Testimony before the U.S.-China Economic and Security Review Commission:

Chinese Intelligence Agencies: Reform and Future

John Costello
Fellow, New America Foundation
9 June 2016

Chinese intelligence is growing in sophistication, continuously adopting newer technologies and methods along with its traditional sources of internal monitoring, surveillance, and external clandestine operations. China is in the transition period of creating a full-scope, full-service intelligence community – even if it remains disjointed and is not a "community" as much as a collection of independent agencies – that is capable of exploiting multiple avenues to collect intelligence on the United States. Buttressed and supported by recent major intelligence wins – the OPM data breach looms large in any discussion of Chinese intelligence – China will likely continue to grow in sophistication, tailoring their collection capabilities to the U.S.'s particular vulnerabilities.

China's Intelligence Agencies

There are a number of intelligence and security agencies within China, and this list is by no means exhaustive. It does, however, represent the agencies whose missions and intelligence and security portfolios are a) most relevant to U.S. national security interests and are b) considered to be the premier agents of the Chinese Communist Party in informing policy and achieving political and military objectives. The People's Liberation Army Political Work Department Liaison Departments, the party's United Front Work Department, the Overseas Chinese Affairs Office, Confucius Institutes, and other forms of low-level academic and informal/extralegal technology transfer fall outside the scope of this testimony and will not be discussed.[1]

Ministry of State Security

The Ministry of State Security is primarily responsible for domestic counter-intelligence, non-military foreign intelligence, and aspects of political and domestic security. The MSS was created in 1983 by merging the Central Investigations Department (CID) with portions of the Ministry of Public Security (MPS) that were responsible for counter-intelligence. The MSS consists of its primary central office, provincial departments, and a number of local and municipal bureaus. These state and local bureaus report to both their national ministries and state and local governments and party committees. [2]

The MSS has maintained both a clandestine and overt HUMINT collection capability through a network of defense attaches, academics, and spies operating in and out of China. The ministry's purview and intelligence collection capability has evolved over time, incorporating new missions

[1] Peter Mattis, "A Guide to Chinese Intelligence Operations", *War on the Rocks,* August 18, 2015, http://warontherocks.com/2015/08/a-guide-to-chinese-intelligence-operations/
[2] Peter Mattis, "The Analytic Challenge of Understanding Chinese Intelligence Services", CIA, Sept. 2012, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding%20Chinese%20Intel.pdf

as technology allows.[3] It purportedly boasts a robust cyber mission, and has been connected to a number of high-profile espionage campaigns targeting government, commercial, or federal entities within the United States. It is believed that the MSS is either directly responsible for or the ultimate benefactor of the 2015 hack against the United States Office of Personnel Management, in which 21.5 million sensitive records of federal works were stolen – including fingerprints, personnel records, and background investigation for security clearances.[4]

The Ministry of State Security's foreign intelligence portfolio and corresponding influence in policy and overseas operations has increased steadily in the last two decades. The head of the MSS was added the Foreign Affairs Leading Small Group in the late 90's.[5] The CCP's selection of Geng Huichang to head up the MSS in 2007 is seen by some as a key inflection point for the intelligence service. Geng is the first head of the MSS to specialize in foreign affairs rather than internal security, having previously served as head of China's Institute of Contemporary International Relations.[6]

Ministry of Public Security

The Ministry of Public Security is China's national police force, responsible primarily for internal security missions, maintain public peace and order, and ensuring stability. They also maintain some oversight and control over the People's Armed Police (PAP) force, in conjunction with the People's Liberation Army.[7] They have been active abroad in protecting Chinese citizens and apprehending suspected criminals. MPS has assisted law enforcement in the Congo in 2010 and in Laos in 2011. In the latter case, MPS and domestic law enforcement were able to help apprehend a drug kingpin suspected of killing 13 Chinese nationals along the Mekong river.[8]

