Statement before the House Energy and Commerce Subcommittee on Communications and Technology

"Securing Communications Networks from Foreign Adversaries"

A Testimony by:

James Andrew Lewis

Center for Strategic and International Studies

February 15, 2024

2123 Rayburn House Office Building

Chairman Latta, Ranking Member Matsui, and distinguished Members of the Subcommittee on Communications and Technology, thank you for inviting me to participate in today's hearing. My comments today are my own and should not be attributed to the Center for Strategic and International Studies.

Poorly secured communications networks create real risk by opening opportunities for espionage and for the disruption of critical services. While there has been real progress in the past few years at improving network security, the United States has only begun to grapple with the broad set of digital vulnerabilities. Many of these are the result of close commercial relations with China. The United States need to rethink and restructure its policies to take into account the competition with China and the importance of network security for our national security.

National security risks are one reason the topic is of strategic interest. The other reason is that technologies like 5G and 6G provide the foundations of the ubiquitous, interconnected digital infrastructure that is the key to future economic growth. Ubiquitous connectivity means there will be globally interconnected networks and services that will be able to access, over the internet, immense data and computing resources. This will over time increase productivity and innovation.. Technology is a new field for international competition and the terms of this competition are the ability to innovate, to build digital infrastructure, and to create resilient supply chains. This is a different kind of competition and China has real strengths. While it is increasingly hampered by its authoritarian political system, it is clearly competitive with the United States in areas like artificial intelligence, quantum communications, satellites, and 5G spectrum allocation.

Digital competition for influence and wealth coincides with the need to reduce China's role in Western supply networks and its presence in Western digital infrastructure. The years since China opened to the West have seen the rise of globally interdependent and interconnected innovation. Chinese companies have been interwoven into Western supply chains. Western companies remain attracted to China as a supplier and as a market, although they are increasingly cognizant of the political risks of doing business there. Careful scrutiny of this commercial and technological relationship with China is long overdue, but mutual interdependence complicates efforts to change it.

The most immediate problem is spying. Chinese espionage against the United States has reached unprecedented levels, greater than anything seen in the Cold War and this comes at a time of steadily increasing global connectivity based on a range of different communications technologies. This means that anything connected to the internet can be used to collect information. China has built the world's largest surveillance system. Information technology is at the heart of this system. Espionage was always part of Chinese policy, both against its own people and against other countries, particularly the United States.

China's intelligence agencies are inventive and well resourced, making them formidable opponents and they have had remarkable successes. China's 2017 National Intelligence Law mandates that all Chinese citizens and companies must support, assist, and cooperate with state intelligence efforts. This law is notable for its extraterritorial provisions, which allows Chinese intelligence agencies to compel cooperation from Chinese citizens and entities overseas. The law significantly expanded the legal framework for China's intelligence activities. There is no appeal and the process is not transparent. Even if a company's record is spotless, it can be compelled at any time to provide data or other assistance. Chinese companies do not have a choice when it comes to cooperating with the Chinese government.

Defending against cyber espionage is a challenge for all countries and this challenge will grow as we move to a world of ubiquitous connectivity over digital networks. Cyber defense has not kept up with cyber espionage. The nature of espionage has changed in an increasingly interconnected world. The ability to manipulate data, sometimes using artificial intelligence tools, has transformed intelligence analysis the same way it is transforming business. Companies collect masses of data and develop sophisticated software tools to better identify customers and markets. Intelligence agencies do the same for espionage purposes. In 2015, Chinese intelligence entities hacked the Office of Personnel Management (OPM), along with several large companies and acquired immense databases containing the personal information of millions of Americans. The OPM hack was part of a larger data-centric intelligence campaign by China to acquire data to populate Chinese "big data" programs for intelligence. OPM data gives China the foundation of data-intensive spying and China, for reasons that are not always apparent, continue to acquire masses of data on Americans.

Fears that the OPM hack would give China insights to improve their recruitment of Americans appear to be misplaced. The primary motive for hacking OPM was, as is so often the case in Chinese surveillance efforts, most likely directed at their own population, to allow the Chinese security services to better identify Chinese citizens who are sources for the United States. China has made massive efforts in data analytics and biometrics (e.g. facial recognition, fingerprinting, and DNA analysis) to create comprehensive surveillance programs and in the last few years appear to have extended these efforts to go beyond their own population (although it is still the primary target, to other countries and in particular the United States.)

The problem of Chinese network espionage comes after years of building a symbiotic and interdependent tech relationship with China. Western investment, trade, and education, combined with China's immense market, human capital resources, economic policies and reinforced by extensive commercial espionage, helped make China the second-largest economy in the world. China's authoritarian governance, disregard for human rights, strategic investments in key technologies like telecommunications and drones, its disregard for international norms, and predatory trade behavior raise unavoidable foreign policy concerns. The interconnected digital supply chain means that China can use its position as supplier for espionage purposes, degrade or

disrupt services, or to deny access to vital technologies. So far, we have seen rampant espionage, but so far no disruption. However, recent testimony from the FBI, Cyber Command and others highlighted that disruption of critical services by China is a growing and significant risk.

