence in Western markets is greatly reduced. The Russian IT sector has been decimated by the war in Ukraine as those with tech skills fled the country. Only China has a major global presence in hardware, software, apps, and increasingly, cloud computing services. China uses information technology companies to censor and to spy on its citizens, and increasingly on the citizens of other countries. China's intelligence agencies are inventive, aggressive, and well resourced, making them formidable opponents and they have had remarkable success in cyberspace.

Market forces drove a close IT supply relationship with China. China was not held accountable; for its predatory behavior and letting China into the WTO without insisting that it observe its commitments was a giant strategic blunder for which Western countries are still paying. This leaves the United States in a difficult spot. Our technology supply chain is so deeply interwoven with China that decoupling is not possible without massive economic dislocation. If it is any consolation, the Chinese are unhappy about this as well. The Chinese government wants to decouple even more than Western countries, but they face even bigger obstacles to decoupling that the West.

Since decoupling is not possible, given the deep interconnections built up over the last 40 years, this makes the problem one of managing technology supply chains with a hostile and untrustworthy partner who uses predatory trade practices and is undertaking the largest espionage campaign in history against the United States. This is an uncomfortable situation to say the least, one that cannot be changed rapidly, but a situation where risk can be minimized and managed.

The difficulty of decoupling has led to calls for “de-risking,” which means restricting or ending commercial relations with suspect entities to avoid risk. De-risking technology trade with China is a step in the right direction since it opens the question of China’s trustworthiness as a supplier. Ultimately any solution needs to be part of a comprehensive multilateral approach that manages risk by limiting China’s access to Western markets, capital, and intellectual property while reducing its role in technology supply chains, something that is in the process of being constructed but is not yet complete. However, an interconnected supply chain creates three sets of risk for the United States. First, China could use its position as supplier for espionage purposes and collect information. Second, it could use its position as a supplier to degrade or disrupt services. Third, it could deny access to technology. De-risking does not address these problems.

Anything that is from China and connects to the internet can be used to collect information. To use TikTok as an example, TikTok connects its users to servers China and its owner, ByteDance, can load software on devices that use the TikTok App, such as a phone, table or computer. Users have no control over this. The Chinese government could compel ByteDance to provide access to TikTok users’ devices and networks. It would be easy for TikTok to provide the personal information it collects to the Chinese government without the user’s knowledge. TikTok of course, denies it would do this.

But Chinese companies do not have a choice in cooperating with the Chinese government. China has privacy and data protection laws, but they do not apply to Chinese security agencies. Chinese law mandates the full cooperation of Chinese companies with any request from an intelligence agency and there are no grounds for appeal. China’s laws give its agencies untrammeled access to networks and data from Chinese companies and take precedent over any other law or commitment. Xi is distrustful of the private sector, has been steadily increasing the Party’s presence and control in Chinese companies with some estimates saying that more than 75% of private companies have Party committees involved in their management. The Chinese government can use what is called a “golden share,” where it takes a small ownership stake in a company that allows for board membership and a role in company decision-making.

All of this means there is always risk in using software, devices or services that digitally connect to China over the internet. It is likely that China will exploit or consider exploiting such devices or services for espionage purposes. If a device or application (app) does not connect to China, the risk of compromise is low, but these “safe” uses are a shrinking set.

The fundamental issue is what opportunities for access to networks, devices, or data, does the technology create for hostile activities. Chinese-made apps are an obvious concern, but the more troubling and more difficult problems is Western software that includes Chinese components. Unpublished industry reporting suggests that dozens of commonly used applications use Chinese software. Managing software supply chain risk is an increasing problem for cybersecurity. Assessing this risk of this involves a complex calculation of the access provided by using the Chinse software. To measure the risk created by using Chinese information and communications technology and services (ICTS) we can ask three questions:

- Is the technology designed, connected, operated, or managed from China? This creates opportunities for access and disruption.
- Who controls the data provided by the device or application? Ownership or control provides the ability to use it for other purposes, including intelligence and political manipulation.
- To what data does the Chinese product or service have access? While not all data has intelligence value, China reportedly now collects personally identifiable information (PII) on Americans and the citizens of other countries?

Answering these questions allows us to assess the risk of specific products.

The way software is created leads to potential opportunities for compromise. Many software products blend code from a variety of sources, including proprietary software (which sometimes can include re-using old code), but also open-source software that is in the public domain, and software provided under license by third parties. Unsurprisingly, given the strong Chinese IT industry and the deep interconnections to it, open source and third-party software modules can come from Chinese sources and can create risk. The way software is used provides opportunities for problems, since software's services can be accessed remotely.

One area of concern is the use of Chinese 'software development kits' (SDKs) in other programs and apps. SDKs are basically a chunk of code that can be inserted into a larger program. They provide tools and functions that speed up the creation of software. SDKs are in effect invisible, embedded in a larger American product. Some reports say that Chinese SDKs developed by major Chinese software companies like TenCent and Alibaba are found in a number of well-known apps and online services. The use of Chinese SDKs could potentially create opportunities for espionage or the disruption of services.

For U.S. government software and technology acquisitions, the risk of hostile Chinese action is almost certain. Unlike the commercial or consumer sectors, where risk thresholds are different and, in many cases, lower, any use by Federal agencies of Chinese software on devices or applications connected to the internet can provide an opportunity for access by Chinese intelligence agencies is a risk. We have already seen this risk in the supply chains for telecom infrastructure, drones, internet-connected cameras, and social media apps. Knowing what software has Chinese components can be difficult. A first step lies with the "SBOM" process now managed by DHS. A "software bill of materials" (SBOM) list the source of a software product and its components. SBOM can let the United States identify software with Chinese elements and decide on the risks and benefits of its use.

The emphasis on secure software development put forward by this administration in response to the Solar Winds incident also can help reduce risk. In the past, some software was written in a haphazard fashion. Legacy code is vulnerable (and anything more than a few years could count as legacy) but still in use, and the standards for secure software writing are unevenly applied. All of these create vulnerabilities that hackers can exploit. Changing this situation will take time but shrink the opportunism for China and others to exploit vulnerabilities. The problem is complicated by the use of commercial software services in the government. A Federal user may download and use a shopping app or a travel app that includes Chinese software modules. While such software can be banned from Federal devices, it cannot be banned if someone chooses to use it on their personal device.

These issues point to the need for a thorough review of the software, applications and internet-connected devices that are acquired by the Federal government, by expanding acquisitions rules to cover the "provenance" of software, using existing rules like FedRamp, the Federal Acquisition Regulations, and the revised NIST Cybersecurity Framework.

The new Office of Information and Communications Technology at the Department of Commerce is creating a process to review information technologies subject to its jurisdiction and has the authority to prohibit or impose mitigation measures on transactions that create risk to infrastructure, privacy, cybercrime and espionage. The Office was established in part to address the need to create a process for review process and action with TikTok that could withstand judicial scrutiny, but its remit is much larger given the scope and scale of the ICTS supply chain problem, and it builds on the work of several executive order issued in the last few years.

This new office, the Executive Orders, and changes in acquisition regulations will let the United States begin to manage a complex national security problem, but we are only at the start. No one ever likes recommending more regulation, but we are in the process of a broad evolution that takes into account the competition with China and the importance of cybersecurity. Government users of Chinese software, apps, or software that uses Chinese code are of particular concern This evolution will not be easy or quick, but it is essential for national security.

I thank the Committee for the opportunity to testify and look forward to any questions you may have.