

CHINA'S INTELLIGENCE SERVICES AND ESPIONAGE OPERATIONS

HEARING

BEFORE THE

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

**ONE HUNDRED FOURTEENTH CONGRESS
SECOND SESSION**

THURSDAY, JUNE 09, 2016

Printed for use of the
United States-China Economic and Security Review Commission
Available via the World Wide Web: www.uscc.gov



**UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW
COMMISSION**

WASHINGTON: 2016

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

HON. DENNIS C. SHEA, *Chairman*
CAROLYN BARTHOLOMEW, *Vice Chairman*

Commissioners:

PETER BROOKES	DANIEL M. SLANE
ROBIN CLEVELAND	HON. JAMES TALENT
HON. BYRON L. DORGAN	DR. KATHERINE C. TOBIN
JEFFREY L. FIEDLER	MICHAEL R. WESSEL
HON. CARTE P. GOODWIN	DR. LARRY M. WORTZEL

MICHAEL R. DANIS, *Executive Director*

The Commission was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act for 2001 § 1238, Public Law No. 106-398, 114 STAT. 1654A-334 (2000) (codified at 22 U.S.C. § 7002 (2001), as amended by the Treasury and General Government Appropriations Act for 2002 § 645 (regarding employment status of staff) & § 648 (regarding changing annual report due date from March to June), Public Law No. 107-67, 115 STAT. 514 (Nov. 12, 2001); as amended by Division P of the “Consolidated Appropriations Resolution, 2003,” Pub L. No. 108-7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of the Commission); as amended by Public Law No. 109-108 (H.R. 2862) (Nov. 22, 2005) (regarding responsibilities of Commission and applicability of FACA); as amended by Division J of the “Consolidated Appropriations Act, 2008,” Public Law No. 110-161 (December 26, 2007) (regarding responsibilities of the Commission, and changing the Annual Report due date from June to December); as amended by the Carl Levin and Howard P. “Buck” McKeon National Defense Authorization Act for Fiscal Year 2015, P.L. 113-291 (December 19, 2014) (regarding responsibilities of the Commission).

The Commission’s full charter is available at www.uscc.gov.

August 11, 2016

The Honorable Orrin Hatch
President Pro Tempore of the Senate, Washington, D.C. 20510
The Honorable Paul Ryan
Speaker of the House of Representatives, Washington, D.C. 20515

DEAR SENATOR HATCH AND SPEAKER RYAN:

We are pleased to notify you of the Commission's June 09, 2016 public hearing on "Chinese Intelligence Services and Espionage Operations." The Floyd D. Spence National Defense Authorization Act (amended by Pub. L. No. 113-291) provides the basis for this hearing.

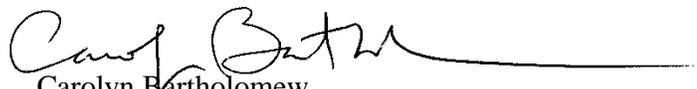
At the hearing, the Commissioners received testimony from the following witnesses: Mr. Peter Mattis, Fellow, Jamestown Foundation; Mr. John Costello, Congressional Innovation Fellow, New America; Mr. Mark Stokes, Executive Director, Project 2049 Institute; Ms. Michelle Van Cleave, Former National Counterintelligence Executive; and Mr. David Major, Founder and President, CI Centre. This hearing examined the structure, capabilities, and recent reforms of Chinese intelligence services. It described how China conducts espionage and other forms of intelligence collection. It also assessed the implications for U.S. national security of Chinese espionage operations in the United States and abroad that target U.S. national security organizations and actors, including U.S. defense industrial chains, military forces, and leading national security decision makers. Panelists discussed recommendations for congressional action to address the threat of Chinese intelligence collection against the United States.

We note that prepared statements for the hearing, the hearing transcript, and supporting documents submitted by the witnesses are available on the Commission's website at www.USCC.gov. Members and the staff of the Commission are available to provide more detailed briefings. We hope these materials will be helpful to the Congress as it continues its assessment of U.S. - China relations and their impact on U.S. security.

The Commission will examine in greater depth these issues, and the other issues enumerated in its statutory mandate, in its 2016 Annual Report that will be submitted to Congress in November 2016. Should you have any questions regarding this hearing or any other issue related to China, please do not hesitate to have your staff contact the Commission at (202) 624-1407 or via email at RBerrien-Lopez@uscc.gov.

Sincerely yours,


Hon. Dennis C. Shea
Chairman


Carolyn Bartholomew
Vice Chairman

CONTENTS

THURSDAY, JUNE 09, 2016

CHINA'S INTELLIGENCE SERVICES AND ESPIONAGE OPERATIONS

Opening Statement of Senator Byron Dorgan (Hearing Co-Chair)	01
Prepared Statement.....	02
Opening Statement of Commissioner Peter Brookes (Hearing Co-Chair)	03
Prepared Statement.....	04

Panel I: Structure, Reforms, and Capabilities of Chinese Intelligence Services

Panel I Introduction by Commissioner Peter Brookes (Hearing Co-Chair)	05
Statement of Mr. John Costello Congressional Innovation Fellow, New America	06
Prepared Statement.....	09
Statement of Mr. Mark Stokes Executive Director, Project 2049 Institute	20
Prepared Statement.....	23
Statement of Mr. Peter Mattis Fellow, Jamestown Foundation.....	28
Prepared Statement.....	31
Panel I: Question and Answer.....	41

Panel II: Chinese Intelligence Collection Operations and Implications For U.S. National Security

Panel II Introduction by Senator Byron Dorgan (Hearing Co-Chair)	60
Statement of Ms. Michelle Van Cleave Former National Counterintelligence Executive.....	61
Prepared Statement.....	64
Statement of Mr. David Major Founder and President, CI Centre	74
Prepared Statement.....	77
Panel II: Question and Answer	94

CHINA'S INTELLIGENCE SERVICES AND ESPIONAGE OPERATIONS

THURSDAY, JUNE 09, 2016

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Washington, D.C.

The Commission met in Room 285 of the Hall of the States Building, Washington, DC at 9:00 a.m. Senator Byron Dorgan and Commissioner Peter Brookes (Hearing Co-Chairs), presiding.

OPENING STATEMENT OF COMMISSIONER BYRON DORGAN HEARING CO-CHAIR

HEARING CO-CHAIR DORGAN: We'll begin the hearing today. This is the U.S.-China Economic and Security Review Commission, and today the hearing is on Chinese intelligence services and espionage operations. We welcome all of you, and this is the sixth hearing of the Commission in the 2016 Annual Report cycle.

Today's hearing is going to consider Chinese intelligence collection operations affecting U.S. national security.

The hearing comes amidst many reports of actors affiliated with the Chinese government extracting or attempting to extract sensitive information from the national defense, from U.S. military forces, defense contractors, government organizations and more. These infiltrations have not been limited to cyber attacks. In many cases, human agents operating in the United States were responsible.

So to understand our vulnerability to Chinese espionage and to raise public awareness of the threat to U.S. national security, it's crucial to defend against it. To this end, this hearing will investigate which U.S. national security entities China targets, how China attempts to infiltrate these targets, and how successful China is in extracting information from these targets.

The hearing will also examine the effectiveness of U.S. actors in deterring, tracking, preventing, and mitigating these operations.

We look forward to exploring these issues with some excellent witnesses and hope to find creative ways the United States can respond to the intelligence threat from China.

Now I'll turn the floor over to my co-chair for this hearing, Commissioner Peter Brookes.

**PREPARED STATEMENT OF COMMISSIONER BYRON DORGAN
HEARING CO-CHAIR**

Hearing on “Chinese Intelligence Services and Espionage Operations”

**Opening Statement of Senator Byron Dorgan
June 9, 2016
Washington, DC**

Good morning, and welcome to the sixth hearing of the U.S.-China Economic and Security Review Commission’s 2016 Annual Report cycle. Thank you all for joining us today.

Today’s hearing will consider Chinese intelligence collection operations affecting U.S. national security.

This hearing comes amid many recent reports of actors affiliated with the Chinese government extracting or attempting to extract sensitive U.S. national defense information from U.S. military forces, defense contractors, and government organizations. These infiltrations have not been limited to cyber attacks. In many cases, human agents operating in the United States were responsible.

Understanding our vulnerability to Chinese espionage and raising public awareness of the threat to U.S. national security is crucial to defending against it. To this end, this hearing will investigate which U.S. national security entities China targets; how China attempts to infiltrate these targets; and how successful China is in extracting information from these targets. This hearing will also examine the effectiveness of U.S. actors in deterring, tracking, preventing, and mitigating these operations.

Today, we look forward to exploring these issues and hope to find creative ways the United States can respond to the intelligence threat from China.

Now I’ll turn the floor over to my co-chair for this hearing, Commissioner Peter Brookes.

**OPENING STATEMENT OF COMMISSIONER PETER BROOKES
HEARING CO-CHAIR**

HEARING CO-CHAIR BROOKES: Thank you, Senator Dorgan, and welcome to our guests and panelists today.

As many of you know, Chinese espionage against the United States is not just a recent phenomenon. Chinese intelligence actors have infiltrated U.S. national security entities since the earliest days of the People's Republic of China.

However, reports of Chinese espionage against the United States have risen significantly over the past 15 years. At the same time, the national security concerns and implications of these breaches have grown and made U.S.-China security tensions, Beijing's expanding military might, and questions about the PRC's strategic intentions.

In addition to the many cases of Chinese espionage conducted in the United States, the threat from Chinese intelligence collection also extends outside of the United States. The United States shares military equipment and national security secrets with many countries that China has targeted with espionage operations. China's infiltration of defense entities in these countries could allow China to extract sensitive U.S. national defense information.

China has also invested significant resources in building up its capabilities to collect military technical intelligence. These capabilities would strengthen China's hand in a military confrontation with the United States, its allies, or partners.

To help us better understand the implications of these developments for U.S. national security, we are joined by distinguished experts and long-time observers of Chinese intelligence. Thank you for taking your time from your busy schedules to appear here today. We look forward to hearing from each one of you.

As a reminder, the testimonies and transcript from today's hearing will be posted on our website, which is uscc.gov. You'll find a number of other resources there, including our annual reports, staff papers, and links to important news stories about China and U.S.-China relations.

Lastly, let me thank the Commission staff, especially Mike Pilger, for his hard work in putting together today's hearing. Let's get started with the first panel unless anybody else wants to say anything. Chairman?

**PREPARED STATEMENT OF COMMISSIONER PETER BROOKES
HEARING CO-CHAIR**

Hearing on “Chinese Intelligence Services and Espionage Operations”

**Opening Statement of Commissioner Peter Brookes
June 9, 2016
Washington, DC**

Thank you, Senator Dorgan, and welcome to our guests and panelists.

As many of you know, Chinese espionage against the United States is not just a recent phenomenon. Chinese actors have infiltrated U.S. national security entities since the earliest days of the People’s Republic of China. However, reports of Chinese espionage against the United States have risen significantly over the past fifteen years. At the same time, the national security implications of these breaches have grown amid U.S.-China security tensions and China’s expanding military capabilities.

In addition to the many cases of Chinese espionage conducted in the United States, the threat from Chinese intelligence collection also extends outside the United States. The United States shares military equipment and national security secrets with many countries that China has targeted with espionage operations. China’s infiltration of defense entities in these countries could allow China to extract sensitive U.S. national defense information.

China has also invested significant resources in building up its capabilities to collect military technical intelligence. These capabilities would strengthen China’s hand in a military confrontation with the United States.

To help us better understand the implications of these developments for U.S. national security, we are joined by distinguished experts and long-time observers of Chinese intelligence. We look forward to hearing from each of you.

As a reminder, the testimonies and transcript from today’s hearing will be posted on our website, www.uscc.gov. You’ll find a number of other resources there, including our Annual Reports, staff papers, and links to important news stories about China and U.S.-China relations.

PANEL I INTRODUCTION BY COMMISSIONER PETER BROOKES

HEARING CO-CHAIR BROOKES: All right. Then with that, I'd like to introduce Panel I on Structure, Reforms and Capabilities of Chinese Intelligence Services. This panel will explore various actors in China's intelligence community, recent and ongoing reforms of Chinese intelligence services, and the capabilities of various intelligence services to conduct intelligence collection operations.

First, we'll hear from John Costello, a New America Congressional Innovation Fellow with the Republican staff of the House Oversight and Government Reform Information Technology Subcommittee. That's quite a title. Previously, Mr. Costello was an analyst at Defense Group Inc's Center for Intelligence Research and Analysis, where he researched Chinese defense and security issues.

As a member of the U.S. Navy and intelligence community, John established himself as a leading thinker in cyber warfare, emerging technologies and information dominance.

His current research focuses on understanding the future of warfare, the role of technology, and finding creative, iconoclast solutions to best prepare the United States for future conflict.

Next we have Mark Stokes. Mr. Stokes is the Executive Director of Project 2049 Institute. Previously, he was the founder and president of Quantum Pacific Enterprises, an international consulting firm, and vice president and Taiwan country manager for Raytheon International.

He has served as executive vice president of Laifu Trading Company, a subsidiary of Rehfeldt Group; a senior associate at the Center for Strategic and International Studies; a member of the Board of Governors of the American Chamber of Commerce in Taiwan.