The deep interconnections in Western and Chinese digital communications technology creates risk. China could use information technologies and services in ways that provide intelligence advantage and can harm American national security and the privacy of Americans. Information technology products and services that are widely used in the United States create risk because of their internet connectivity. Millions of devices in use in the United States currently run software from companies with ties to China or Russia and source code developed by companies in these countries is embedded in IT products and services. The Department of Commerce's new Office of Information and Communications Technology and Services (ICTS) is a first step in trying to manage this problem.

It will take years to reduce these risks. Decoupling or derisking are not solutions, at least in the near term. Currently, the West cannot "decouple" from China, nor can China decouple from the West. Global technology markets are too interconnected for Cold War-style bifurcation or regime modeled on antiques like COCOM, a Cold War export control regime. Decoupling is not achievable, even though China itself wants to decouple. While China remains reliant on Western technology, markets, and finance, western companies rely on China for components and significant dependencies have developed between Western companies and Chinese suppliers and markets. Given this, reducing China's presence in the digital ecosystem and the digital technology supply chain will be incremental and iterative.

Between Chinese government investments, industrial espionage, and Western companies decision to move manufacturing to China, it plays a central role in supplying hardware, eliciting concern and countermeasure since 2015. China role in software is not as widely recognized. The way software is written provides opportunities for spying. Software is often written in a haphazard fashion. Software products blend code from a variety of sources, including proprietary software (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. Legacy code is vulnerable (and anything more than a few years counts 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. Creating disclosure or reporting mechanisms for software and communications devices originating from foreign entities that are deemed adversarial to the United States could also be a first step.

There are other opponents who are part of the global software industry, but none are as deeply intertwined with the American tech sector and none of them have the scope or wealth of China. The DPRK has a software industry and uses it for both espionage and for income, but it is small and limited. Iran has a software industry and it can supply 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, has its presence in Western markets greatly reduced. The Russian IT sector has been decimated by the war in Ukraine as many Russians with tech skills fled the country. Only China has a major global presence in hardware, software, apps, and increasingly, cloud services. China's leaders are determined to keep the Chinese Communist Party in power and their intention, under President Xi, is to reshape international affairs and assert China's dominant rule in them Information technology plays a central role in this.

For U.S. government software and technology acquisitions, critical infrastructure, and for leading technology companies, the risk of hostile Chinese action to penetrate networks and acquire data is certain. Any use of Chinese software on devices or applications connected to the internet can provide an opportunity for access by Chinese intelligence agencies is a risk. Knowing what software has Chinese components can be difficult. A first step lies with the "Software Bill of Material (SBOM)" process now managed by the Department of Homeland Security. A "software bill of materials" (SBOM) list the source of a software product and its components. SBOM can help identify software with Chinese elements and decide on the risks and benefits of its use.

It would be useful to increase transparency in the source of digital technology as a first step towards assessing risk. Proposed legislation for a study on the national security risks posed by routers, modems, and devices would be helpful. Small and home office networks have become a target for foreign adversaries, as they are often less secure and can offer access to corporate networks. Just this month, the Department of Justice announced that it has disrupted a network made of hundreds of based small office or home office routers used by China for possible use against critical infrastructure.

Another example is the use of 'software development kits' (SDK) that provide portions of code for larger programs and apps. SDKs provide tools and functions that speed toe creation of software. Some reports say that Chinese SDKs developed by major Chinese software companies like TenCent are found in a number of well-known apps and online services. The use of Chinese SDKs could potentially provide access to data disruption of services. SDK are in some ways the greatest risk because they are in effect invisible, embedded in an American app.

The emphasis on promoting secure software development put forward by this Administration in response to the Solar Winds incident also can help reduce risk. Changing this situation will take time but there are ways to shrink the opportunity that technological interdependence creates for China and others to exploit vulnerabilities.

Banning the use of federal funds to purchase Huawei and ZTE equipment in the Secure and Trusted Communications Networks Act of 2019 was an important step, but only an initial one. Adding additional companies, such as DJI, builds on this precedent. But decoupling or derisking are, at best, long-term solutions. Pursuing individual companies, even large ones, creates the risk of leading to cumbersome bureaucracies that provide piecemeal solutions. Some existing authorities, like the International Economic Emergency Powers Act (IEEPA) provide a good starting point, but additional authorities from Congress may be necessary.

While China remains reliant on Western technology, markets, and finance, significant dependencies have developed between Western companies and Chinese suppliers and markets. The Department of Commerce's new office, recent 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.

Since decoupling is not possible, given the deep interconnections built up over the last forty 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 that cannot be changed rapidly, but by using a combination of new legislation and executive branch authorities, the risk can be minimized and managed.

Broader solutions could include finally passing a national privacy law, expanding transparency in supply chain networks, and restricting egregious cases where the use of Chinese technology poses potential risk. These should be seen as initial steps to reduce the risk created by technology dependence. Not all Chinese technology poses risk, those risks can vary with use, and many risks can be mitigated, but the Subcommittee's work in building a framework of new authorities is important, essential, and long overdue.

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