In 1983, a substantial portion of MPS's counter-intelligence mission was transferred to the newly established Ministry of State Security, which became the primary security agency for those matters.[9] However, in recent years the MPS has taken on a more assertive and formidable role in

---

[3] Peter Mattis, "The Analytic Challenge of Understanding Chinese Intelligence Services", CIA, Sept. 2012, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding%20Chinese%20Intel.pdf

[4] Ellen Nakashima, "With a series of major hacks, China builds a database on Americans", *The Washington Post,* June 5, 2015, 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

[5] Lu Ning, "The Central Leadership, Supraministry Coordinating Bodies, State Council Ministries, and Party Departments,", *The Making of Chinese Foreign and Security Policy in the Era of Reform 1978–2000*, ed. David Lampton (Stanford, CA: Stanford University Press, 2001), pp. 50, 414.

[6] Peter Mattis, "The Analytic Challenge of Understanding Chinese Intelligence Services", CIA, Sept. 2012, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding%20Chinese%20Intel.pdf

[7] "Ministry of Public Security", *Global Security,* http://www.globalsecurity.org/intell/world/china/mps.htm

[8] Peter Mattis, "Angola Operation Shows China Testing Overseas Security Role; Cambodian Visit to China Rubs Salt in ASEAN Wounds", *China Brief Volume: 12 Issue: 17*, The Jamestown Foundation, Sept. 7, 2012, http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=39812&no_cache=1#.V1fBTZErLZt

[9] Peter Mattis, "The Analytic Challenge of Understanding Chinese Intelligence Services", CIA, Sept. 2012, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding%20Chinese%20Intel.pdf

domestic intelligence and counter-espionage. MPS's steadily growing budget, technical and cyber sophistication coupled with its control over networked surveillance resources and national databases have made it a powerful counterintelligence operation in its own right.[10]

At the national level, Ministry of Public Security is made up of its central office in Beijing and directly subordinate offices in each province, autonomous region, and municipality, known as public security bureaus (PSB). All provincial, regional, and municipal PSB's have subordinate offices a lower-echelon administrative levels.[11]

Chinese Military Intelligence

The military reforms announced in November 2015 made substantial changes to the PLA's organizational structure, knocking down silos, abolishing old organizations, and creating new ones. The changes also shook up operational responsibilities and reorganized units along new administrative lines. These changes have left the status of the PLA's intelligence organizations unclear. The testimony below will reflect what is known about the PLA's known intelligence agencies prior to the reforms, unless otherwise indicated.

The General Staff Department Second Department

The General Staff Department Second Department (2PLA), also known as the GSD Intelligence Department, is roughly equivalent to the U.S Defense Intelligence Agency, combining functions associated with the National Geo-Spatial Intelligence Agency (NGA) and the National Reconnaissance Office (NRO). The 2PLA is responsible for foreign military and political intelligence collection and analysis. The department also engages in both overt and clandestine HUMINT operations and manages PLA military attaches stationed in PRC embassies around the world.[12]

While the 2PLA has been better known for its HUMINT collection capabilities, it has a growing technical intelligence portfolio and is regarded as increasingly reliant on space-based and airborne intelligence, surveillance, and reconnaissance.[13] Two subordinate bureaus manage and oversee the technical and operational details of its space and air collection capabilities. The Aerospace Reconnaissance Bureau (ARB) is responsible for space-based intelligence, surveillance, and reconnaissance. The ARB seems primarily focused on overhead imagery (IMINT) and electro-optical collections.[14] The Tactical Reconnaissance Bureau is responsible

[10] Peter Mattis, "Informatization Drives Expanded Scope of Public Security", *China Brief Volume: 13 Issue: 8*, The Jamestown Foundation, April 12, 2013, http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=40721&no_cache=1#.Vcj1rvlViko

[11] "Responses to Information Requests", *Immigration and Refugee Board of Canada*, Oct. 10, 2014, https://www.justice.gov/sites/default/files/eoir/legacy/2014/11/13/CHN104967.E.pdf