A 20-year U.S. Air Force veteran, Mr. Stokes has served as team chief and senior country director for the People's Republic of China, Taiwan and Mongolia in the Office of the Assistant Secretary of Defense for International Security Affairs.

Finally, we have Peter Mattis. Mr. Mattis is a Fellow in the China Program at the Jamestown Foundation and a Ph.D. student in Politics and International Studies at the University of Cambridge. He edited Jamestown's biweekly China Brief from 2011 to 2013. Prior to the Jamestown Foundation, Mr. Mattis worked as an international affairs analyst for the U.S. government.

He also previously worked as a Research Associate at the National Bureau of Asian Research in its Strategic Asia and Northeast Asian Studies Program.

Welcome, all of you. Mr. Costello, if you'd like to start us off, we would appreciate it. Thank you.

**OPENING STATEMENT OF MR. JOHN COSTELLO
CONGRESSIONAL INNOVATION FELLOW, NEW AMERICA**

MR. COSTELLO: Thank you.

Commissioner Brookes, Senator Dorgan, and distinguished members of the Commission, I'm honored to testify on the structure, reforms and capabilities of the Chinese intelligence agencies. Thank you to the U.S.-China Economic and Security Review Commission for inviting me to testify today, and thank you for your interest in Chinese intelligence services. It's a topic that's not often discussed in open forum, but the importance of which grows daily.

In my testimony, I'll give a brief overview of the Chinese intelligence services and state and Party organs they answer to; a brief synopsis about what we know about tasking, command and control. The majority of my testimony will focus on implications of the recent military reforms on China's military intelligence services, their future capabilities, and areas where the United States is most vulnerable.

I should also note that the views and opinions expressed in this testimony do not represent the New America Foundation or the U.S. Committee on Oversight and Government Reform.

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.

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 U.S.'s particular vulnerabilities.

Now on to sort of the overview of the Chinese intelligence agencies. On the civilian side, China's intelligence agencies consist of the Ministry of State Security, or MSS, and the Ministry of Public Security, or MPS.

The MSS is primarily responsible for domestic counterintelligence, non-military foreign intelligence, and aspects of political and military security. Most notably, it's widely believed that they are either responsible for or the ultimate benefactor of the OPM data that was taken in 2014 and 2015.

The Ministry of Public Security is China's national police force responsible primarily for internal security missions and maintaining public peace and order and ensuring stability. However, due to its growing internal database, technical sophistication and cyber capabilities, it is having a more counterintelligence mission shared with the MSS.

On the military side, China has three major intelligence organs: the General Staff Department Second Department, responsible for general military intelligence, HUMINT, and overhead imagery; the Third Department, or Technical Department, is responsible for SIGINT and cyber espionage; and the Fourth Department, or Electronic Countermeasures and Radar Department, is responsible for elements of computer espionage and electronic intelligence, or ELINT.

Now, again--and this is important to keep in mind--China has no intelligence community equivalent like the sort we have in the United States. Understanding the coordination between their security and intel services is an extremely murky proposition. We just don't know enough to be able to reach any sort of conclusion about how Chinese intelligence

actors are tasked or who sets their priorities.

We can, however, discuss their chains of command. The Politburo Standing Committee governs civilian agencies through its Central Political Legal Affairs Commission, and the Central Military Commission governs the military intelligence organs through the previous General Staff Department, or what's now known as the Joint Staff Department, under the round of recent of military reforms.

That is about as much as we know as to these organs strict command and control. Now we do know that they do answer to certain leading small groups of foreign affairs and national security. They provide them with information. But the degree to which their tasking is governed by their we'll say their authorizing organs or the people that they provide information to is totally unclear.

And it might not even have a set institutionalized procedure. That said, I'll remove on to reforms. Xi Jinping announced a series of reforms in November, and we have steadily watched the CMC make what seems to be enormous and unprecedented changes to the way China's military has functioned for much of the last century.

The 2PLA, 3PLA, and Fourth PLA will all be shuffled and moved around. Their missions and administrative command will likely change substantially even if they stay in their current form at all. But based on the reforms we've seen so far, there are a few key developments that will substantially affect China's military intelligence.

One, creation of a Joint Staff Department, an actual true headquarters department for the PLA, is extremely significant when it comes to intelligence. It means that the Army's stranglehold over the PLA's intelligence apparatus will be lessened and China's substantial ISR capabilities may be opened up to missions that more need them such as the PLA Navy's growing maritime presence and space surveillance.

Secondly, the creation of the Strategic Support Force responsible for space, cyber, and electronic warfare, the functional equivalent to the United States Strategic Command, or STRATCOM, will centralize command and control of space ISR assets, allowing the CMC to shape them and leverage their use for more strategic priorities and more respondent to military operations.

Finally, China's cyber missions are seemingly to be centralized. Now this isn't, hasn't been said in open press by official sources, but semi-official sources or unofficial sources have indicated that China's cyber mission will be centralized, and what that means is whether the 3PLA, Fourth PLA cyber mission will be merged or taken away separately, or it will be transferred to the MSS, or just the opposite, the MSS cyber mission may be transferred to the military, is unclear. But it is an important factor to note when looking at the future of Chinese intelligence.

Based upon these 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 toward centralization and deconfliction in military intelligence will likely continue.

For the future, it's clear that Chinese intelligence will need to create a more robust and reliable collection infrastructure that is more respondent to policymaking and military operations.

Firstly, Chinese civilian and military agencies will likely continue to focus on "legitimate" intelligence targets that offer more relevant intelligence into U.S. policy, diplomacy and military operations.

Secondly, if China continues on the path of centrally coordinating its cyber espionage mission, which I expect it to do, it will go to what's called a more "Russian" model of cyber espionage, leveraging more long-term, long-term cyber intrusions rather than "smash and grab" tactics that we've seen in economically motivated cyber campaigns recently.

Finally, and most chillingly, China will marry its database of federal and military workers with real-time intelligence collected from other sources. While the OPM data itself isn't a--it's a good snapshot of federal workers; it isn't live; it can't change and grow and respond to military operations and policy and policymaking--it does provide a perfect targeting set for follow-on exploitation and a natural framework in which to correlate and evaluate new intelligence. And that is most likely how it will be used in the future.

Now, all of these sort of future trends speak to--and I'm keeping track of time here--will speak to the key vulnerabilities the United States has shown. Our contractors have been sort of the soft weak underbelly of the federal government. Keypoint Government Solutions credential was used through OPM. F-22 and F-35 plans were stolen from government contractors.

These are definitely a huge vulnerability regarding our cyber security, and I know Congress has done some things on the defense acquisition to strengthen cyber security requirements for contractors. It's sort of my hope that this will be extended to general contractors because defense contractors aren't the only ones who are contracting for the federal government.

Finally--and, again, I see I'm keeping track of time here--we are remarkably vulnerable to open source, especially if you look at the OPM data and you look at what's available online. Merging those two creates a nightmarish picture for military operations that can be tracked for policymaking that can be preempted or seen before it's even announced by the government and as a huge database of targets for follow-on cyber espionage and HUMINT targeting. Unsecured Facebook pages, Twitter and LinkedIn all can lead to these sorts of vulnerabilities.

So my recommendation to Congress in this regard is to include a lot of this stuff into background investigations and to have greater oversight over the military and federal agencies' OPSEC programs, not to control what people say online but to make sure that privacy and security controls for social media and network accounts are being followed appropriately.

And in the interest of time, that will conclude my testimony. Thank you.

**PREPARED STATEMENT OF MR. JOHN COSTELLO
CONGRESSIONAL INNOVATION FELLOW, NEW AMERICA**

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

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>

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 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 at 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 (NSA) 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 for joint airborne reconnaissance and intelligence in addition to managing a fleet of strategic

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#.Vej1rvlViko

¹¹ "Responses to Information Requests", *Immigration and Refugee Board of Canada*, Oct. 10, 2014, <https://www.justice.gc.ca/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

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 for computer network exploitation (CNE) and cyber espionage. Its 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 known. 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 electronic denial missions like satellite jamming. According to some analysts the 4PLA is capable of disrupting adversary communications, navigation, and synthetic aperture radar (SAR)

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 Kaoliang, Wen Xinyu, Huang Zhenyu, Gu Chuhui*, 1 May 2014, <https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf>

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

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

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

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

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 Groups²² 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, 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

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>

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 impending 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 more joint-force components better able to support the theater’s mandate of “focusing on fighting.”³²

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/>

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

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. Its 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 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

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

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. 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

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>

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>

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 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

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

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-osis-opm-breach/28977277/>

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 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.

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>

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>

**OPENING STATEMENT OF MR. MARK STOKES
EXECUTIVE DIRECTOR, PROJECT 2049 INSTITUTE**

MR. STOKES: Mr. Chairman, commissioners, I'd like to express my appreciation for the opportunity to come here and address one of my, one of my favorite topics. I was asked to discuss China's technical intelligence capabilities and their relevance for human resource intelligence collection, to include priorities and issues like that.

I divided up my written statement into three areas and then with conclusion of the relevance to HUMINT operations. But the three areas, basically it's ground-based, airborne, and then space-based.

For the purpose of in terms of outlining the relevance to human resource intelligence collection, I focus mostly on the ground-based ISR, which primarily is going to be an organization that John addressed, which is the, what used to be called the General Staff Department Technical Reconnaissance Department, or 3PLA for short, because that's probably the area that has the most relevance, direct relevance, to HUMINT operations.

China's ground-based ISR capabilities are significant and diverse. I say significant because don't exactly know how many people they have, for example, exactly how many English language, English intercept operators they have, for example, English-language-capable intercept operators. But it's expansive. Just to give you a sense, as I outlined in my written statement--I gave some examples--the 3PLA, as roughly analogous to U.S. National Security Agency, consists of 12 functional or operational bureaus, three research institutes that develop requirements for, let's say, for example, crypto material, requirements for hardware, requirements for computer software and things like this, and then a computing center. It's not exactly clear what this is, but it appears to be able to store the massive amounts of data that's collected through signals intelligence.

Signals intelligence, of course, includes communications intelligence, or COMINT, electronic intelligence, and then other esoteric issues, like MASINT, measurements and signature types of intelligence. So it's not just cyber. I consider cyber to be sort of communications intelligence, or an aspect of that, but with at least 12 operational bureaus. Let's give an example. The First Bureau. A bureau will consist of anywhere between eight and 12 subordinate offices or divisions. So we're looking at one bureau by itself is fairly large. The First Bureau is responsible for nothing but basically encryption and decryption, breaking and making codes, for, at least for the PLA itself or protecting their own classified information.

The most significant--one of the most significant bureaus is the Second Bureau headquartered in Shanghai. It became popular from New York Times and also the indictment of five officers that at one point in their career had an affiliation with the Second Bureau, or 61398 Unit. This particular bureau, based on research that I've done, isn't just cyber. It often is referred to as the Cyber Command, but my impression, this is mostly a traditional communications intelligence, HF, high frequency intercept, based upon at least just hints and indications of what, of subordinate units, of subordinate offices. It's not just based in Shanghai, but it has subordinate offices in other parts of China.

For example, an HF site up in, basically what's called, used to be called a elephant, "elephant cage," sort of HF, high frequency direction finding system. One in northeast, northeast China, one out in, one out in Sichuan, one down in Guangdong, in the southern part of China, very useful, for example, for getting a fix on U.S. naval operations, anything that--anybody that uses HF over-the-horizon communications.

And that's another bureau. The Third Bureau is another one. That tends to focus on, appears to focus on what's called "TEMPEST," basically electronic emissions that comes from their own computer systems.

Fourth Bureau, based up in Qingdao, and so on. They even have a bureau that's dedicated, appears to be dedicated toward nothing but intercepted telemetry and space launch types of communications.

So another bureau, 12th Bureau, also based in Shanghai, appears to be primarily responsible for intercept of satellite communications and also tracking of satellites, noncooperative satellite targets.

And this is just the 3PLA. Each military region, what used to be known as the military region, now theater command, has at least one technical reconnaissance bureau, or SIGINT organization, that appears to be primarily responsible for operations across borders that are directly relevant to the particular area.

So we're looking at a very expansive community. The PLA Navy has its own, has two technical reconnaissance bureaus. The PLA Air Force has three technical reconnaissance bureaus. So this is a very, very large organization.

Now just imagine this organization that, of course, they have to have set priorities. And so in terms of direct relevance to HUMINT operations, let's say, for example, you're going to set your priorities for key decision-makers, key senior policymakers. And not just them but also their social network. Basically whoever is able to influence them. Bear in mind that HUMINT--and Peter is going to address this in a lot more detail--HUMINT is more--isn't necessarily what we would consider it, but it also includes influence operations, basically being able to affect perceptions of senior leaderships, senior policymakers, and to be able to influence not just how they view the world, but influence policies directly.

And if you're able to, if you're able to affect what could be referred to as a global digital electronic fishbowl, if you're able to get basically every single electronic movement that an individual makes, that a policymaker makes, and that his circle makes, naturally that enables you to be able to influence not that individual directly but at least through other areas because people still are going to communicate, whether it's making a phone call on your cell phone or emails or whatever is on your files. It's a significant, it provides significant advantages to those who are able to get, basically be able to track an individual and what they do.

