Michelle Van Cleave
Statement for the Record
U.S.-China Economic and Security Review Commission
June 9, 2016

Chinese Intelligence Operations and Implications for U.S. National Security

Chinese intelligence routinely is ranked number one or two in the hierarchy of foreign intelligence threats to the United States and America's interests worldwide.[1] Yet to date the U.S. government has little in the way of agreed national strategy or coherent policy guidance for countering them. Building upon the questions the Commission has asked me to address, I would like to offer a framework for thinking about these Chinese intelligence activities and what they imply for our nation's security and prosperity. And I will share some observations why, in my view, the United States needs a national level strategic counterintelligence program to contain them.

What espionage operations does China run in the United States and who are their targets?

Chinese intelligence activities within our borders are wide-ranging and growing. For all the benefits that may accrue from what has been a bipartisan policy of engagement with China together with the ripple effects of globalization, they also have opened the door to new espionage opportunities. Chinese operations are facilitated by an extensive foreign presence that provides cover for their intelligence services and agents operating in the United States, where effective integration of cyber and human espionage magnifies the reach of both. Specifically, they seek to

- Penetrate, collect, and compromise U.S. national security secrets (information, plans, technology, activities, operations, etc.), in order to advance their interests and defeat U.S. objectives.
- Acquire critical U.S. technologies and other sensitive proprietary information to enhance their military capabilities or to achieve economic advantage.
- Manipulate and distort the picture of reality upon which U.S. policymakers plan and execute national security strategies, technology developments, and economic well-being, including corrupting the intelligence we gather, and conducting influence operations aimed at U.S. decision-makers.[2]

Targets

U.S. counterintelligence is identifying human and technical collection activities by the Chinese and others targeted against all the essential elements of our national defenses and the supporting structures that maintain our Nation's technological advantage at home and abroad. From the standpoint of foreign intelligence interest, there are many potentially valuable targets outside of our borders, such as American government personnel and the far-reaching activities of critical U.S. commerce and industry. But the real intelligence treasure trove for foreign powers is here in the United States.

---

[1] DNI worldwide threat testimony Feb 2016: "We assess that the leading state intelligence threats to US interests will continue to be Russia and China, based on their capabilities, intent, and broad operational scope… "

[2] *Ibid*. "Penetrating and influencing the US national decision-making apparatus and Intelligence Community will remain primary objectives for numerous foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other sensitive areas will remain a persistent threat to US interests."

The institutions and people responsible for the formulation and implementation of American plans, intentions and capabilities – the central targets of foreign intelligence collection and influence – are principally here within the borders of the United States. Intelligence production and weapons design, the secrets of our nuclear labs, and the strategic advantage afforded the Nation's security by R&D at American companies like Bell Labs or Boeing or Dupont are all here in the U.S. Within our borders, there are thousands of facilities engaged in classified national security work, and hundreds of thousands of workers who hold security clearances (all of which have been collection targets for Chinese intelligence, as discussed below).

Operations

The counterintelligence problem is not one of sheer numbers (though by any measure there are more foreign intelligence operatives in the United States than we have personnel to address them.)[3] Contrary to the popular image (the "thousands grains of sand"), strictly speaking there are not thousands of Chinese "spies" – *i.e*., officers in the employ of Chinese intelligence -- in the United States. Like all intelligence services, they also use informational sources, one-time contacts, incidental contacts (both witting and not), and agents of influence to carry out their work. In other words, espionage may be big business but the management tier (the foreign spies) is a more tractable number. The larger and more compelling issue is the scope of their activities.

Historically, embassies and other diplomatic establishments within the U.S. have served as the hub for foreign intelligence activities because of the operational security they afford. Not surprisingly, the 20,000-strong diplomatic community has commanded the lion's share of attention.[4] Our counterintelligence resources, especially those of the FBI, have been scoped against this threat population and its geographic concentrations in Washington and New York, and consular offices in such cities as San Francisco, Chicago, Los Angeles and Houston.