[12] Kevin Pollpeter and Kenneth Allen, *PLA as Organization 2.0*, (2016), pp. 145-148

[13] Easton and Hsiao, "The Chinese People's Liberation Army's Unmanned Aerial Vehicle Project: Organizational Capacities and Operational Capabilities", *The Chinese People's Liberation Army's UAV Project,* Project 2049 Institute, March 11, 2013, https://project2049.net/documents/uav_easton_hsiao.pdf

[14] Kevin Pollpeter and Kenneth Allen, *PLA as Organization 2.0*, (2016), pp. 145-148

for joint airborne reconnaissance and intelligence in addition to managing a fleet of strategic long-range UAV's, likely based in Shahe airfield near Beijing.[15]

The 2PLA is suspected to operate regional liaison offices in Tianjin, Beijing, Guangzhou, Shanghai, and Shenyang, reportedly occasionally using unnamed, numbered municipal offices as a cover.[16]

The General Staff Department Third Department

The General Staff Department Third Department (3PLA), also known as the Technical Department, is roughly equivalent the United States National Security Agency (NSA) in function and mission. The department is responsible for the PLA's signals intelligence (SIGINT) mission with some additional responsibility for cryptographic and classified systems. Additionally, the 3PLA has become the PLA's premiere department responsible or computer network exploitation (CNE) and cyber espionage. It's advanced technical capabilities, facilities, cryptographic mission, and linguistic personnel make the CNE mission a natural fit within the 3PLA's purview.[17]

The 3PLA's cyber espionage mission is both well-documented and well know. The TRB's and subordinate offices have been linked to a number of high-profile campaigns in recent years, with security researchers able to collect enough data to identify specific PLA individuals involved in intrusions.[18] In 2013, the United States Justice Department famously indicted a group of five 3PLA hackers for intellectual property theft.[19] The five were identified as personnel belonging to Unit 61398, a 3PLA Second Bureau unit based out of Pudong, Shanghai. In 2014, the cyber intelligence firm ThreatConnect and the defense contractor Defense Group Inc. identified another hacker operating within a Chengdu Military Region TRB (Unit 78020).[20]

General Staff Department Fourth Department

The General Staff Department Fourth Department (4PLA), also known as the Electronic Countermeasure and Radar Department, is primarily responsible for electronic attack (or jamming), electronic protection, and electronic support measures. The 4PLA is the sole organization responsible for electronic intelligence (ELINT) in the PLA and covers both the technical (TECHELINT) and operational (OPELINT) missions. Its mission has evolved and expanded over the years to also include computer network attack (CNA) and more strategic

---

[15] Easton and Hsiao, "The Chinese People's Liberation Army's Unmanned Aerial Vehicle Project: Organizational Capacities and Operational Capabilities", *The Chinese People's Liberation Army's UAV Project,* Project 2049 Institute, March 11, 2013, https://project2049.net/documents/uav_easton_hsiao.pdf

[16] Peter Mattis, "China's Espionage Against Taiwan (Part II): Chinese Intelligence Collectors", *China Brief Volume: 14 Issue: 23,* The Jamestown Organization, Dec. 5, 2014, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=43161&cHash=65b3729a7a402f49610ea0b38e9463ee#.V1eNWZErLZs

[17] Kevin Pollpeter and Kenneth Allen, *PLA as Organization 2.0*, (2016), pp. 148-150

[18] "Exposing One of China's Cyber Espionage Units", Mandiant, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

[19] *United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chuhui*, 1 May 2014, https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf

[20] "Camerashy: Closing the Aperature on China's Unit 78020", ThreatConnect Inc. and Defense Group Inc., 2015, https://cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf

electronic denial missions like satellite jamming. According to some analysts the 4PLA is capable of disrupting adversary communications, navigation, and synthetic aperture radar (SAR) satellites.[21]

The 4PLA's cyber mission is first and foremost focused on the disruption and denial of enemy computer networks. The targeting necessary to successfully carry out these missions requires the 4PLA to have a strong network surveillance component. This operational targeting in both cyber and electronic domains form the basis of 4PLA's role as an intelligence service.