As one example, the Second Bureau, based in Shanghai, allegedly, for example,--just using Taiwan as an example--supposedly, at least according to some references, the Second Bureau targets every military officer on Taiwan that has a rank of colonel and above. It's updated every two weeks. Bear in mind that Taiwan's location allows a lot more collection to be done by what used to be the Nanjing Military Region Second Technical Reconnaissance Bureau. There's other reconnaissance bureaus that are able to do the same thing for northern India, for example, on the Tibet border, along the border with Burma. This would be the Chengdu Military Region Second Technical Reconnaissance Bureau. So this is a significant organization.

There are other parts of their technical intelligence community. For example, space, and John addressed the, in his written statement addressed some of the space capabilities that have been resubordinated to the new Strategic Support Force.

You also have airborne. The PLA Air Force, of course, operates, in their Technical Reconnaissance Bureau operates their own assets. And the space, of course, you're looking at imagery, both electro-optical imagery, synthetic aperture radar. The electronic intelligence basically track the signatures of U.S. aircraft carrier and other, basically U.S. naval

activity in the region as well as activities of other partners and allies in the region.

So, all in all, we're looking at a very significant technical intelligence capability that has relevance to their HUMINT operations.

So with that, I'll turn it over to Peter.

**PREPARED STATEMENT OF MR. MARK STOKES
EXECUTIVE DIRECTOR, PROJECT 2049 INSTITUTE**

**Prepared Statement of
Mark A. Stokes
Executive Director
Project 2049 Institute
Before
The U.S.-China Economic and Security Review Commission**

Hearing on Chinese Intelligence Services and Espionage Operations

**Thursday, June 9, 2016
Room 285, Hall of States
444 North Capitol Street NW, Washington, D.C. 20001**

Mr. Chairman, thank you for the opportunity to participate in today's hearing on an issue that is important to U.S. interests in peace and stability in the Asia-Pacific region. It is an honor to testify here today. The evolving capacity of the People's Republic of China (PRC) to leverage technical intelligence collection assets presents a number of challenges for the United States, allies, and friends in the Asia-Pacific region. In my presentation this morning, I will address PRC technical intelligence that enables or supports human intelligence (HUMINT) operations.

The People's Liberation Army (PLA) is rapidly advancing its technical intelligence, surveillance, and reconnaissance (ISR) capabilities. In doing so, the PLA advances the legitimacy of the Chinese Communist Party (CCP), and defends against perceived threats to national sovereignty and territorial integrity. PLA ISR assets support party and state interests, including military operations in the land, maritime, and space domains. For purposes of strategic, operational, and tactical awareness, the PRC is engaged in the research and development (R&D) and acquisition of space-based, airborne, and surface-based sensors that support human intelligence and clandestine influence operations. ISR assets also enable monitoring of military activities in the Western Pacific and beyond.

Ground-Based ISR. The PRC's ground-based signals intelligence (SIGINT, or technical reconnaissance in Chinese lexicon) system is significant and diverse. Before the most recent military reorganization that commenced in late 2015/early 2016, the PLA's SIGINT community consisted of at least 28 technical reconnaissance bureaus (TRBs), each roughly equal in grade to a PLA Army division. The GSD Technical Reconnaissance Department, often referred to as 3PLA, had direct authority over 12 functional bureaus, three research institutes, and a computing center. Each bureau, along with subordinate offices, appeared to have a unique individual missions. Missions presumably include intercept of communication transmissions throughout the frequency spectrum. At least one bureau appeared to exploit satellite communications, while others likely tap in to fiber optic communications. No single 3PLA unit appeared to have a monopoly on cyber espionage, or the collection of data contained within foreign computer

networks. While the on-going military reforms likely have affected the PRC's SIGINT organization, the basic missions of individual bureaus and offices probably have remained intact.

Eight of the 12 operational bureau-level headquarters were clustered in Beijing. Two others were based in Shanghai, one in Qingdao, and one in Wuhan. For illustrative purposes, the Third Department First Bureau may have played an important role in breaking advanced encryption systems and other computer network operations. The First Bureau headquarters reportedly oversaw at least 12 offices operating in various parts of China.

As another example, the Second Bureau (Unit 61398) was one of the largest among the 12 operational bureaus that comprised 3PLA. The unit consisted of at least 12 subordinate offices and work stations garrisoned in the greater Shanghai area and other parts of China. Among these include work stations positioned near major submarine cable landing stations within Shanghai City that handle a significant volume of communications entering and leaving China. Officers assigned to the Second Bureau have allegedly engaged in cyber espionage. The bureau's network may also have included at least three high frequency direction finding (HF/DF) sites in northeast, southwest, and southern China. Through the geolocation of HF transmissions, the system may be intended to monitor, interfere, or block signals unfavorable to the CCP's goals. Potential collection targets may also include U.S. Air Force and Navy HF beyond line-of-sight communications. Civilian networks of interest may include international air traffic control managed by the International Civil Aviation Organization (ICAO), maritime safety, Radio Free Asia, and other networks.

As a final example, the Third Department 12th Bureau, headquartered in Shanghai, appeared to support space surveillance and intercept of satellite communications. Personnel from the bureau may intercept uplinked and/or downlinked electronic transmissions between satellites and transmitters on the surface. Another mission may be surveillance, identification, and tracking of satellites and other space vehicles. Passive space tracking involves the use of antenna systems on the ground that can locate with precision the source and characteristics of signal and associated transmitter. Detection of a signal may cue other space surveillance assets. Although unclear at the current time, the 12th Bureau could be resubordinated to the newly established Strategic Support Force. A separate bureau appeared to specialize in intercept of telemetry data associated with missile tests and space launch operations.

Before January 2016, each of the PLA's seven Military Regions also exercised authority over at least one technical reconnaissance bureau (TRB). The mission of a Military Region TRB, which consisted of between eight and 12 subordinate offices and work stations, likely included border and coastal defense. For example, the Guangzhou Military Region TRB probably focused on communication networks associated with maritime activity in the South China Sea. The Nanjing Military Region's First TRB, headquartered in Nanjing, presumably supports coastal defense operations in the East China Sea, while the region's Second TRB, headquartered in Fuzhou, was concentrated on communications networks on Taiwan. The Chengdu Military Region First TRB may have targeted Indian communication networks along the border with China. Chengdu's Second TRB may have concentrated efforts on communication networks along the border with Burma. Military Region TRBs likely have been resubordinated to newly established Theater Commands.

The PLA Navy (PLAN) oversees two TRBs that probably target foreign navies operating in the Western Pacific Ocean. PLAN TRBs presumably leverage ship-based technical reconnaissance collection assets. The PLA Air Force (PLAAF) leadership is supported by three TRBs that appear to target foreign air defense and surveillance communication networks in the region. In addition to operating ground-based SIGINT facilities, PLAAF TRB personnel presumably support peacetime aerial reconnaissance flights within the Asia-Pacific region.

Regional SIGINT assets are likely augmented by ground-based electronic and air surveillance radar networks. MRs (Theater Commands) likely oversee organic electronic intelligence systems that support border and coastal defense, among other missions. For example, a Guangzhou MR radar reconnaissance unit has been noted tracking U.S. Navy radar activity in the South China Sea. The PLA Navy's South Sea Fleet's Observation and Communications Brigade manages more than 20 electronic surveillance sites across three provinces in southern China, including one on Subi Reef.

In addition to SIGINT collection assets, the PLA has made significant advances in its joint air surveillance system. In the past, the PLAAF and PLAN appeared to divide air defense responsibilities, with the Navy responsible for defense of major naval bases (eg., East and South Sea Fleet homeports). Since at least 2006, authoritative media outlets have indicated that the PLAAF has been granted responsibility for developing and fielding a new automated joint air surveillance system. The system relies on a network of sensors that provides data to centralized air command and control centers. The PLA also operates over the horizon (OTH) radar systems capable of tracking air and surface targets at extended ranges. OTH systems, which have both military and civilian applications, support China's scientific community, including atmospheric and oceanic studies.

Space-Based ISR. Increasingly greater spatial resolution and an ability to monitor U.S. activity in the Asia-Pacific region (including the locations of US aircraft carrier battle groups) in all weather conditions are likely to enhance China's capacity for power projection. Over the years, the PLA and civilian defense industry have fielded electro-optical (EO), synthetic aperture radar (SAR), electronic intelligence (ELINT), and other space-based sensor platforms that can transmit images of the earth's surface and emitter data to ground stations in near-real time.

Since at least 2006, the PLA and China's defense R&D community have been developing and fielding a dedicated military EO satellite system with increasingly high resolution. China is expected to have multiple types of space-based SAR systems on orbit over the coming years that cater to various users. SAR satellites use a microwave transmission to create an image of maritime and ground based targets. They can operate night or day and in all weather conditions, and are therefore well suited for detection of ships over a wide area. Processed SAR imagery may depict a ship in various ways, depending on weather conditions, ship orientation and construction, and beam focus. A SAR satellite is also able to image ship wakes from which information on ship speed and heading can be deduced.

Chinese military analysts view space-based electronic reconnaissance as necessary to accurately track and target U.S. carrier strike groups in near real time from lower earth orbit as part of

China's long-range precision strike capability, including its anti-ship ballistic missile (ASBM) system. Major surface vessels, such as aircraft carriers, have prominent electromagnetic, acoustic, and infrared signatures and large radar cross section. Although controlling emissions from carriers is feasible for limited periods of time, air operations depend on electromagnetic radiation.

The newly created PLA Strategic Support Force most likely drives requirements and leverages the data produced by space-based sensors. Space assets enable the monitoring of naval activities in surrounding waters and the tracking of air force deployments into the region. A constellation of small SAR and ELINT satellites could provide commanders with geolocation data on mobile targets. In a crisis situation, China may have the option of augmenting existing space-based assets with microsatellites launched on solid-fueled launch vehicles. Increasingly sophisticated satellite communications also offer a survivable means of linking sensors to strike systems, and will become particularly relevant as PLA interests expand further from Chinese shores. Existing and future data relay satellites could transmit targeting data to and from command centers.

Airborne ISR. Airborne ISR assets include manned ISR platforms and an increasingly advanced and diverse range of unmanned aerial vehicles (UAVs). Operated by the Central Military Commission (CMC) Joint Staff Department, PLAN, PLAAF, and other PLA organs, conventional high altitude, long endurance UAVs are said to employ EO, SAR, and electronic reconnaissance sensor packages. The PLA also appears to be investing in the R&D of “near space” flight vehicles, operating at altitudes between 20 and 100 kilometers, and equipped with a range of sensors.

Support to National Leaders and HUMINT Community. The PRC's ability to coordinate military and civilian intelligence disciplines is unknown. At the national level, technical intelligence and HUMINT communities likely suffer a similar type of stovepiping that exists in other countries. The PRC's policymaking, technical intelligence, and HUMINT communities probably have a symbiotic relationship. In particular, the PLA's SIGINT community presumably provides direct support to senior policymakers and HUMINT community, including the Ministry of State Security (MSS), CMC Joint Staff Department Intelligence Bureau, and the CMC Political Work Department Liaison Bureau. The structure and process for intelligence tasking is also unclear. However, intelligence collection priorities of the Politburo Standing Committee are likely coordinated by the CCP Secretariat and Central General Office, CMC General Office, and State Council General Office. At the national level, priorities may range from perceived challenges to sovereignty and territorial integrity, to political and economic negotiations.

At the local level, technical and HUMINT communities may have formal or informal mutual support arrangements. For example, PLA technical reconnaissance assets in Shanghai could provide communications intelligence support to local MSS and PLA HUMINT operations. The capacity to intercept email exchanges, computer files, cell phone calls, and text messages of targets of interest in the U.S., Taiwan, and elsewhere may facilitate assessment of individuals—both military and civilian—with access and influence for political purposes. At the operational level, however, the PLA has invested heavily in R&D and deployment of a system, the Integrated Command Platform, which appears capable of correlating or fusing sensor data within intelligence information centers at the national and regional levels.

The effectiveness of China's technical reconnaissance, including cyber espionage, is unknown. However, the organization and engineers responsible for R&D and acquisition of technical intelligence systems appear sophisticated and capable of meeting future requirements. Exploiting vulnerabilities in international communications systems and computer networks, the PRC's creation of a global digital electronic fishbowl would have significant implications for U.S. national security interests and warrants further study.

**OPENING STATEMENT OF MR. PETER MATTIS
FELLOW, JAMESTOWN FOUNDATION**

MR. MATTIS: Thank you to Senator Dorgan and Commissioner Brookes and the rest of the Commission for inviting me here to speak. It's a subject that has been near and dear to my heart for quite some time, and when I left the U.S. government, I was told by some of the people on the security side of things that "good luck, good writing, don't make us come find you."

[Laughter.]

MR. MATTIS: Because in the absence of information, all we're going to get is hyperbole, and there are reasons to think that the Chinese have struggled in the HUMINT realm for quite some time, and if we treat them as hyperbole, we allow those views to be dismissed, and it's at a time when I believe that the Chinese intelligence services are regaining their past sophistication and are on the cusp of some major changes in terms of building their HUMINT capabilities.

For many years, China's HUMINT ops against the United States were deemed a threat at the level of say the Russians, not because they demonstrated the same kind of operational sophistication that the KGB's First Chief Directorate or that the SVR had demonstrated, but simply the scope, scale and potential impact of Chinese intelligence operations was such that they, it would have a serious impact on U.S. national security interests.