Now, however, foreign powers including China increasingly are running intelligence operations with unprecedented independence from the former safe havens of their diplomatic establishments. The number of formal and informal ports of entry to the country, the ease with which people can travel internally and the relatively benign operational environment of the U.S. are tailor made for embedded clandestine collection activities. Thousands of foreign owned commercial establishments within the United States, the routine interactions of trade and transnational business and finance, and the exchange of hundreds of thousands of students[5] and academicians, all potentially extend the reach of Chinese intelligence into the core structures of our Nation's security.

Moreover, China has an extensive intelligence apparatus and highly coordinated tasking and collection activities targeting U.S. information and computer systems. All U.S. national weapons laboratories,

---

[3] The integrated execution of the three essential CI tools (physical surveillance, electronic surveillance, and HUMINT agent contact) is time and resource intensive, forcing trade-offs and a sharp prioritization of U.S. CI effort.

[4] As of February 2016, there were 352 Chinese diplomatic personnel accredited to the embassy in Washington DC (http://www.state.gov/s/cpr/rls/dpl/) plus another 137 at the Chinese mission to the United Nations in New York (https://www.un.int/protocol/sites/www.un.int/files/Protocol%20and%20Liaison%20Service/bb305.pdf) – which doesn't count their New York consulate or their four other consulates in the cities listed above.

[5] As of the 2014/15 academic year, some 304,000 Chinese students were studying in the U.S., nearly 11% increase over the prior year and more than ever before. http://foreignpolicy.com/2015/11/16/china-us-colleges-education-chinese-students-university/

Pentagon computers and communications systems, and other sensitive government networks have been targeted by China-based cyber intruders. According to the Pentagon's 2016 *China Military Power* report,

> China is using its cyber capabilities to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs. The information targeted could potentially be used to benefit China's defense industry, high technology industries, and provide the CCP insights into U.S. leadership perspectives on key China issues. Additionally, targeted information could inform Chinese military planners' work to build a picture of U.S. defense networks, logistics, and related military capabilities that could be exploited during a crisis.[6]

By all appearances, these cyber operations are part of a long term, sophisticated campaign to get inside US networks so that once there, intruders can exfiltrate information, manipulate data, and implant stay-behind devices for return visits. False information planted in computer systems could potentially mislead or confuse decision makers, while the discovery of false data may be even more effective in sowing uncertainty and undermining confidence in the integrity of the information stored and processed by compromised systems.

Human penetrations into U.S. intelligence remain the gold standard for any adversary service. The pending court marital of a naval intelligence officer on espionage and related charges is especially noteworthy for the access and insights he would have had to highly sensitive matters inside the U.S. SIGINT community.[7] To date, only one other spy has ever been caught inside U.S. intelligence working for China.[8] There are two ways of looking at this. Perhaps the Chinese have not been very successful at such recruitments. Or perhaps they have been very good at not getting caught.

Either way, we urgently need a better understanding of what they are doing and how they are doing it, because Chinese espionage in the United States is poised to get much worse.

Grim outlook

As this Commission is aware, last year cyber intrusions originating in China breached the files of the Office of Personnel Management (OPM). Early estimates of 4 million personnel files compromised were revised upwards to closer to 18 million… and then to 22 million… or roughly 7% of the total US population.[9]

The standard background investigation questionnaires cover extensive biographical information, personal data, employment and military records, fingerprints, foreign travel and contacts.[10] The investigative files also include candid evaluations and comments from co-workers, neighbors, family and others; records forwarded by other agencies such as polygraph results; and other sensitive matters such as interactions with the police, use or abuse of illegal drugs or alcohol, detailed information on financial problems,

---

[6] http://www.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf

[7] Lt. Cmdr Edward Lin, born in Taiwan and suspected of working on behalf of Taiwan or China or both, has pleaded not guilty to all charges. http://www.navytimes.com/story/military/2016/05/13/accused-navy-spy-faces-court-martial/84329026/

[8] In 1986, CIA translator Larry Wu-tai Chin was convicted of suppling secrets to China for decades, which among other things had led to the deaths of U.S. agents. The case of Katrina Leung, a 20-year FBI asset believed to have been under Chinese control, is discussed below.