Campaign and Tactical

This overarching structure in the General Staff Department is mirrored in the PLA Navy, PLA Air Force, Second Artillery Corps, and the PLA's seven subordinate military regions. The operational units of the 4PLA are mirrored in counterparts existing at the national level for the services and embedded within group armies for the military regions. The degree to which these parallel structures coordinate with their GSD counterparts is unclear and remains one of the biggest questions in how the PLA oversees, coordinates, and fuses its intelligence at regional levels.

Chinese Intelligence and Policymaking

Analyzing how and by whom Chinese policy is formed is a murky prospect even under the best of circumstances. Introducing questions of how and to what degree intelligence shapes and informs these policies compounds this problem further, adding an additional layer of obscurity that makes it nearly impossible to "seek truth from facts" on Chinese intelligence. What we can do, however, is identify the intelligence agencies responsible for collection and analysis and their chains of command they are nominally intended to inform.

Leadership

The civilian intelligence services are overseen and governed by the Politburo Standing Committee (PSC). Reporting to the PSC, the Central Political-Legal Affairs Commission is the party's central coordinating body and authority overseeing domestic security, police actions, and the counter-intelligence and counter-espionage missions, including the Ministry of Public Security and Ministry of State Security. While both are nominally ministerial-level organizations of the State Council, it is presumed that the party's Political-Legal Affairs Commission is the real tasking and leading authority over the intelligence activities of both ministries.

The Chinese military intelligence services are overseen and governed by the Central Military Commission. The newly-created Joint Staff Department is directly subordinate to the state and party CMC's, and manages operations and intelligence portfolio of the Chinese military. Before the recent reforms, the General Staff Department oversaw the 2PLA, 3PLA, and 4PLA and was the major organ in charge of military intelligence

Tasking and Priorities

[21] Kevin Pollpeter and Kenneth Allen, *PLA as Organization 2.0*, (2016), pp. 157-158

It's unclear to what degree the topical leading small groups task intelligence services or set priorities – if they do at all. The control and major decisions may lie in the Central Military Commission and the Central Political-Legal Committee, but the subordinate organs may report to and inform various leading small groups, offices, and departments across the party, government, and military across all levels as necessary. For instance, the Foreign Affairs and National Security Leading Small Groups[22] are places where the MSS may report information and deliver intelligence, but final tasking and control of intelligence operations may lie with the Political-Legal Commission. It's unclear who sets priorities and tasking, and who the ultimate "customer" of intelligence may actually be.

State Security Committee

It is also unknown what role the State Security Committee, also known as China's "Nation Security Council" will play in guiding or overseeing intelligence operations. Established in November 2013 at the third Plenary Session of the 18th Central Committee, the committee is headed by Xi Jinping and is answerable to the Politburo Standing Committee (PSC).[23] It is responsible for "making overall plans and coordinating major issues and major work concerning national security."[24] Some have suggested that the committee may just be another Xi-created organ to ensure stability of the party.[25] The stated mission, role, and even the name of the committee suggests that it will focus more on domestic security and public stability than outward national security issues, but this does not necessarily exclude external national security from its remit.[26] There is still much we don't know about the organization, including its full membership and exact functions, and its exact role in intelligence operations and coordination – if it has any at all – is currently unclear.