But as China's global interests have expanded, the intelligence services are trying to catch up and are trying to support those interests. This leads to the important point that the conventional view of Chinese human intelligence operations, whether you've heard it as the "mosaic" or the "grains of sand," is simply wrong. It was never right in the first place; it's not a product of any particular time. It's simply wrong.

Intelligence is a very specific subset of information in the Chinese system. It is information, in the words of a U.S. trained scientist, Qian Xuesen, who was the father of the rocket program and one of the fathers of the scientific and technical information collection system, which is a completely different professional system than I'll be talking about today, is information that resolves specific decision-making problems.

It's information that resolves specific decision-making problems, not just sort of information that supports national security interests, but that is tailored to decisions in a much stronger way than we tailor it in our say Executive Order 12333.

Second, the Chinese Communist Party has considered intelligence to be a professional's game since 1927 when they created their first intelligence service. It is not left up to the amateurs. It has been professional from nearly the entire history of its existence.

They've employed clandestine tradecraft. They use negative incentives like coercion, blackmail, and they were trained by the Soviets in the 1930s after the end of the Long March. The Soviet expertise in running clandestine HUMINT filtered into how the Chinese were training their case officers. Luckily, they killed off a lot of those people in the political upheavals of the early days of the People's Republic and the Cultural Revolution.

The traditional methods of HUMINT apply, and this includes using diplomats, using journalists, using defense attaches, academics, both in terms of providing clandestine or cover for clandestine operations, as well as for open source collection, and efforts to recruit sort of young people or mid-career people who will then apply and go into U.S. national security agencies.

And this has been an area that the United States has been effective in preventing,

at least for the last 30 years or so, and including with the arrest of the young man named Glenn Duffie Shriver in June 2010.

China does not need to recruit agents with direct access. They're actually comfortable in many cases recruiting people with a broad degree of second-hand access. So a friend of mine who was pitched by Chinese intelligence had a think tank affiliation in D.C., and his value was in, at least as it was described to him, was being able to write reports about U.S.-China relations or U.S. policy toward China because of a broad range of contacts that he could reach out and touch and speak to.

Most recruitments that we've seen have occurred inside China. So it's not a traditional case officer recruitment that many services use worldwide outside of the target country, but they exploit people who are traveling in and out of China for business, for study, and then those people sort of go back to their home countries and either try to find work in the national security system or try to sort of hustle their connections, like a Louisiana furniture salesman named Kuo Tai-Shen, who recruited two Department of Defense employees to work for Chinese intelligence.

If there's anything to describe the operational evolution of Chinese intelligence in the last 15 years, it's simply aggressiveness and the need to get results. When you put money on the table, you expect results. And there have been a number of cases of direct pitches to Americans that have been delivered within one, one to two or three meetings with Chinese intelligence. And money is literally put on the table as part of the offer. This is not this view that they take years to develop sources. It's much more common now to simply say this is what we want; here's what we're willing to pay; will you provide it?

The operational restrictions that were placed on the Ministry of State Security in 1985 have clearly been lifted that prevented them from operating overseas as aggressively as they might. And it's only been in the last 15 years that we've seen the reemergence of Chinese espionage cases that have been conducted entirely outside China. Taiwanese General Lo Hsien-che and a Uighur in Sweden named Baibur Maihesuti. These are the only two cases that we know of, and I've got a personal database of 60 or 70, that have been conducted entirely outside of China.

As to the effectiveness of Chinese intelligence, when you operate with a domestic focus this way of picking people who are coming to China, you may learn a lot about other countries' interactions and policy toward China, but it creates blindspots that if you've got a growing stake in the Middle East, U.S. policy is a significant factor, but U.S. Middle East specialists don't go to China and spend a year or two or make regular trips that allow them to be accessed.

And so because of these kinds of stakes, Chinese intelligence is in the position where they need to go abroad. They need to push out like much of the rest of the Chinese system to try to find sources that will meet the intelligence requirements of the leadership.

If there are particular vulnerabilities that are worth highlighting that the United States has, it's that a lot of young Americans going abroad who will come into the national security system, such as the Boren Fellowship recipients in the National Security Education Program, you know, we publicly highlight that these people are required to take a national security job, and yet they're going abroad without preparation of what they should look out for, the things that they should do to ensure that people can keep track of them, that they're able to fill out an SF-86 appropriately when they come back, and have verifiable things that we can look to.

Some of the other places where we've had, where the U.S. and other countries have had, trouble is with retirees and through third-country vulnerabilities. The U.S. alliance system is an incredibly valuable policy tool, but it also creates vulnerabilities, and there's clearly a lower threshold for people to betray a third country than to betray their own. It's one thing to say be a Japanese official who betrays the Japanese government specifically than it is to say perhaps give up U.S. government information.

As far as how effective the United States has been at dealing with them, I don't think you can put a clear judgment on the basis of open sources. If you're not in the community and you're not active in it, and you don't have a broad view across what the community is doing, it's very difficult to say.

Suffice it to say there simply isn't enough knowledge publicly to have a robust and ongoing discussion of Chinese intelligence and its threat to U.S. interests. I'll leave it there.

**PREPARED STATEMENT OF MR. PETER MATTIS
FELLOW, JAMESTOWN FOUNDATION**

**Testimony before the U.S.-China Economic and Security Review Commission:
Chinese Human Intelligence Operations against the United States**

*Peter Mattis
Fellow, The Jamestown Foundation
June 9, 2016*

China's intelligence services are among the world's most active against the United States, but the Chinese approach to human intelligence (HUMINT) remains misunderstood. Observers have conflated the operations of the intelligence services with the amateur clandestine collectors (but professional scientists/engineers/businesspeople) who collect foreign science and technology. The Chinese intelligence services have a long professional history, dating nearly to the dawn of the Chinese Communist Party, and intelligence has long been the province of professionals. The intelligence services were not immune to the political purges and the red vs. expert debates, and the Cultural Revolution destroyed much of the expertise in clandestine agent operations.¹ As China's interests abroad have grown and the blind spots created by the country's domestic-based intelligence posture have become more acute, the Chinese intelligence services are evolving operationally and becoming more aggressive in pursuit of higher-quality intelligence.

* * *

The principal intelligence services conducting HUMINT operations, both clandestine and overt, against the United States are the Ministry of State Security (MSS) and Joint Staff Department's Intelligence Bureau (JSD/IB) in the People's Liberation Army (PLA). Prior to the military reforms announced in November 2015, the latter was known as the General Staff Department's Second Department (commonly abbreviated 2PLA). Because the full ramifications of the PLA's reform effort have unclear implications for intelligence, the testimony below will reflect what was known about 2PLA rather than the JSD/IB, unless specifically noted.

The MSS consists of the central ministry, provincial state security departments, and municipal/county state security bureaus. At least the central ministry and the provincial departments conduct clandestine agent operations, though only a few provincial departments are routinely active in collecting on the United States. The others exploit targets of opportunities passing through their jurisdictions and occasionally pursue them outside of their ostensible turf.

The 2PLA conducted both clandestine and overt HUMINT operations through case officers operating under traditional covers and defense attaché offices, respectively. The clandestine collectors operate from liaison offices in China, official missions overseas, and non-official cover platforms abroad. It is believed that there are five liaison offices in Beijing, Shanghai, Shenyang, Guangzhou, and Tianjin, which as the principal stations for 2PLA's clandestine agent

¹ David Ian Chambers, "Edging in from the Cold: The Past and Present State of Chinese Intelligence Historiography," *Studies in Intelligence*, Vol. 56, No. 3 (September 2012), pp. 31-46.

operations.²

Chinese HUMINT operations use case officers as well as other collectors operating under a wide variety of covers and different operational modes to collect intelligence both overtly and clandestinely. Here are five well-documented ways in which Chinese intelligence, both civilian and military, collect intelligence.³

- Diplomats, defense attachés, and journalists form the cadre of embassy-based case officers under official cover. Mostly these collectors pursue internal security targets (which may not be scrutinized by local counterintelligence/security services), interviews commensurate with their cover, and other open source information. Only recently have these officers appeared to engage in clandestine agent operations.
- Seeding operations involve recruiting an individual and then trying to direct them into positions where they can collect valuable intelligence. These kind of operations originated in the Chinese Revolution and have remained a staple approach with a very mixed record of success.⁴
- Academics and scholars have been familiar feature of China's public face for intelligence, through such august organizations as the MSS bureau known as the China Institutes of Contemporary International Relations. For the most part these organizations do nothing more nefarious than open source collection and elicitation through interviews. Occasionally, however, case officers covered as academics have run clandestine agent operations.
- Domestically, local government offices, such as numbered but otherwise anonymous municipal offices (e.g. the Shanghai Municipal Government Office No. 7), are frequently used to create a fig leaf between intelligence officers and those with whom they are in contact.
- Business people at home and abroad also are used as case officers, collaborators, and principal agents who develop spy networks themselves.

Other Chinese bureaucracies are involved in covert action, such as political influence, and intelligence, such as monitoring ethnic Chinese and minorities; however, their role in targeting the U.S. Government directly is limited. These include the Ministry of Public Security, Liaison Department of the PLA's Political Work Department, the party's United Front Work Department, and the Overseas Chinese Affairs Office. Though these organizations and others do represent a threat to U.S. interests, their activities are beyond the scope of this testimony and require a different kind of discussion.

Similarly, the largest portion of China's efforts to acquire foreign scientific and technological information is not run from the intelligence services, but a specialized bureaucracy for cataloguing and disseminating technical information.

² Kan Zhongguo, "Intelligence Agencies Exist in Great Numbers, Spies Are Present Everywhere; China's Major Intelligence Departments Fully Exposed." *Chien Shao* (Hong Kong), January 1, 2006.

³ For a lengthier treatment, see, Peter Mattis, "Five Ways China Spies," *The National Interest*, March 6, 2014.

⁴ "Shriver Case Highlights Traditional Chinese Espionage," *Jamestown Foundation China Brief*, Vol. 10, No. 22, November 5, 2010

Ultimately, the activities of the intelligence services are governed by the Politburo Standing Committee and the Central Military Commission. Beneath these two bodies, the Political-Legal Affairs Commission system and the Joint Staff Department have direct responsibilities for the intelligence services. The Minister of State Security and the JSD deputy chief with responsibility for intelligence and foreign affairs both sit on the relevant leading small groups, including, at least, foreign affairs, Hong Kong & Macao affairs, Taiwan affairs, countering evil cults, and preserving stability. While the intelligence services may only provide information to these groups, presumably they receive guidance about important intelligence requirements when these bodies deliberate. The State Security Committee (sometimes referred to as China's National Security Council) also may oversee intelligence operations; however, the membership and functioning remains mostly unknown and its focus may be more on protecting the party-state than guiding foreign and national security policy.⁵

What Do the Chinese Mean by Intelligence?

Most writing about Chinese intelligence suggests the Chinese conduct intelligence in a completely different way while avoiding traditional methods of clandestine agent operations. Variouslly called the “grains of sand,” “mosaic,” or “vacuum-cleaner” approach to intelligence, the conventional perspective holds that Chinese intelligence relies on amateur collectors with little clandestine tradecraft, does not exploit negative vulnerabilities like venality, and collect little bits of information that can be assembled later in China. This view fails in the face of Chinese intelligence history, concepts, and practices beginning from the beginning of CCP intelligence in 1927.⁶

One of basic mistakes foreign analysts have made about the Chinese is to say that the Chinese make no meaningful distinction between intelligence and information, leading to broad-based collection of information almost irrespective of specific intelligence requirements. Former FBI Special Agent I.C. Smith and intelligence historian Nigel West wrote “In the Chinese language, there is no real distinction between ‘intelligence’ and ‘information’ in common usage, and there is no specific term for ‘intelligence-gathering.’ *Qingbaosou* refers to ‘information-gathering,’ an essential ingredient of the mammoth intelligence gathering effort directed at Western countries.”⁷ From a purely academic perspective, two British intelligence scholars stated “traditionally, the Chinese vocabulary has not distinguished between ‘intelligence’ and ‘information.’ Accordingly, China’s agencies operate different than other espionage organizations by collecting large quantities of open information.”⁸

At least since the early 20th Century, the Chinese have defined intelligence in ways recognizable in Western terms. The common element is information serving a specific purpose and in support

⁵ David M. Lampton, “Xi Jinping and the National Security Commission: Policy Coordination and Political Power,” *Journal of Contemporary China*, Vol. 24, No. 95 (2015), 759–777; Samantha Hoffman and Peter Mattis, “Inside China’s New Security Council,” *The National Interest*, November 21, 2013.

⁶ For a full accounting of these problems, see, William Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (New York: Routledge, 2013), 186–216; Peter Mattis, “Assessing Western Perspectives on Chinese Intelligence,” *International Journal of Intelligence and Counterintelligence*, Vol. 25, No. 4 (Fall 2012), 678–699.

⁷ I.C. Smith and Nigel West, *Historical Dictionary of Chinese Intelligence* (Lanham, MD: The Scarecrow Press, 2012), 220.