[9] http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731

[10] https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-central-9-personnel-investigations-records.pdf

detailed summaries of psychological and emotional health counseling, and (post-Wikileaks) unauthorized use of information technology systems.

In the espionage business, spotting and assessing are the first steps in developing new sources or recruiting new assets. Identifying who has access to sensitive information is step one. Learning their vulnerabilities may be step two.

By this measure, the OPM files are gold. The Chinese now have a detailed roster of most if not all American contractors and government employees who have access to classified information, plus a roster of their friends, colleagues or co-workers who may be useful conduits or potential assets in their own right. (Step One, check). They also have a treasure trove of data that can be used to coerce, blackmail or recruit U.S. sources or simply enable personalized phishing schemes --- one-stop shopping for Step Two. But it doesn't end there.

The stolen files also include records of where American officials have lived or traveled plus contact reports on foreign nationals abroad and at home. Such details may help a foreign security service piece together U.S. intelligence networks and operations – and develop a blueprint for disrupting them. According to press reports, CIA pulled a number of officers from the American Embassy in Beijing as a precautionary measure after the OPM breach.[11] Other news reports suggest that "at least one clandestine network of American engineers and scientists who provide technical assistance to U.S. undercover operatives and agents overseas has been compromised."[12]

A key point is this. Cyber espionage and the human espionage go hand in hand. Recruiting an insider with user privileges may be more effective than searching for cybersecurity vulnerabilities to exploit. Access is always key. Access to computer systems that may enable the implanting of the next nasty bug. Access to information about individuals that may prove compromising or otherwise useful to a resourceful intelligence service.

And because the OPM data bases are so comprehensive, they are the gift that keeps on giving for years and years to come.

And OPM is not alone. Back in January 2013, computer networks at the Energy Department were breached, compromising the personnel files of some hundred thousand employees. USIS, a federal government contractor that conducted most of the background investigations for OPM and the Department of Homeland Security, was hacked the following year. Ditto computer files at Commerce, State, DoD, Navy, EPA – the list goes on.[13]

Then there's all the personal information that is out there for the taking, no hacking skills required. For instance, last year an enterprising outfit published the resumes of over 27,000 people working in the US intelligence community, all mined from LinkedIn. They claim the resumes mention secret codewords and surveillance programs. [14] That could be hype (or not) but at a minimum is indicative of the valuable

[11] https://www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html
[12] http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html
[13] https://www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html
[14] http://www.zdnet.com/article/linkedin-serves-up-resumes-of-27000-us-intelligence-personnel/

insights to be gleaned by adversaries who have a more focused purpose in going after these publicly available records.

Beijing has also been linked to penetrations of several health insurance companies that hold personal data on tens of millions of Americans. Investigators believe the same units responsible for the attacks on OPM had previously breached computer networks at Anthem Inc. and Premera Blue Cross. Chinese hackers have also stolen the passenger records for at least one major airline,[15] and possible others.[16] Last year also brought us the Ashley Madison breach – an online dating service for extramarital affairs – which, according to the *New York Times*, netted "personal information attached to more than 30 million accounts, including those of 10,000 American government officials, a handful of celebrities, a few clergymen and, apparently, very few real female profiles."[17]

It's hard to escape the conclusion that the Chinese government is building massive databases of Americans' personal information.[18] Beyond the obvious value to traditional espionage operations, what more they intend to do with this vast and growing collection is an open question. What is clear is that the job of U.S. counterintelligence is becoming much harder – and more compelling.