Political Neutrality

Despite the political leadership of China's intelligence services, there is a distinct desire by all party factions for counter-espionage and intelligence agencies to be "faction neutral", if not wholly apolitical. This is likely due to the Party's storied legacy of using "counterespionage" charges to purge enemies and settle ideological differences. As such, there is a real reluctance for any one political leader to have control over the state's intelligence apparatus. The previous head of the Political-Legal Affairs Commission, Zhou Yongkang, was ousted from his spot and removed from the Politburo Standing Committee likely out of fears that he was using domestic security and intelligence apparatus for political ends – particularly in connection with Bo Xilai.[27] It was the desire to depoliticize the intelligence services that motivated moving substantial portions of the MPS's counterintelligence mission to the newly-created MSS in 1983. Notably,

---

[22] Alice Miller, "The CCP Central Committee's Leading Small Groups", *China Leadership Monitor, No. 26,* The Hoover Institute, http://www.hoover.org/sites/default/files/uploads/documents/CLM26AM.pdf

[23] Ankit Panda, "What Will China's New National Security Council Do?", *The Diplomat,* Nov. 14, 2013, thediplomat.com/2013/11/what-will-chinas-new-national-security-council-do/

[24] "Xi Jinping to lead national security commission", *China Daily,* Jan. 24, 2014, http://www.chinadaily.com.cn/china/2014-01/24/content_17257409.htm

[25] You Ji, "China"s National Security Commission: theory, evolution and operations"*, Journal of Contemporary China*, 2016, http://www.tandfonline.com/doi/full/10.1080/10670564.2015.1075717

[26] Yun Sun, "China's New 'State Security Committee': Questions", *PacNet Number 81*, Pacific Forum CSIS, Nov. 14, 2013.https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/Pac1381_0.pdf

[27] Jeremy Page, "China Reins In New Security Boss's Clout", *The Wall Street Journal,* Nov. 20, 2012, http://www.wsj.com/articles/SB10001424127887323622904578128683521454390

the first chief of the MSS, Ling Yun set the tone of the ministry as a neutral and reliable organ in internal security and counter-espionage, indicating that counterespionage wouldn't be exploited for ideological purges and power plays within the party.[28] The subsequent chiefs of the Ministry of State Security are seemingly chosen for their lack of connections to any one party faction and degree of "political reliability."[29]

Military Reforms and Military Intelligence

In November 2015 China announced a series of impeding reforms that would shake up military services and ultimately effect a substantial realignment of its institutions, transforming their antiquated Soviet-era structure into a more modern, updated force able to fight and win wars. In what is considered to be the largest and most sweeping reforms since the 1950's, there are still many unanswered questions.[30] The status of the main intelligence organs of the PLA – the 2PLA, 3PLA, and 4PLA – is at the heart of understanding what's next for Chinese military intelligence. We must first examine what we do know and the broad strokes of what has changed.

Joint Staff Department and the Intelligence Bureau

At the very top level, the PLA has been reshuffled. Under the reforms, the General Staff Department has been reorganized into the new Joint Staff Department (JSD), with the PLA Army getting a new independent headquarters separate and distinct from the JSD. The JSD has formed a new Intelligence Bureau (IB), likely as a successor to the 2PLA's mission. It is unclear, however, to what degree its personnel, mission, or organization were pulled from the previous 2PLA or were created entirely anew.

Open questions aside, both of these measures reduce the primacy of the PLA Army in the intelligence bureaucracy, and at least removes many of the institutional barriers that allowed the PLA to dominate both intelligence and operational authorities. This change at least has the potential for new resources to be made available for use by the other services, the PLAN, PLAAF, and the newly created PLA Rocket Force (PLARF).[31]

These changes should also have a cascading effect down to the operational and tactical levels. The previously Army-dominated military region's reorganization into joint military theaters or "battle zones" necessitates a change in structure and operation at the campaign and operation levels of war. The theater commands may completely reorganize the military theater technical reconnaissance bureaus, intelligence departments, and electronic countermeasure brigades into

---

[28] Peter Mattis, "China's Intelligence Reforms?", *The Diplomat*", Jan. 23, 2013, http://thediplomat.com/2013/01/chinas-intelligence-reforms/

[29] Peter Mattis, "Assessing the Foreign Policy Influence of the Ministry of State Security", *China Brief Volume: 11 Issue: 1,* The Jamestown Foundation, Jan. 14, 2011, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=37368&cHash=0239321b02#.V1hHQ5ErLZs