⁸ Richard J. Aldrich and John Kasuku, “Escaping from American Intelligence: Culture, Ethnocentrism, and the Anglosphere,” *International Affairs*, Vol. 88, No. 5 (September 2012), 1020.

of decisionmaking. One of the most commonly used Chinese definitions of intelligence comes from the U.S.-trained rocket scientist Qian Xuesen, who also played an important role in systematizing the collection of foreign scientific knowledge. Dr. Qian stated “Intelligence is the knowledge necessary to solve a specific [decision-making] problem. This view embodies two concepts. One is that [intelligence] is knowledge, not false, nor random. And the other? It is for a specific requirement and also for a specific question, so timeliness and relevance are very important ...”⁹ Numerous PLA publications and intelligence histories reinforce the view that intelligence is specially-collected, -processed, -analyzed, and -disseminated information for policymakers and other decision makers.

Intelligence also is a form of clandestine or covert power. The inclusion of intelligence warfare as one of the four components of information warfare—the other three are network warfare, electromagnetic warfare, and political/psychological warfare—is rooted in China’s strategic tradition dating back to the *Sunzi Bingfa*.¹⁰

China’s Evolving Approach to HUMINT

The best word to describe China’s changing approach to intelligence collection in the last fifteen years is aggressiveness. Elements of this aggressiveness have risen and then faded, such as the very direct use of sexual entrapment and blackmail.¹¹ Other parts of this aggressiveness remain. As China’s intelligence services have demonstrated greater willingness to pay human agents, they have become impatient for results. Most analyses of Chinese tradecraft suggested they used long development phases and may never have reached the stage for formal recruitment. Based on this analyst’s interviews with individuals and foreign intelligence services, the Chinese are perfectly willing to pitch a potential source within one to three meetings including an initial spot payment and promise of future remuneration.

Perhaps the most notable specific development has been the recruitment of clandestine agents abroad by case officers posted outside China. The first example is Taiwan army general Lo Hsien-che, who the Taiwanese authorities arrested in early 2011. Chinese intelligence, probably 2PLA, recruited Lo sometime during his posting as a military attaché in Bangkok in the early 2000s. There is nothing in the public record to suggest General Lo was ever handled at meetings taking place inside China, and his primary case officer (though not the necessarily the one who recruited him) was covered as a Thailand-based businesswoman with legitimate Australian citizenship.¹² The second example is Baibur Maihesuti, a Uighur living in Sweden and who the Swedish authorities arrested in 2009 for spying on fellow Uighurs living outside China. Chinese intelligence, most likely the MSS, used two case officers: one covered as a journalist for an

⁹ Chen Jiugeng, “Guanyu qingbao he xinxi [Regarding Intelligence and Information],” *Qingbao zazhi* (Journal of Information) 19, No. 1 (January 2000), 4–6.

¹⁰ Ralph Sawyer, “Subversive Information: The Historical Thrust of Chinese Intelligence”, in Philip H.J. Davies and Kristian Gustafson, eds., *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere* (Washington, DC: Georgetown University Press, 2012), 29–48.

¹¹ This culminated in the suicide in 2006 of a Japanese code clerk posted at the Shanghai Consulate. See, Justin McCurry, “Japan Says Diplomat’s Suicide Followed Blackmail by China,” *The Guardian*, December 20, 2005; Reiji Yoshida, “China Slammed Over Diplomat’s Suicide,” *Japan Times Online*, December 29, 2005.

¹² Peter Mattis, “Taiwan Espionage Cases Highlight Changes in Chinese Intelligence Operations,” *Jamestown Foundation China Brief*, Vol. 11, No. 12, July 1, 2011.

official Chinese paper and that other covered as a diplomat in the embassy.¹³

It is possible, if not probable, that Chinese intelligence recruited agents in ethnic Chinese overseas communities, Chinese ethnic minorities, and Taiwanese, but U.S. and other local counterintelligence services did not focus on such activities. In democracies, such activities may not even necessarily break the law. China's intelligence services first and foremost have a responsibility for the protecting the party-state and this is why what some analysts have called "ethnic targeting" occurred. But as China's global interests beyond state security have expanded, Chinese intelligence must shift its operational footing to protect sources who receive a higher degree of scrutiny and accept a greater risk to their careers and livelihoods. A government official, contractor, or interlocutor often needs clandestine tradecraft as reassurance that a foreign intelligence service for whom they spy can take care of them. The pressure to support decisionmakers should be moving Chinese intelligence, both 2PLA and MSS, toward more sophisticated clandestine tradecraft, including such techniques as covert communications, overseas surveillance teams, using agents to enable access to closed networks or provide other technical collection, etc.

The publicly-available data on military intelligence and MSS operations is insufficient to judge the distinctions, if any, between the two sets of intelligence services. Both seem to use more than one intelligence officer whenever handling a source, and both rely heavily on operations conducted inside China. The domestic base for operations often means that what counterintelligence officials see are principle agents, not professional intelligence officers, trying to operate and find sources overseas. It can look amateurish because it is, and the truly professional relationship often remains hidden from view unless a principle agent decides to cooperate after his arrest.

The distinctions between the U.S. and Chinese approaches to HUMINT probably are questions of specific techniques and comfort operating overseas. There is no recorded example of the Chinese using a dead drop, i.e. leaving messages, money, or other items in specific place to pass between case officer and agent. However, the Chinese have used live drops, i.e. a signal is sent to trigger a meeting where items are passed between officer and agent. The number of examples of the Chinese identifying and recruiting an agent outside China are few and relatively recent, suggesting that conducting clandestine agent operations abroad remains tightly controlled.¹⁴

Chinese HUMINT in Three Cases

The U.S. espionage cases centered around Larry Wu-Tai Chin, Kuo Tai-Shen, and Glenn Duffie Shriver offer a window into the conduct of Chinese clandestine agent operations. They demonstrate China's capability and highlight the Chinese use of the traditional tools of espionage that are shared among most of the world's intelligence services involved in the HUMINT business.

¹³ Paul O'Mahony, "Pensioner Indicted over China Spy Scandal," *The Local* (Sweden), December 15, 2009; "Refugee Spy Remanded into Custody," *The Local* (Sweden), 6 June 2009; Paul O'Mahony, "Security Police Arrest 'Refugee Spy'" *The Local* (Sweden), June 4, 2009; "Sweden Jails Uighur Chinese Man for Spying," *Reuters*, March 8, 2010.

¹⁴ Peter Mattis, "The New Normal: China's Risky Intelligence Operations," *The National Interest*, July 6, 2015.

Larry Wu-Tai Chin was recruited by Chinese intelligence while he was working for the U.S. mission in Nanjing prior to the formation of the PRC in 1949. Chin continued to report to Chinese intelligence for almost forty years until his arrest in 1985. For most of this time, he worked as a translator in various capacities, such as for the U.S. Army in Korea helping with prisoner interrogation and later at the Foreign Broadcast Information Service. Chinese intelligence may have paid him over a \$1 million. Throughout the operation, Chin made several surreptitious trips into China for meetings and to be recognized for his reporting. When Chin was ready to pass documents onward, he would mail a letter to an accommodation address in Hong Kong and that would signal a follow on meeting at a preset time in Canada, where he would pass the documents to a courier.¹⁵

Kuo Tai-Shen was a naturalized U.S. citizen and Louisiana-based furniture salesman who was recruited in the 1990s during one of his frequent business trips to mainland China. Although Kuo had access to some political circles in Taiwan through his marriage, he had no direct access to U.S. Government information. His handlers in 2PLA encouraged to develop contacts in the U.S. Department of Defense, and he successfully recruited James Fondren and Gregg Bergersen to spy for China. Fondren was a retired military officer who returned to work for the U.S. Pacific Command office in Washington, DC, after working as a consultant whose primary client was Kuo for whom he wrote assessments of U.S. policy. Bergersen worked for the Defense Security Cooperation Agency, and he provided classified information to Kuo on U.S. arms sales to Taiwan thinking that Kuo worked for Taipei. Kuo persuaded Bergersen that they should set up an arms export business once he retired to sell military-related components to Taiwan. 2PLA met Kuo exclusively inside China, but did provide him with courier and tried to teach him how to communicate discreetly via email.¹⁶

Glenn Duffie Shriver was a recent university graduate in China when he was spotted by Chinese intelligence, probably the MSS, through an essay contest on U.S.-China relations. The contest was a gimmick intended to draw out individuals who might have long-term intelligence value to Chinese intelligence. Shriver met several times with a younger case officer and at least one or two others. He was arrested in Summer 2010 on his third attempt to join the U.S. national security establishment, this time at the Central Intelligence Agency. He had applied twice previously to the U.S. Department of State, but failed to pass the foreign service examination with sufficiently high marks. For his attempts to join, Shriver was \$70,000. Shriver never met Chinese intelligence officers outside of China, and he used only email rather than any special equipment for communication.¹⁷

These cases highlight a few points of Chinese tradecraft that are worth noting. First, the agents

¹⁵ Ronald Ostrow, "Accused Spy Chin Faces New Charges," *Los Angeles Times*, January 3, 1986; Chitra Ragavan, "A Spy Who Changed History," *U.S. News and World Report*, November 20, 2003; Nicholas Eftimiades, *Chinese Intelligence Operations* (Annapolis, MD: Naval Institute Press, 1994), 32–34; Bill Gertz, "Former FBI Agent Cites Penetration of CIA by China," *Washington Times*, December 15, 2004.

¹⁶ "Defense Department Official Charged with Espionage Conspiracy," Department of Justice Press Release, May 13, 2009; Jerry Markon and Carrie Johnson, "Former Pentagon Official Pleads Guilty to Espionage," *Washington Post*, April 1, 2008; and *United States v. Tai Shen Kuo, Gregg William Bergersen, and Yu Xin Kang*, Affidavit before the US District Court for the Eastern District of Virginia (2008).

¹⁷ David Ashenfelter and Lori Higgins, "Former Grand Rapids Man Pleads Guilty to Spying for China," *Detroit Free Press*, 22 October 2010; "Michigan Man Pleads Guilty to Attempting to Spy for the People's Republic of China," Department of Justice Press Release, October 22, 2010.

recruited by Chinese intelligence spent substantial amounts of time in China. Second, Chinese intelligence demonstrated operational tradecraft and exploited traditional motives like greed. Third, potential Chinese agents do not need to have direct access to sensitive or desired materials, just a willingness to make attempts to acquire them.¹⁸ Fourth, Chinese intelligence handled all of these agents from within China.

Chinese Effectiveness in Human Intelligence Collection

Without the benefit of inside information from the Chinese intelligence services, judging Chinese effectiveness and success involves speculating off the basis of a small percentage of Chinese espionage cases. These cases also may not represent the most sophisticated operations, and China's intelligence services have demonstrated the ability to handle a clandestine source for more than a decade. With these caveats aside,

The Chinese intelligence services benefit enormously from the resources available domestically to surveil targets, access their possessions, and exploit their personal electronics. Instead of days past where physical surveillance was required to evaluate visitors to China, the services can bring to bear advanced technical resources to follow individuals and find out who they are through their electronics without the manpower requirements of physical surveillance.

Perhaps the strongest part of China's HUMINT operations are the efforts to collect open source intelligence. The think tanks run by Chinese intelligence, such as the China Institutes of Contemporary International Relations (CICIR) and the China Institute for International and Strategic Studies (CISS), host a steady stream of foreign visitors, regularly send delegations abroad, and even post their analysts abroad on visiting fellowships. The Internet may have made gathering reports and publications much easier, but these direct person-to-person interactions offer another avenue for open source collection that often is not considered in the U.S. context. Foreign interlocutors can provide the gossip of their home country's policy community (useful for targeting), background information that never makes newspapers or reports, and occasionally more direct intelligence reporting.

The shortcomings to how China conducts clandestine HUMINT operations are threefold: the domestic base creates blind spots; the legacy of the Cultural Revolution damaged Chinese clandestine tradecraft; and wide variations in the training of Chinese case officers.

The domestic base for Chinese operations probably creates blind spots in the intelligence support available to Chinese decisionmakers. The kinds of sources that China can recruit easily are best positioned to report on their country's China-related affairs. Foreign specialists on China and, to a lesser extent, Asia travel to China, but those focused on other geographical areas do not necessarily go to China with the frequency or duration that would make a recruitment possible.

To date, China's clandestine tradecraft probably does not rate among the world's most

¹⁸ This particular feature is seen frequently in Taiwan's espionage cases, where a retired official, businessperson, or traveler is recruited to cultivate his friends, family, and former classmates/colleagues to collect intelligence. See, Peter Mattis, "China's Espionage Against Taiwan (Part I): Analysis of Recent Operations," *Jamestown Foundation China Brief*, Vol. 14, No. 21, November 7, 2014.

sophisticated at least with any consistency across a large number of intelligence officers. The Cultural Revolution and previous political movements purged (or killed) many of the Chinese case officers with professional knowledge, experience, and training in assessing, developing, recruiting, and handling clandestine sources, especially foreigners. The close compartmentation of sources restricted knowledge of HUMINT operations and left case officers vulnerable to charges of espionage for their contacts with foreigners.¹⁹ Such tradecraft is important for handling sensitive sources who place their lives in the hands of their case officer. For some time now, the Chinese intelligence threat could best be described as based on the scope, scale, and potential impact of these operations, not operational skill.

Although military intelligence is more centralized, the MSS is a far-flung, sprawling operation with a central headquarters, provincial departments, and municipal/county bureaus. At least the center and provincial departments run operations against foreign targets. Each is responsible for inducting new officers, mirroring the rest of the government. Local universities vary substantially in their quality and presumably this creates unevenness across the ministry's personnel. With little indication of centralized training program for new MSS officers from the ministry headquarters to the state security bureaus, the MSS appears to lack a way to ensure operations are conducted with a minimum level of competence.