National policy of economic espionage

According to the Office of the NCIX, the Chinese have "a national policy of economic espionage in cyberspace," as an integral part of their technology theft and industrial espionage activities overall.[19] Consider what that means in practice:

- ***A dedicated enterprise to acquire prioritized technologies or know-how***. The FBI estimates that the Chinese Army has developed a network of over 30,000 Chinese military cyberspies, plus 150,000 private-sector computer experts, whose mission is to steal American military and technological secrets. They are part of an extensive government apparatus and highly coordinated tasking and collection activities targeting U.S. technologies.[20] China clandestinely employs commercial firms – front companies -- to acquire the controlled technologies they want,

[15] https://www.washingtonpost.com/news/the-switch/wp/2015/07/29/why-would-chinese-hackers-would-want-to-go-after-an-airline/

[16] http://www.bloomberg.com/news/articles/2015-08-07/american-airlines-sabre-said-to-be-hit-in-hacks-backed-by-china

[17] http://www.nytimes.com/2015/08/29/technology/ashley-madison-ceo-steps-down-after-data-hack.html?_r=0

[18] https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html?tid=a_inl

[19] From the Defense Department's 2016 China Military Power report: **"**China uses a variety of methods to acquire foreign military and dual-use technologies, including cyber activity and exploitation of the access of Chinese nationals—such as students or researchers—acting as procurement agents or intermediaries. China very likely uses its intelligence services and employs other illicit approaches that violate U.S. laws and export controls to obtain key national security and export-restricted technologies, controlled equipment, and other materials unobtainable through other means."

[20] According to data from combined Pentagon data bases, Chinese targets cover most of the Militarily Critical Technologies List maintained by the State Department: telecommunications, INFOSEC technology, communications and data links, lasers, optics and supporting technology, aeronautics, sensors, armaments and energetic materials, electronics, space systems, marine systems, materials and processing, signature control technology, chemical technology, biological technology, positioning, navigation and time technology, guidance, manufacturing and fabrication, energy and power systems, nuclear technology, directed energy and kinetic energy systems, weapons effects, biomedical technology, and ground systems technology.

in violation of U.S. export control laws. They also insert collectors inside US companies. This is not a casual undertaking; in fact, the Chinese have set up organizations in the US to track the access of these experts.

- ***Specifically targeting key industries to meet requirements***. China's most recent five-year plan identified the country's key "strategic sectors" on which its future growth, prosperity, and economic strength would hinge: technology, aerospace, telecommunications, energy, transportation, engineering services, and high-tech electronics. These are the same sectors that China's cyber espionage has targeted. In other words, if they can't get it legally through trade, or creatively through mergers and acquisitions, they are prepared to steal it.
- ***Strategic investments in the means to get at those targets.*** Hackers find and exploit existing cyber vulnerabilities; a nation-state that takes the long view, such as China, may also seek openings in the supply chain to implant vulnerabilities that can be exploited later. Were Huawei or ZTE to succeed in entering the U.S. telecommunications market, for example, their opportunities for supply chain manipulation could be significant.[21]
- ***An economy structured to take advantage of a policy of national industrial espionage***. Chinese government and business are often so close together as to be indistinguishable. Further, Chinese party official interests and business interests are often the same thing, which helps when it comes to tasking intelligence collection. In other words, Chinese economic espionage is driven by two powerful motives: state power plus personal wealth.

And what are the results? According to the U.S. Commission on Intellectual Property Theft (Blair/Huntsman Commission), China is responsible for as much as 80% of all intellectual property theft against U.S. companies.[22] Technology theft amounts to loss of more than $300 billion a year – more than the annual US exports to Asia. Former DIRNSA Gen. Keith Alexander's characterization bears repeating: "the greatest transfer of wealth in human history."

It also bears repeating that Chinese espionage directed at more traditional targets – such as defense capabilities and other national security secrets – is as aggressive (and I fear as successful) as their economic espionage activities. Which should give us pause.