[30] David M. Finkelstein, "Initial Thoughts on the Reorganization and Reform of the PLA", CAN Corporation, January 15, 2016, https://www.cna.org/cna_files/pdf/DOP-2016-U-012560-Final.pdf

[31] Peter Mattis, "China's Military Intelligence System is Changing", *War on the Rocks,* December 29, 2015, http://warontherocks.com/2015/12/chinas-military-intelligence-system-is-changing/

more joint-force components better able to support the theater's mandate of "focusing on fighting."[32]

Strategic Support Force

The reforms have introduced a new service called the Strategic Support Force that will almost certainly have a profound effect on China's military intelligence community and its capabilities, although it is as yet certain what those effects may be. Initial reports suggest that the force is primarily responsible for the PLA's space, cyber, and electronic countermeasure mission.[33] At its most basic, Strategic Support Force may be the Chinese equivalent of United States Strategic Command (STRATCOM). Like STRATCOM, the force is intended to combine strategic information operations, such as cyber warfare and electronic warfare, with strategic C4SIR. Whether the PLA will treat the SSF as a service or more as a functional, operational set of units remains to be seen. It's specific roles, mission, and administrative/operational context will likely remain unclear for the foreseeable future.[34]

- On the cyber intelligence front, it's unclear if the SSF will centralize China's cyber mission by reducing the institutional barriers separating computer network attack, espionage, and defense, which have traditionally been "stove-piped" and handled by separate organizations within the PLA. There has been little-to-no information regarding the status of either the 3PLA or 4PLA's cyber missions or whether they have been modified, abolished, or transferred wholesale to the Strategic Support Force.

- The picture is a bit clearer on the space-based ISR mission, with initial experts suggesting that the SSF would almost exclusively manage China's space-based strategic ISR, including "target tracking and reconnaissance, daily operation of satellite navigation, operating Beidou satellites, [and] managing space-based reconnaissance assets."[35] These claims are validated somewhat by the recent announcement that Zhou Zhixin, the previous head of the 2PLA's Aerospace Reconnaissance Bureau in charge of space-based ISR, will be heading up an "unidentified bureau" in the SSF.[36]

- For electronic warfare and electronic support measures, the 4PLA will almost certainly form the core of this new force. The 4PLA's supposed strategic electronic warfare capabilities against satellites and its dominance in radar and ELINT make it an almost

---

[32] http://thediplomat.com/2016/01/china-finally-its-centralizes-space-cyber-information-forces/

[33] John Costello, "The Strategic Support Force: China's Information Warfare Service", *China Brief Volume: 16 Issue: 3*, The Jamestown Foundation, February 8, 2016, http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=45075&no_cache=1#.V1jXRZErLZs

[34] http://thediplomat.com/2016/01/china-finally-its-centralizes-space-cyber-information-forces/

[35] John Costello, "The Strategic Support Force: China's Information Warfare Service", *China Brief Volume: 16 Issue: 3*, The Jamestown Foundation, February 8, 2016, http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=45075&no_cache=1#.V1jXRZErLZs

[36] "中科院院士周志鑫出任战略支援部队某局局长" ["Chinese Academy of Sciences Academician Zhou Zhixin to Become Bureau Chief of Unidentified Bureau in Strategic Support Force"], *IFeng Talk,* April 9, 2016, http://news.ifeng.com/a/20160409/48403966_0.shtml

certainty that the 4PLA will form a substantial portion of the SSF's electronic warfare force.

Regardless of the specifics of how the 3PLA and 4PLA will integrate with this new force, it's clear that the concentration of strategic intelligence, surveillance, and reconnaissance missions within the Strategic Support Force gives the Central Military Commission a much freer hand in setting priorities, evaluating tasking, and shaping the force to better serve military objectives.