This helps explain why so many China's intelligence successes have involved ethnic Chinese living overseas. Case officers with little foreign exposure, living inside China, cannot be expected to routinely approach potential foreign sources in the appropriate way. As former British Secret Intelligence Service director-general Richard Dearlove observed, human agents can only be recruited when "asked in the right way, by the right person, at the right time."²⁰

Challenges and Recommendations for Countering Chinese Human Intelligence Operations

No one outside the U.S. Government, especially the Central Intelligence Agency, Federal Bureau of Investigation, and National Security Agency, can answer whether U.S. counterintelligence is up to the task of countering Chinese human intelligence operations. The biggest complaint by former U.S. counterintelligence officials is that the amount of effort the United States expends against the Chinese pales in comparison to the effort Beijing expends to collect intelligence on the United States.²¹

One of the biggest U.S. vulnerabilities is young people in or recently graduated from university who go to China for extended stretches of time for study, research, or work. China's intelligence services have demonstrated repeatedly over the last three decades the willingness to recruit students and others inside China who might be directed to join the U.S. Government in the hopes of future access. Americans generally lack basic security awareness and have little reason to gain it as they grow up. Appeals to an optimistic future of U.S.-China relations, being a friend of China, and mutual understanding are easy pathways to engage the unwary and naïve. Programs,

¹⁹ Chambers, "Edging in from the Cold."

²⁰ Sir Richard Dearlove, "The Plot Thickens," *Financial Times*, September 2, 2007.

²¹ For example, Jeffrey Bliss, "China's Spying Overwhelms U.S. Counterintelligence," Bloomberg, April 2, 2007. Former National Counterintelligence Executive Michelle Van Cleave observed "The Chinese are the biggest problem we have with respect to the level of effort that they're devoting against us versus the level of attention we are giving to them," see, "Caught on Tape: Selling America's Secrets," CBS 60 Minutes, February 25, 2010.

like the National Security Education Program scholarships, also highlight U.S. students who will pursue a career in the national security and foreign policy establishment, saving Chinese intelligence the effort of identifying them.

The loss of Office of Personnel Management (OPM) files on millions of Americans with a security clearance and their associate foreign national contact data offers China something that it has not possessed previously on the U.S. national security establishment: a database of who's who. This data allows China's intelligence services, or at least the MSS, to validate the bona fides of potential U.S. sources, plan operational approaches through friends and acquaintances, and systematically approach Americans who hold or previously held security clearances. Having such a vast database of names and relationships is one of the ways in which Chinese intelligence has been able to sustain a high tempo of operations against Taiwan. Knowing who is potentially valuable allows them to exploit the constant stream of visitors from across the strait. The OPM data makes it possible to identify persons of interest as soon as they apply for a visa or enter the country²²

Retirees from government and military service also provide an avenue that the Chinese intelligence services have exploited in the United States and elsewhere. As retired officials, they are not subject to further background checks and or the other security measures that countries often put in place monitor officials with sensitive access. Although these officials no longer have direct access to policy deliberations and documents, they are in a position to provide assessments of policy developments informed by how the policy process and bureaucracy work as well as to identify and assess former colleagues. Chinese intelligence often asks for such reports rather than piles of documents.

Another area of U.S. vulnerability is losses through third-country partners, such as Japan, South Korea, Taiwan, Thailand, and many others. The U.S. alliance system, whatever its other national security benefits, creates vulnerabilities and access points to sensitive U.S. technology and information. For years, some of these countries had serious problems in trying to protect even their own information and systematic weaknesses in their ability to investigation problems. These vulnerabilities cannot be addressed unilaterally and require more routine cooperation with foreign counterintelligence authorities, like the effort that led to the arrest of Taiwanese General Lo Hsien-che in 2011.²³

One of the outstanding issues in how the United States confronts Chinese intelligence is how the U.S. Department of Justice declines to prosecute espionage-related cases. The most notable recent example is the case of Helen Xiaoming Gao, who worked as a contract translator for the U.S. Department of State and other foreign policy-related organizations around Washington, DC. On the basis of unsealed court documents, it is not clear why someone who admitted taking money from persons she believed to be Chinese intelligence to report on U.S. Government employees would not be prosecuted.²⁴ There are legitimate reasons why prosecutors may choose

²² Peter Mattis, "China's New Intelligence War against the United States," *War on the Rocks*, July 22, 2015.

²³ "AIT Confirms U.S. Role in Major Spy Investigation," *Taipei Times*, February 18, 2011.

²⁴ "Catherine Herridge, "State Dept. Contractor Allegedly Paid by Chinese Agent to Spy on Americans – Yet No Charges Filed," Fox News, April 22, 2015; *United States v. Helen Xiaoming Gao*, Affidavit before the U.S. District Court for the District of Maryland (2014).

not to pursue prosecution and why a case may not be as substantial as it appears.²⁵ However, because FBI operations are centered around cases, the inability to make a case can have far-reaching implications if the Justice Department's declinations to prosecute are viewed as repeatedly unjustified and politically motivated as the incentives to pursue Chinese intelligence-related cases disappear. As part of Congress's oversight role, requesting the Department of Justice to explain specific decisions not to prosecute going back over the last two decades would go a long way toward addressing concerns at the operational level about whether Chinese counterintelligence is a worthwhile pursuit.

²⁵ Several recent economic espionage cases, such as Sherry Chen and Xi Xiaoxing, have fallen apart on further scrutiny after sloppy investigative work, but serious problems go back to the Wen Ho Lee investigation and the leaks of nuclear secrets in the 1980s and 1990s as well as Katrina Leung investigation. See, Nicole Perlroth, "Accused of Spying for China, Until She Wasn't," *New York Times*, May 9, 2015; Devlin Barrett and John R. Emshwiller, "U.S. Drops Charges That Temple University Professor Sought to Give Tech Secrets to China," *Wall Street Journal*, September 11, 2015.

PANEL I QUESTION AND ANSWER

HEARING CO-CHAIR BROOKES: Senator, do you have a question?

HEARING CO-CHAIR DORGAN: I do, but why don't you proceed?

HEARING CO-CHAIR BROOKES: Okay. I'll start the questioning. Thank you very much for your thoughtful, your thoughtful testimony.

How does--do we have a sense at all of which intelligence organizations within Chinese intelligence structure have the most influence on policymakers and how that raw information that's collected is analyzed and provided to policymakers?

Anyone? I'll leave it open to the panel, but if anybody has a sense of that or you can all give a short answer.

MR. MATTIS: From the 1970s to probably the early 2000s, up through Jiang Zemin, it's fairly clear that the PLA's intelligence apparatus was the most influential on policy, simply because it's the only, it's the only potential all-source system in the Chinese government, and because of the direct personal relationship that existed between Xiong Guangkai and Jiang Zemin. Xiong, General Xiong being the head of the military intelligence system, there was an opportunity to provide analysis in a sense, in a very real sense.

Because of how sensitive analysis is in a Marxist-Leninist system, this is not something that's done routinely or at lower levels, the way it is within say the U.S. system. It's done at a very high level. It's carefully controlled, and if you don't have a sense of personal safety and responsibility, you can't pass unwelcomed judgments up.

And this is why I think they go to agents to say what is your assessment of this particular issue? That way they can say, well, we're just the messenger. This is what someone says, and you can take it or leave it. So there's not necessarily a formal processing system that evaluates the intelligence reporting, analyzes it, and then disseminates it to people.

HEARING CO-CHAIR BROOKES: Anybody else have any?

MR. COSTELLO: Just to mirror Peter's remarks. I mean it is noteworthy that we compare DIA, CIA, NSA to specific military organs within China. And it's, to be fair, it's not totally unlike the--there's a primacy of the DoD in intelligence work in the United States. With China, as Peter noted, there are major differences in analysis.

HEARING CO-CHAIR BROOKES: Mark, do you have some thoughts on this?

MR. STOKES: I would just say it's a very difficult question to answer. I would make a case in saying that what used to be called the General Political Department Liaison Department has the most significant access to senior policymakers.

HEARING CO-CHAIR BROOKES: Which department?

MR. STOKES: What used to be called General Political Department Liaison Department. These are the guys that are responsible for influence operations within the PLA.

HEARING CO-CHAIR BROOKES: Another question in the remaining time is who are the, do we have any sense of who the Chinese are cooperating with internationally on intelligence issues regarding U.S. interests?

MR. MATTIS: The answer to that question on the basis of open sources is relatively few. The best, the most visible examples of travel come from the Ministry of Public Security and now Commissioner of the, the head of the Political Legal Commission, Meng Jianzhu, who traveled quite extensively in Southeast Asia and in Central Asia to build the counterterrorism as well as some of the maritime policing, surveillance of the Mekong, and I think one of the points about Chinese intelligence is that international liaison is not really a part

of what they've done the way that the U.S. intelligence community, as it's constructed today, basically was formed in the middle of a liaison partnership. It was present at birth. And that simply isn't the case for the way the Chinese do business.

HEARING CO-CHAIR BROOKES: Okay. Good.

Mark, are the Chinese doing signals intelligence--because you noticed that they're all domestic--domestic--the TRBs are all domestically located--are they doing SIGINT operations overseas?

MR. STOKES: I don't know the answer to that. I would make an assumption that the answer is yes in a whole range of collection efforts.

MR. COSTELLO: It should be noted that they just, the PLA--the 2PLA related entity, specifically closely tied to the Aerospace Reconnaissance Bureau, just opened up a space monitoring and tracking station in Argentina.

Now they are sort of--not aerospace--they are astronomical-like telescopes. China does operate a suite of astronomical-like sort of telescopes within China and a growing--and obviously Argentina is the first one outside of its borders, but it is military related, and it--

HEARING CO-CHAIR BROOKES: Are the Argentineans aware of the nature of this operation?

MR. COSTELLO: Almost--it would be hard to--I'd be hard-pressed to see how they wouldn't be. I mean it is a known--the military affiliation is known. So.

HEARING CO-CHAIR BROOKES: Thank you.

Senator.

HEARING CO-CHAIR DORGAN: First of all, thanks for your being here and your testimony. It was very interesting.

Two things. One, first an observation. In the briefing material last evening, I smiled a bit when I saw something that Commissioner Tobin reminded me of in the material. It's a National Security Agency map marked "secret," and then also marked "NBC News, July 30, 2015." And it's a map of U.S. victims of Chinese cybersecurity over the past five years with red dots, and the only state that does not have a red dot is North Dakota--

[Laughter.]

HEARING CO-CHAIR DORGAN: --which is where I'm from, which--

COMMISSIONER WESSEL: Because you live here now.

[Laughter.]

HEARING CO-CHAIR DORGAN: Which happens to be one of the largest repositories of nuclear weapons in the world. Two major military installations with substantial nuclear weapon storage. I was very surprised by that. But also kind of surprised that it is "secret" on NBC News. But that's another story for another hearing perhaps.

You, Mr. Costello, you mentioned federal contractors being the consistent soft-underbelly, I believe. And I suspect all of you have observations about it, but you, you say federal contractors are, rather than were, the soft- underbelly. I assume that--and then describe the office of--the OPM Keypoint Government Solutions issue. What have you observed since that time--since the OPM data was breached? Has the government done what you think it needs to do to provide greater protection with respect to contracting agencies? There are so many federal contractors, it's unbelievable, in virtually every agency and every area.

So what's your sense of it? Have we, have we learned from the OPM breach? What has transpired since to try to tighten this up? And perhaps, Mr. Mattis and Mr. Stokes, if you have observations, I'd like to hear them as well.

MR. COSTELLO: It's difficult to sort of assess where current contractors stand as far as their information security. The updated rules to DFAR, the Defense--the acquisition regulations for Defense--to include a cybersecurity requirement and gives greater oversight to contractor information security--is a good step in the right direction.

I don't think we've seen any sort of equivalent for general contracting, specifically any contracting service that directly connects to federal information technology systems.

I think just the fact that we're shining light on this and it's becoming more like a known sort of problem, and I think that is what is sort of needed right now.

I think it would be bad form and sort of not prudent to sort of have a knee-jerk reaction and just push out legislation, blanket legislation. I think what's going on right now with investigations and oversight into particular instances where contractors have been breached and have led to large federal breaches I think is the right way right now. So if that answers your question, Senator.

HEARING CO-CHAIR DORGAN: Uh-huh. Uh-huh. Any other observations?

MR. STOKES: I can't think of--I don't have any particular insights on that one.

HEARING CO-CHAIR DORGAN: All right.

HEARING CO-CHAIR BROOKES: Commissioner Fiedler.

COMMISSIONER FIEDLER: I'd like to direct this to you, Mark. Why should we trust sharing information with Taiwan? We've had so many major high-level breaches.

MR. STOKES: If I can sort of first ask what information are we sharing with Taiwan--to begin with? I'm not aware of any classified U.S., any classified U.S., you know, basically classified secret or above that has been provided to Taiwan that has leaked over to China. I'm not aware of any.

Unclassified stuff, yes, there has been lots of, lots and lots of cases. Unclassified but sensitive or whatever term one wants to use. But whatever technology that we transfer, my impression is, it is given a red team. It's red teamed. It's part of the standard process in which we transfer technology, that it's, basically there's sort of a worst case assessment, that if it ends up in the hands of the People's Liberation Army, what effects is this going to have on the United States?