It has been a decade since the Cox Commission issued its findings on the loss of nuclear weapons information to the PRC. It is well worth a moment to remind ourselves: The PRC stole design information on all of the United States' most advanced thermonuclear weapons. This includes every currently deployed thermonuclear warhead in the U.S. ballistic missile arsenal, as well as design information on enhanced radiation weapons. *We still do not know how they did it.* The troubling question is, why not?

How effective are U.S. actors in deterring, tracking, preventing, and mitigating these espionage operations?

Measured by arrests and prosecutions, U.S. government successes against Chinese technology diversions are growing. FBI investigations and arrests for industrial espionage and violations of export control laws

[21] http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf

[22] Last year, the FBI released the results of a government survey of 165 companies, half of which reported said that their proprietary information had already been targeted by foreign spies. And in 95 percent of those cases, the companies suspected China was to blame. http://www.thedailybeast.com/articles/2015/07/23/fbi-probes-hundreds-of-china-spy-cases.html

are at an all-time high, predominately linked to the Chinese government.[23] The number of economic espionage cases investigated by the Bureau's counterintelligence division increased 53% from 2014 to 2015; the precise number of total cases is classified, but the FBI has disclosed that it's "in the hundreds" including such large corporate victims as DuPont, Lockheed Martin and Valspar and involving the loss of hundreds of billions of dollars. Prosecutions went up 30% in 2013 and another 30% in 2014, more than half of which have a China connection.

Yet this impressive record of arrests and prosecutions captures just the tip of the iceberg of China's intellectual property theft and other economic espionage operations against us. Despite these hard-won successes for U.S. law enforcement, China's raiding of U.S. technology and trade secrets continues unabated, leaving open the question of what can be done, if anything, to stop the hemorrhage of America's wealth.[24]

Similar questions pertain to China's attacks against U.S. government and other computer systems. For years, the US intelligence community has been warning about China's predatory cyber espionage. Private studies have provided chapter and verse about their sweeping, persistent global operations supporting the exfiltration of cyber data and other purposes (such as corrupting data). As this Commission reported last year,

> The Chinese government appears to believe that it has more to gain than to lose from its cyber espionage and attack campaign. So far, it has acquired valuable technology, trade secrets, and intelligence. The costs imposed have been minimal compared to the perceived benefit. The campaign is likely to continue and may well escalate as the Chinese Communist Party leadership continues to seek further advantage while testing the limits of any deterrent response.

Instead of looking at the strategic implications of China's intelligence operations, the U.S. government for the most part has adopted a case-by-case approach to dealing with the threat they represent. In the wake of the OPM breach and the cumulative effects of China's intelligence successes against us, there is little hope that we can ever get ahead of the curve by staying the course. Perhaps the time has come to take a hard look at how the considerable resources of U.S. counterintelligence are organized and work to counter foreign intelligence services.

Over 80% of U.S. CI resources are based at home[25], where our CI effort has been concentrated on counterespionage investigations, (*i.e.,* on violations of criminal statutes against espionage and related offenses such as failure to register as foreign agent, mishandling of classified information, and certain violations of export control laws). Where successful, these cases may result in prosecutions, demarches, or the expulsion of diplomatic personnel for activities inconsistent with their status. But with rare exception, their disposition is decided on the merits of the instant case and not as part of a larger effort to counter the foreign intelligence service as a strategic target.

---

[23] http://www.cnn.com/2015/07/24/politics/fbi-economic-espionage/

[24] Last year, the U.S. and China entered into an agreement not to conduct "cyber-enabled theft of intellectual property." The jury is out whether it will have any effect. Since stealing western technology and other commercially valuable information is integral to how China's economy works, it's hard to envision them honoring an agreement to stop.

[25] Three-quarters of the U.S. CI budget post-World War II has been devoted to activities within the U.S. carried out by the FBI. In addition, most of the remainder allocated to CIA, the Defense Department, and to small pockets elsewhere in the government, has gone to programs and personnel based wholly or in part within U.S. borders.