The new guiding principles of the reforms "CMC will lead, the services will build, and the theaters will fight" institute a division of labor that if followed will create an environment that will allow the services to create ever-more sophisticated methods of intelligence collection and allow the CMC to more ably tailor intelligence operations to support the strategic needs of the Chinese military.[37]

The centralization of the cyber mission, too, would have profound effects on the PLA, likely allowing for a more effective and sophisticated cyber mission that combines all elements of computer network operations – reconnaissance, exploitation, attack, and defense.

The Future of Chinese Intelligence

Driven by the desire for economic growth, energy security, and shoring up its own domestic control, the Communist Party has pushed China militarily and economically outward into international areas of strategic competition. As it has done so, the intelligence needs of the central government in Beijing have changed dramatically and have required a requisite shift in its intelligence services.

Based upon the recent reforms and the changing intelligence needs of the central government we can expect that Chinese intelligence agencies will continue to grow in sophistication and operational tradecraft. Additionally, the trend towards centralization and de-confliction in military intelligence will likely continue, substantially helped along by both anti-corruption campaigns and the rice-bowl-breaking reforms we've seen in the past year. This trend may even eventually extend outward to the broader civilian and political intelligence mechanisms, but this is by no means a certainty.

For the future, China's intelligence agencies will need to create a more robust and reliable collection infrastructure that can produce regular sources of intelligence that is both timelier and more relevant for national policy-making and military operations.

Based on these facts, we can surmise the following specific trends in future Chinese intelligence collection:

Firstly, China's civilian and military intelligence agencies will likely continue to focus on "legitimate" intelligence targets that offer more relevant intelligence into U.S. policy, diplomacy, and military operations. We should expect to see continuing Chinese efforts to breach U.S.

---

[37] Phillip C. Saunders and Joel Wuthnow, "China's Goldwater-Nichols? Assessing PLA Organizational Reforms", *Strategic Forum,* National Defense University, April 2016, http://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-294.pdf

government and military systems, building upon their database of federal workers and military personnel. While the verdict is still out on whether the Xi-Obama joint declaration to not conduct economic espionage will prove to be long-lasting, the last year and a half *have* shown a significant drop in the number of Chinese cyber intrusions against U.S. companies.[38] The military may still target industrial and commercial targets, but these cyber missions would be focused on the needs of PLA decision-makers to field new countermeasures and capabilities, rather than supporting existing defense programs.[39]

Secondly, if China continues on the path of centrally coordinating its cyber espionage mission, the United States is likely to see a substantial decrease in number of cyber intrusions while their overall sophistication will likely increase; this is the so-called "Russian" model of cyber espionage. There are two reasons for this change. Growing professionalism, mission de-confliction, and coordination will undoubtedly cause cyber operations planners to be more selective in their targeting and risk-averse in their tradecraft in order to optimize success. Two, desire for sustained collection to develop longer-term sources of intelligence collection will require a more cautious approach and will prioritize maintaining a persistent presence at the expense of short-term gains. Likely passed are the days of "smash and grab" tactics many defense firms and U.S. agencies are used to. Long-term capabilities will be the primary cyber imperative rather than the short-term intelligence gains inherent in economically motivated cyber campaigns.

Finally, China will likely marry its database of federal and military workers with real-time intelligence collected from other sources. While the OPM data itself likely gives a good static snapshot of federal and military workers, the data is limited. It isn't "live"; It can't provide operational details of military and federal personnel or answer broader questions on their work. However, the data provides a perfect targeting set for follow-on exploitation and a natural framework with which to correlate and evaluate new intelligence. Cyber intrusions against communications, social media, and data-service providers may provide real-time intelligence that, when correlated with OPM data, could provide remarkable insight into U.S. policy and government and military operations.

Vulnerabilities and Recommendations

Chinese intelligence capabilities remain as much a black box as they ever have been. However, the last few years have shown that the Chinese are capable of sustained, sophisticated intelligence operations targeting areas where the United States is most vulnerable.