I would say that there are other governments that get more advanced technology. Taiwan doesn't get our best.

COMMISSIONER FIEDLER: I'm not only talking about technology. I mean Taiwan has always been one of the chief gatherers and then sharing with us information on the mainland, and my own sort of experience is that is not going to be a one-way street. So that there are other sensitive operations in the U.S. intelligence community that are probably being shared with Taiwan that I--I mean I personally think it's a sieve at the moment, and that we have a counterintelligence problem. That's all that I'm saying.

MR. STOKES: If I can, one last one quick one, and I'll turn it over to Peter.

COMMISSIONER FIEDLER: Now, by the way, I don't want, I mean I have all kinds of other views on Taiwan--

MR. STOKES: Right.

COMMISSIONER FIEDLER: --that are not influenced by that. But it is a national security problem for the United States, it seems to me.

MR. STOKES: My last comment, and I'll turn it over to Peter, is that it's certainly worth studying and looking at in more detail. I would recommend doing a case study that would compare Taiwan's, any potential leaks, security breaches on Taiwan, and compare that with what

we faced with other sovereignty-related disputes that have occurred throughout history including West Germany, looking at some of the breaches that occurred in West Germany and also, of course, looking at South Korea as well.

COMMISSIONER FIEDLER: Just a quick answer because I've got another question.

MR. MATTIS: A very quick point given that I've written a paper on this and presented at Project 2049 on this very subject.

There are a few points that are worth sort of looking at the long-term to be optimistic about Taiwan. First, when you look at a number of these big cases that have happened in the last five years, it has been senior officers with an old kind of mainland affiliation and thinking. And as they've been leaving the service, they've tried to find young officers to replace who will continue to provide information. Those young officers have turned them in. That has been the primary source of Taiwan's counter-espionage leads.

And this younger generation coming up within the national security establishment has a much stronger Taiwanese identity that is simply not tied to the mainland China, and to be dismissive of how important this has been to the successes of Taiwan's counterintelligence community I think is to not give them credit for how well they've done.

COMMISSIONER FIEDLER: For arresting those people. I get it. Yeah.

MR. MATTIS: The second, you know, with respect to can we trust them, can we work with them, can we share with them, the Taiwanese have had successes in the PRC that no one else has duplicated ever. Central Committee members have been recruited by Taiwanese intelligence. In the mid-2000s, Taiwan controlled or had recruited the entire leadership of the PLA Air Force Command College, and many, and many, many others.

COMMISSIONER FIEDLER: I'm going to ask another quick question. On the impact of Zhou Yongkang prosecution, clean-up of his network, in the anti-corruption campaign run by Xi, what's been the impact on state security? Is it discernable to us? Any impact on state security? He must clearly have used his state security operation to enhance his political life.

MR. MATTIS: A couple of quick points. One is that there's been no discernable operational impact on MSS operations abroad. There were efforts to manipulate parts of the Ministry of State Security for political purposes. But it's worth noting that the creation of the MSS and the political reliability but lack of independent political clout that the ministers of State Security have had represent an effort to keep the intelligence services out of elite politics.

This is actually one of the violations that Zhou Yongkang committed that made him vulnerable was that there was a view to keep it separate.

COMMISSIONER FIEDLER: So do we have a sense of how deep that went in terms of removing of people from positions if not prosecuting them?

MR. MATTIS: The head of the Beijing State Security Bureau was removed. There were reports that Qiu Jin, who was the head, a Vice Minister in charge of counterespionage and investigations within the MSS, was removed. He wasn't removed, but he was clearly demoted for a time, and he's returned to a position after, of another Vice Minister, Ma Jian, who had been promoted up in his place, was removed because he had--was linked to Guo Boxiong and military corruption.

COMMISSIONER FIEDLER: Thank you.

HEARING CO-CHAIR BROOKES: Commissioner Wessel.

COMMISSIONER WESSEL: Thank you all for being here. Mr. Stokes, good to see you again.

I sort of feel like we're flat-footed. You know, a little more than two years ago, we had the five PLA indictments you mentioned. Two years later no real sanctions to ensure that there was an understanding that a price was to be paid for those kind of activities.

China is, you know, actively engaged in their 1,000 Talents Plan, which I'm sure you know about, where they seek to recruit major researchers at R&D institutions, companies, universities, et cetera, many of who have received federal benefits here in terms of their fellowships, et cetera, and are asking them to take full professorships in China. It's open source. Just google "1,000 talents," and you'll find it.

Since last October, September-October's summit with President Xi and President Obama where the MOU was signed, there's been sort of a diminished attention to all the kind of espionage that's going on, but to me it appears that it's not abating in any way. Am I correct? How is China organized to pursue this? Has the threat abated in any way? And, please, from all three of the witnesses.

MR. COSTELLO: I think from my understanding, I think earlier this year, Director of National Intelligence James Clapper did mention that there's been a down tick in the number of Chinese sort of cyber intrusions into U.S. systems.

Whether you can sort of attribute that to any sort of diplomatic pressure of the MOU, I think that's difficult to tell at this time. Personally, I think it's more a tribute to the military reforms. I think Xi--Xi doesn't want--you know, I mean a lot of these guys, sort of the idea is a lot of these guys were contracting themselves out, were moonlighting as hackers, you know, on their nights and weekends or even during the day.

I think for good order and discipline, to use an old Navy term, I think, you know, Xi Jinping sort of wanted to get rid of those sort of secondary and tertiary sort of paymasters, and I think that's, you know, for the professionalization of the service, I think that's extremely key.

To what degree he's doing this in, for lack of a better term, in good faith, you know, to do the sort of legitimate intelligence targeting, it's really unclear, and it's also unclear whether it's going to sort of pick up again in the future. My personal view is that it won't. I think we are seeing a growing professionalization of Chinese military and Chinese state intelligence agencies, and I think we will see them to be used for legitimate intelligence targeting.

Now that does not speak for any contracting companies, contracting groups, unofficial or semi-official, or any number of sort of like, you know, terms that may be hacking for their own ends.

COMMISSIONER WESSEL: Couldn't this also be a function of, you know, we talked about "grains of sand," that there's been the grains of sand, there's been the mapping of the networks, et cetera, and identification of, I guess, early harvest or low-hanging fruit. U.S. Steel, which filed a case on cyber intrusions just a couple of weeks ago, indicated that the incursion was focused on one file. So rather than going into their entire R&D database, they were looking for one thing. So to me the level or the number of incursions doesn't mean that the threat has abated in any way.

MR. COSTELLO: Well, I mean, so, excuse me, perhaps I misunderstood your question.

COMMISSIONER WESSEL: Okay.

MR. COSTELLO: I mean do I think the threat has gone down? Absolutely not. The thing about a Russian model of cyber sort of espionage is that the overall number of intrusions will likely go down, but the sophistication and impact of those intrusions will go up dramatically because if you start to centralize and coordinate cyber efforts, what you get is you

share vulnerabilities. You share intelligence. You share resources. You share tradecraft. You share personnel.

You also deconflict mission so you're not stepping on each other's toes. I'll give you a for instance. In the OPM, in 2014, there were two sets of we'll say a certain country in Asia's cyber actors that were present on the network at the same time. Now deconflicted, normally these would be coordinated and they would sort of be sharing intelligence. I think that is what we can expect to see in the future, not, maybe not because for whatever reason, but mostly because it's good tradecraft, and it's good intelligence.

And also it will produce the type of results that I think China needs as they expand their influence outward. The intelligence agencies need to provide real-time ongoing intelligence. "Smash and grab" tactics where they're stepping on each other's toes and using contractors that may have a financial stake in this, that's not a viable method of going forward.

MR. STOKES: I don't have a lot more to add than what John said, but I would give one anecdote. As an institute, Project 2049 Institute, we do focus a bit on looking at--we do research on PLA and do research on Taiwan issues, cross-Strait issues, things like this.

About five years ago, we were hit pretty often with intrusion attempts, multiple ones, especially after we released a particular product, and it was pretty obvious and quite in your face, almost purposeful, almost a form of political signaling. But over the last year or two, it's dropped off significantly. I don't think we make an assumption that they're not still interested in us, they don't love us anymore, but I would, I would just say that one of the theories that we had before is the concept of an A team and a B team.

China has some of the best computer engineers in the world, information security engineers in the world. In the B team a lot of amateur hackers that John referenced were out and running around. I would say these days there have been reports of diminished amount, but maybe it's just a little bit less on the B team, but the A team is still just as active. I would still make an assumption that there's a lot of--that unprotected computer systems are still vulnerable and are exploited.

MR. MATTIS: Coming at this question from the HUMINT perspective, I wouldn't say that it's so much as flat-footed as that there are simply too many things for us to prioritize well in terms of how we deal with them because one of the issues that I take with the "grains of sand" perspective is that it says that this is an amateurish operation. And China has more professional intelligence systems that are focused on particular customers than any other country that we know of ever existing.

For example, there's the Institute of Scientific and Technological Information of China, which is basically a national library system to feed foreign S&T information to researchers in China, to package what they need to know about the state of the field and where they should go in research avenues and particular technological solutions to engineering problems.

You have the intelligence services doing a variety of things. We talk about pushing people-to-people exchanges. Yet the institutions on the Chinese side that are responsible for people-to-people exchanges are organizations that have existed since the 1930s for exploiting those kinds of relationships. They're not--it's not the intelligence services, and it's not called intelligence in the Chinese system, but United Front Work is still sort of a key function of what they're doing.

And if you're thinking about the kind of limited resources that we have to put against these kinds of threats across this whole spectrum, it's not very easy to say, oh, well, this

is more important than this particular other one because you have to--you spend a ton of investigative resources even to gain a little bit of traction to figure out what's going on.

And then the question is can you make a case on it? And sometimes the answer is yes and oftentimes the answer is no. It's one of the wonderful things of living in a democratic system, but it's also one of the challenges in how do you deal with people who are injecting themselves into public debate without perhaps the integrity that were intended with the responsibilities of freedom of speech?

HEARING CO-CHAIR BROOKES: Thank you.
Commissioner Cleveland.

COMMISSIONER CLEVELAND: So in the Shriver case, they went after somebody who was not ethnically Chinese. Compensation rather than moral inducement was the approach, and they were trying to seed him first into the Foreign Service and then the Agency, and I think, Mr. Mattis, you described them as patiently waiting for opportunities.

Is that any different than anything that we do? I ask this of all of you because I think there's kind of an inclination to be alarmists about what the Chinese are doing. I think cautious and prepared is appropriate, but I'm not sure in all of this other than maybe the amateur hackers that what's going on isn't something that every intelligence agency in the world does.

And then I'll have a second question. So, yes or no, do we all engage in this kind of conduct?

MR. MATTIS: The differences are largely in the use of specific techniques rather than any kind of approach or methodology. For example, there's no one who can point to any record of the Chinese ever using a dead drop.

COMMISSIONER CLEVELAND: Okay. So we're down to tactics, yeah.

MR. MATTIS: But, you know, it's really, but it's really down at that level that you start to see the differences, and, you know, a common element, if you read all of the documents that are out there on Glenn Duffie Shriver, is he very rarely met with just one person. And many espionage cases don't involve a single Chinese case officer, almost always a second person in the room, and there's almost always another person who's injected in as a senior manager to come and sort of introduce and say, hey, we care about you.

COMMISSIONER CLEVELAND: So techniques may differ, but let's be real.

MR. MATTIS: Right.

COMMISSIONER CLEVELAND: We're all engaged in the same kind of activity. So that raises the second question, and it tees off of a comment that you made, which is in Marxist-Leninist--I think those were your words--systems that, in my view, are rigid and have perhaps very politically skewed expectations. It's not what you're collecting; it's how you're using it. How you're putting the information together.

And I'd ask all of you, your presentations have focused on the operational side, whether it's collection of technical or other data, what seems to me missing in your analysis is some kind of assessment of when consumers, when politicians, when policymakers drive the collection agenda, it tends to skew the analysis.

I thought your comment was interesting about they used their assets to essentially convey the bad news that people don't want to hear, but can you talk a little bit about there is this whole incredibly intense collection effort that's I think legitimately troubling, but then what? What's happening on the analytical side? And how useful is information that's being collected? How is it put together? How is it presented?

I get it when it comes to stealing technology for the economy, but more broadly,

what's happening on the analytical side, and what difference does all this make?

MR. MATTIS: As I think we echoed--we all echoed each other on--that making a judgment about what takes place at the top levels of the Chinese intelligence system is basically a fool's enterprise. I mean you say we're missing analysis. I would say that if we put something down on paper, we'd be guessing. And--

COMMISSIONER CLEVELAND: Not your analysis. I'm interested in what you think happens with all of this stuff that gets gathered.

MR. MATTIS: The one place where there is information that suggests how it gets used is the collection of personal information as it goes into the preparation for negotiations. Every single study that's been done, whether it's Richard Solomon, Lucian Pye, Albert, Alfred Wilhelm, has talked about how prepared the Chinese interlocutors are to come and deal with the U.S. perspective.