By way of example, the government's espionage case against suspected Chinese agent Katrina Leung resulted in a 2005 plea bargain with no jail time and a $10,000 fine, in return for which the accused agreed to 10 debriefing sessions about her interactions with the Chinese.[26] The U.S. attorney in Los Angeles entered into the agreement because it served the government's prosecutorial interest in concluding a case that was not going well in the courtroom; but it effectively forestalled CI efforts to engage Leung's future cooperation to learn what national security information she had compromised during her 20 years of passing information to Beijing, or to uncover other Chinese operations against the U.S. government.

The FBI's counterintelligence division, which first took on responsibility for export control investigations in 2005,[27] has seen a loss of resources and senior leadership attention in favor of the Bureau's weighty counterterrorism responsibilities.[28] Behind the surge in the FBI's economic espionage caseload is an allocation of agent and other time and effort to pursue these investigations potentially at the cost of others. As a result, there are significantly fewer resources devoted to traditional counterintelligence now (*i.e.,* finding, tracking and disrupting foreign intelligence activities in the U.S.) than in the years before 9/11.

Foreign powers such as China have not been blind to the opportunity presented by these constraints on U.S. CI resources. Their numbers and operations in the United States have expanded, enhanced by cyber espionage successes and a benign environment of global engagement. Just as China has become more aggressive in asserting its territorial ambitions in recent years, so might they be expected to press their carefully cultivated intelligence advantages against the United States and our allies.

In my judgment, if the U.S. counterintelligence enterprise continues to operate solely within the confines of its existing business model, we will fall even farther behind, to the detriment of our national security and prosperity.

The Need for a Strategic Counterintelligence Program

When I served as the National Counterintelligence Executive,[29] my office conducted a top-to-bottom review of the U.S. CI landscape and the challenges we faced. We concluded that the national counterintelligence enterprise needed to be reconfigured to go on the offense, to exploit where we can, and interdict where we must, with the purpose of degrading adversary intelligence services and their ability to work against us.

---

[26] See report from the office of the Inspector General https://oig.justice.gov/special/s0605/

[27] In 2005, the FBI sought and received concurrent jurisdiction with the Bureau of Immigration and Customs Enforcement over the enforcement of export control laws.

[28] By FY 2014, there were 4,136 full time agent and other personnel assigned CI vs 7,132 assigned to CT https://www.justice.gov/sites/default/files/jmd/pages/attachments/2015/02/02/24._federal_bureau_of_investigation_fbi.pdf

[29] Established by the *Counterintelligence Enhancement Act of 2002*, the National Counterintelligence Executive (NCIX) serves as the head of U.S. counterintelligence. The office was created to provide strategic direction to the many and disparate elements of U.S. Counterintelligence and ensure the integration of U.S. CI activities. I was the first person to hold the new office, appointed by President Bush in July of 2003. Later made subordinate to the office of the DNI, the NCIX now serves as the DNI's mission manager for counterintelligence and heads the National Counterintelligence and Security Center. The Intelligence Authorization Act of 2017 would restore the position to a Presidential appointment, with Senate confirmation.

In 2005, President Bush signed the first *National Counterintelligence Strategy of the United States*,[30] which had this proactive reorientation as its central goal. However, I must report with regret that we made little progress in executing that strategy. The reasons were many but the principal problem was this: While creating a head of counterintelligence, the law establishing the NCIX did not create a corresponding strategic CI program by which such a mission could be accomplished.

Nor has there been any progress toward creating a national strategic CI program under President Obama; on the contrary, we're going backwards. Intelligence Community Directive 750,[31] signed by DNI Clapper in 2013, explicitly devolves authority and responsibility for all CI programs to the department/agency level, to meet the requirements of the executing department/agency. There is not a whiff of a national-level effort left, other than caretaker duties such as taking inventory and writing reports.