Federal Contractors and Cybersecurity

Federal contractors are the consistent soft-underbelly in cyber intrusions targeting the federal government and the military. Poor information security and cybersecurity practices have

---

[38] Joseph Menn and Doina Chiacu, "Cyber attacks from China against the US may be slowing down ahead of Obama's meeting with Xi Jinping", *Business Insider,* September 19, 2015, http://www.businessinsider.com/chinese-cyber-attacks-against-the-us-are-slowing-2015-9

[39] Peter Mattis, "Military Intelligence at a Crossroads", *The Cipher Brief,* Feb. 19, 2016, https://thecipherbrief.com/article/asia/military-intelligence-crossroads

consistently allowed federal and defense contractors to be the vector by which major national security breaches have occurred. In 2014, hackers were able to steal a Keypoint Government Solutions credential to obtain access to the Office of Personnel Management, ultimately leading to largest national security breach in United States History.[40] In 2009, Chinese hackers were able to penetrate Boeing's servers and steal advanced technical documents related to the F-22 and F-35.[41]

The Department of Defense's Defense Federal Acquisition Regulations have recently been updated to include cybersecurity requirements for acquisitions and defense contractors. These requirements expand the scope of information security oversight for defense contractors and require a higher degree of incident reporting and, among other things, dual-factor authentication on local network access.[42]

Although this is a step in the right direction, defense contractors are not the only contractors in use by the federal government. Congress should consider using DFAR cybersecurity requirements as a model for new legislation that would allow for the same protections and requirements extended to all government contractors that use or connect to federal information security systems.

Federal Workers and Open-source Exploitation

For open-source exploitation, the OPM data breach looms large. This data provides a comprehensive target set for reconnaissance and exploitation of our most trusted government workers. Underpinned and informed by the OPM data and other related breaches, Chinese intelligence agencies have a veritable road-map of who to target and exploit. The wide-spread use of LinkedIn, Facebook, Instagram, Twitter, and other public networking sites have created a host of opportunities for both large-scale collections and reconnaissance as well as tailored-targeting on U.S. persons. If secured improperly, these sites could allow analysts to track military operations or provide further opportunities for compromise or cyber intrusion. What's more, the usage of lesser-known adult dating sites and "deep" and "dark" web provides further opportunities for U.S. military and government personnel to be blackmailed or exploited based on their online activity.

Congress should continue to review new ways to incorporate open-source exploitation, social media accounts, and illicit or covert web activity into the background investigation process, particularly for individuals seeking higher-level clearances in federal agencies and the military.[43]

---

[40] Aaron Boyd, "Contractor Breach Gave Hackers Keys to OPM Data", *Federal Times,* June 25, 2015, http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/23/keypoint-usis-opm-breach/28977277/

[41] Bill Gertz, "China Hacked F-22, F-35 Stealth Jet Secrets", *Washington Free Beacon,* March 24, 2016, http://freebeacon.com/national-security/china-hacked-f22-f35-jet-secrets/

[42] *Defense Federal Acquisition Regulations, SUBPART 204.73- --SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING, accessed on June 1, 2016 at* http://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm

[43] Zach Noble, "OPM Wants to Fold Deep Web, Social Media into Background Checks", *FCW,* April 12, 2016, https://fcw.com/articles/2016/04/12/social-media-clearance.aspx

There has been movement in both the House towards updating the background investigation process with this in mind, hopefully these efforts will continue.[44]

Secondly, military organizations and federal agencies should strengthen their OPSEC programs. This would include teaching personnel how to properly manage privacy and security controls on their social media and networking accounts as well as occasionally monitoring them for OPSEC violations and indications of exploitation and/or targeting.

[44] Mario Trujillo, "Congress Probes Use of Social Media in Background Checks", *The Hill,* May 16, 2016, http://thehill.com/policy/technology/279715-congress-probing-use-of-social-media-in-government-background-checks