The problem is not a lack of funding. True, total funding for counterintelligence is pitifully low relative to the penalty foreign intelligence successes can exact. But more money is not the cure, so long as the resulting business model of U.S. counterintelligence remains optimized for a defensive posture of working individual cases at home, rather than working the foreign intelligence service as a strategic target globally.

Executing an offensive CI strategy against Chinese intelligence would require a new way of doing business, beginning with working the target abroad. The considerable resources of the members of the U.S. intelligence community that have global reach would need to be directed to help identify and then disrupt or exploit China's intelligence activities, wherever they are directed against U.S. interests worldwide. At home, the proactive CI mission calls for a coordinated, community-wide effort of aggressive operational activity and analysis to obtain the intelligence necessary to neutralize the inevitable penetrations of our government.

Conceptually, this undertaking consists of three parts:

1. Develop the foreign intelligence services "order of battle" (presence, capabilities and activities) thru focused collection and assessment of vulnerabilities
2. Conduct strategic operational planning to redirect or reallocate U.S. collection & operations against this now understood target set based on our capabilities and opportunities for interdiction
3. Integrate and orchestrate CI resources to achieve these strategic objectives.

The proactive approach to counterintelligence requires a generous dose of creativity to turn threat into opportunity. We need to ask, how and where do the Chinese intelligence services operate? Where do they train? How are they tasked? What are their liaison relationships? What are their vulnerabilities? How can they be exploited? For example, more refined insights into the system by which the PRC tasks and executes technology acquisition may suggest means of disrupting or exploiting their operations – techniques effectively employed by the U.S. government against the KGB Line X during the Cold War.[32]

Likewise, the best cyberspace defense is likely to be a good offense. From a counterintelligence perspective, such an approach would require getting inside the attacker's intelligence operations to find out what they are doing and how they are doing it, in order to stop them, confuse them, and otherwise

[30] https://www.ncsc.gov/publications/strategy/docs/FinalCIStrategyforWebMarch21.pdf
[31] https://www.dni.gov/files/documents/ICD/ICD750.pdf
[32] file:///C:/Users/Michelle/Documents/Documents/Earhart%20Project/Vignettes%20research/The%20Farewell%20Dossier%20--%20Weiss.htm

tip the scales in our favor. The Chinese clearly understand the advantages of linking cyber exploits to human operations and inside agents; the U.S. response needs to be equally agile, proactive, and strategically coherent.

The missing element is a national CI program to enable the integrated planning, orchestration and execution of strategic CI operations. The Commission may wish to recommend that Congress consider directing the DNI to establish a pilot strategic CI program, focused on the Chinese intelligence services, to develop options to counter their activities as directed. Here is a draft mission statement, for your consideration:

> U.S. Strategic Counterintelligence shall develop options to degrade the ability of the People's Republic of China to project force or prosecute national objectives, establish or maintain hostile control, or securely conduct operations or collect intelligence and other information against U.S. interests globally, by means of their intelligence activities.

Assigning a strategic, proactive mission to U.S. counterintelligence would be a sharp departure from past practices. In my view, this expansion and strategic reorientation of the U.S. CI enterprise is long overdue. There is no question that our Nation's very talented CI professionals can do this job, provided their leadership sets the right course.

Final thought.

In the wake of the 1995 "walk-in," when the FBI first learned of the shocking compromise of U.S. nuclear weapons design information, Congress levied a series of reporting requirements concerning Chinese espionage activities and what the U.S. government was doing to counter them. (See in particular 42 U.S. Code § 7383e "Annual report by the President on Espionage by the People's Republic of China.") Among other things, the Office of the NCIX inherited the referenced annual reporting responsibility when I first took office. Last year, that law was repealed along with a number of other reporting requirements from which the DNI requested relief. The Commission may wish to consider recommending that it be reinstated.[*]

[*] Disclaimer requested by ODNI: *All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the US Government, ODNI, or intelligence community.*