And this is where I think you can say that the Chinese are good with the open source because there's so much that you can collect by simply having somebody running around Washington, D.C., going to meetings and talking to people, and I think since the mid-'90s someone from the MSS--it's either the Eighth or the 11th Bureau, the China Institutes of Contemporary International Relations--has been a visiting fellow somewhere in a D.C. think tank since I think '94 or '95. That offers a lot of opportunities to pick stuff up that you wouldn't necessarily hear because people talk, people gossip.

COMMISSIONER CLEVELAND: Cocktail circuit is a rich source, yeah.

MR. MATTIS: And, but to give you a sense of how rigidly controlled analysis might be in the Chinese system, the MSS does not actually have a sort of an intelligence analytic bureau, to our best knowledge. That analysis as the MSS does it is conducted by senior staff that are connected to a vice minister's office or the minister's office, who are brought along with that person to say, you know, when a report needs to be put together, that person will get tapped to write it.

But it doesn't happen, again, as a routine bureaucratic basis. We simply know that information is collected, it's processed in some form, and then it's pushed forward into the system.

COMMISSIONER CLEVELAND: I think the worry for me is that the risk of miscalculation because of that gap between what's collected and then whoever the person is who's writing the report, those risks in terms of we like to talk here about connected dots, whatever it is that happens in that world.

Mark.

MR. STOKES: I'll pick up on a point that you made about the nature of the system, nature of the political system in Beijing and throughout the country, which is the Marxist-Leninist system.

One of the most significant differences between a Leninist system and systems of, you know, the United States and other, other open societies, one of the most significant ones is in the organizational structure, which when you have a, you know, a central propaganda department, or they call it public publicity department, that's one example. When you have an organization within the PLA that is equal in grade, equal in stature to the 2PLA, you know, the PLA Intelligence Department, or roughly to say or equal in stature to the Third Department, and this is the General Political Department Liaison Department that's responsible for clandestine HUMINT collection but also influence operations, on anything that has, that touches upon defense, and so when you have this sort of organization that uses intelligence that's collected

specifically for a purpose for propaganda, for influence operations, this is one of the most significant differences between their system and our system.

I mean there are other major differences that's well known. For example, on the economic front, that's use of intelligence information to be able to support trade, investment sort of negotiations, the use of intelligence, for example, linked with economic, for example, investments in the United States, for that matter, that are geared toward gaining access, for example, to U.S., let's say, for example, top U.S. federal labs, and there's at least one case that's pretty significant, I think, having to do with an aviation related issue. So these would be some of the main areas that I see some differences.

MR. COSTELLO: I'll be quick. I'll go to the exact opposite sort of route. I'm going to go down to very tactical level because that's with what I'm most familiar. There's a sort of very keen pattern to Chinese sort of command and control in the lower levels of military, which is there's a fundamental distrust of subordinates, not to say that they think they're going to be stabbed in the back, but this sort of, you know, like you say like sort of censorship is a sort of an idea that society can't trust itself, right, and it sort of bleeds over into the military as well and I think in intelligence. So China has created its sort of command and control infrastructure that allows senior military commanders to get large amounts of information and process it themselves rather than have it fused and processed at lower levels.

Now I think that's reflective of the national structure as well, or it might just--that might actually be a sort of a ramification of having a national structure in which things are analytically fused at higher levels. So what you get is, I mean ideally what you want your intelligence community to look like is a Leviathan. You want these large like tentacles like reaching out and fusing things and having it come back.

So right now what China's sort of intelligence community looks like is more like a hydra. I mean you've got sort of competing heads that have their own analyses and that are advocating for their own programs. And I think you'll see a shift towards a more, if you want to use that, as a Leviathan model, over time. But there is a very real understanding that a Marxist-Leninist political system institutes this sort of distrust of subordinates for political reasons and judgment reasons at all echelons from the national level down to the tactical.

COMMISSIONER CLEVELAND: Very helpful. Thank you. But it reinforces my view that they could ultimately be very wrong in terms of how policymakers use whatever it is that's collected.

MR. COSTELLO: That's a good point, but I mean China makes note, and I know time, really crazy, but the 2013 Science and Military Strategy, China makes a really I'd say a weird sort of odd point. They noticed the deterrence factor of intelligence surveillance. I mean specifically they talk about the use of overhead satellites to shape sort of carrier group like operations on the sea, and as a sort of corollary to that, active intelligence operations, they have a very real understanding that they can shape U.S. behavior through active intelligence operations.

So when it comes to like them being wrong, my counter to that is, is sometimes they don't necessarily need to be wrong. By virtue of the fact that they're running an intelligence operation and an intelligence operation is known, they can shape U.S. perceptions and behavior.

COMMISSIONER CLEVELAND: Interesting. Thanks.

HEARING CO-CHAIR BROOKES: Quickly, sure.

MR. MATTIS: Just a very quick point. In terms of intelligence history, even in the last say 50 years of American history, the idea of all- source analysis being the sine qua non of intelligence is kind of a false concept. Successful intelligence has often always involved sort

of concrete reports.

The second point is that in the Chinese system, there is a distinction of intelligence, but there are also several rings of behavior, and Mark has talked about this issue of influence. And in many cases, what we talk about as intelligence is, in fact, sort of a covert--we should be thinking of it as China's covert power in a much broader way because of how it bleeds over from support to decision-making to targeting influence operations to trying to shape sort of who knows what about which side.

COMMISSIONER CLEVELAND: Thank you. That's a good distinction.

MR. COSTELLO: Peter said what I said, just much better.

[Laughter.]

COMMISSIONER CLEVELAND: No, it was all very--very, very helpful.

Thanks. Sorry, Peter.

HEARING CO-CHAIR BROOKES: Commissioner Tobin.

COMMISSIONER TOBIN: Great. Thank you, all.

Mr. Mattis, you gave us in your written and oral testimony a sense of what intelligence is, you relayed the quote that it is "information that resolves specific decision-making situations." What I wanted to talk about is the shake-up in MSS. You touched on it when you responded to Commissioner Fiedler's question explaining why there were these two, at least two levels of changes on vice ministers.

This was several months ago now. I'd like to hear from you, Mr. Mattis, but also Mr. Stokes and Mr. Costello. What do we know about the new people that have come in and how that is playing out, and to use your definition again, what kind of specific decision-making situations is going on? What do we know?

MR. MATTIS: The unfortunate thing is that the MSS has learned since it was exposed during the Wang Lijun and Bo Xilai incident that with just the slimmest leads that an MSS person was going from Beijing to escort Wang Lijin from the U.S. Consulate back to Beijing, that Bloomberg was able to identify exactly who it was who was going down, which was Vice Minister Qui Jin, and sort of say what his responsibilities were.

And I wrote a piece on the vice ministers--I guess it's over a year ago now--and I could not write that piece again because of how thoroughly the Web has been scrubbed of that kind of information about people at the vice minister level. It is incredibly difficult to find any information now on some of the people that were there. Many of the Web links that I had are simply gone. You can't find the original sources for some of them.

So to be able to give a good answer about what the impact has been, it's really that they've learned that information shouldn't be out there because they haven't wanted it to be out there, and they've sort of slowly squeezed out some of the areas where it's appeared so you can't make a good judgment about these things.

The one thing that I would say about the one new person that we know who has come in named Chen Wenqing as the Party Secretary for the Ministry of State Security is that he, he began his career as a Ministry of Public Security official in Sichuan. When the Sichuan State Security Department was created, roughly ten years after the creation of the Ministry of State Security, this was not an even process across the country--it was a very slow one that wasn't completed until the mid to late 1990s--he was moved over to State Security. He was simply told one day that you're no longer a Public Security Department official for Sichuan, you are a State Security Department official.

After that, he moved into the procuratorate so he is an official who has moved his

way up the ranks, and he has seen the entirety of the political legal apparatus. So he's been involved in police work. He's been involved in counterintelligence and counterespionage. He's been involved in the prosecution and investigation, you know, in a legal sense. So he has a broad perspective about what the system is and where it can play.

What does that mean? There is simply not enough information to even begin to speculate simply other than to say that he's an experienced professional, and like the minister who's currently serving, Geng Huichang, these are--previously they were political appointees without necessarily a lot of professional experience. These two--

COMMISSIONER TOBIN: So he has that professional experience.

MR. MATTIS: Experience.

COMMISSIONER TOBIN: Any of the other leaders?

MR. MATTIS: No way to know how the vice ministers have changed. For example, the last person in my records who was probably overseeing foreign intelligence for the MSS, Sun Yonghai, I can't tell whether he still works there. I can't find other information that would allow me to say, you know, if he isn't, who replaced him.

COMMISSIONER TOBIN: Mr. Stokes.

MR. STOKES: I'd defer to Peter on anything directly related to MSS, but what I would say is recommend keeping an eye on the ongoing military reform and PLA reorganization and looking at particularly at something called military-civilian fusion and exactly what is its potential relevance to the intelligence field in addition to a whole range of other areas.

Could there be some sort of, some sort of restructure that occurs within the PLA and could there also be some sort of connection with MSS in terms of either transfer of responsibilities or something like that? I have no information that would confirm this, but it's just something that could be worth keeping in mind.

COMMISSIONER TOBIN: Okay. Mr. Costello.

MR. COSTELLO: Regarding the specifics of your question, I'd also have to defer to Peter. But also in sort of response to sort of Mark's comments, there have been sort of suggestions by experts, by Chinese experts and U.S.-China experts, that, you know, with the current round of military reforms, we may see sort of a rejiggering of some key sort of specifically cyber missions between the MSS and 3PLA and the 4PLA. While that doesn't talk, that doesn't address your question specifically, I feel like it should be noted.

COMMISSIONER TOBIN: It is somewhat ironic, I think, that there is this effort against the corruption, and there was a vehicle that could have helped get at some of that, and yet for understandable other reasons, they had to close that down.

Okay. We'll watch the military reform. Thank you, all.

HEARING CO-CHAIR BROOKES: Commissioner Shea. Chairman Shea.

CHAIRMAN SHEA: Thank you. Thank you, all, for being here today.

I'm going to try to cram two questions in. I think, Mr. Mattis, you said that the Chinese engage in classic intelligence gathering, and intelligence is information that resolves specific decision-making problems. Do we know what those specific decision-making problems are currently other than just beyond, you know, they want a lot of technology, they want access to defense technologies and systems, but do we know--do we have a sense of what the specific questions, priorities that they're seeking?

And the second question that goes back to this Glenn Duffie Shriver situation, is what, how big of a problem is this or a potential problem? Are a lot of American university studies studying in China potentially at risk? I mean is this a major, a one-off thing, or is this

something we should take more seriously? And if so, do U.S. universities brief their students who may go over to China to alert them of the potential risk of being recruited by Chinese intelligence agencies?

MR. MATTIS: Let me start with the easy question first, which is your second, and the answer to that is no. I mean the U.S. government is not even particularly good at briefing people ahead of traveling abroad in some of these areas, in part because Americans aren't necessarily born or raised with the concept of security the way you get in most other societies in the world.

You know we've been blessed with a wonderful history that doesn't involve being in a police state, but unfortunately that means that the rest of the world has an experience with these kinds of things that we simply don't. Or that most Americans don't. And we don't hear from our parents and our grandparents.

With respect to the--

CHAIRMAN SHEA: So universities should be warning their students who may be going abroad for junior year or senior year or on a fellowship to just be a little bit careful? Is that something universities should do routinely in the United States?

MR. MATTIS: I think it probably could be folded into a generic travel security briefing, not something related to China specifically but sort of good, good tips for being abroad, no matter where you are, because there are a number of other things that would be beneficial for students, and especially if you wanted to work in the national security community, there are a number of very concrete steps that you can take to sort of make sure that you can fill out your forms appropriately and that the people who are responsible for investigating you can sort of verify and validate some of that information.

With respect to sort of the specific decision-making kinds of problems, the biggest ones really are support to military operations, monitoring what U.S. forces are doing, what Japanese forces are doing, what the Taiwans are doing, what other border areas are, the protection of state security, meaning sort of threats to the Party State, whether they range from Falun Gong to democracy activists to Tibetans and Uighurs, both domestically and in exile.

I would highlight, though, that on the issue of collection of science and technology, when you look at who collects what, the intelligence services tend to collect things that are either directly relevant to say supporting military operations. If you're trying to acquire the quiet electronic drive for the Virginia-class submarines, you know, it's a classic military intelligence target, not necessarily first a reverse engineering one, but what is the U.S. submarine going to look like that we need to look for?

They're getting whole systems and the kinds of things that someone who has been trained in liberal arts and foreign languages can understand very easily--someone like me--whereas, when you look at what sort of call it the amateur collectors, but professional engineers and scientists and information workers, are after, they're looking for parts to complete systems.

They're looking for components, very specific components that can be folded into sort of bigger projects, and that's why you find these weird cases of, you know, 15,000 units of widget X being shipped to China because they're actually just going to take that little part, and they're going to plug it into the system, and so, you know, it runs the gamut from the professional intelligence services to across whether it's companies or sort of criminal entrepreneurs who are trying to start their own business.

CHAIRMAN SHEA: Mark or John?

MR. STOKES: Very quickly augment what Peter just said, priorities at the

national level, anything that could be deemed a threat to the Chinese Communist Party and its monopoly on power. That would be number one. And so, therefore, as Peter mentioned, anybody calling for--basic democracy advocates. Bear in mind I don't think they distinguish between--most of these threats would be domestic, but I don't think they distinguish between, between domestic democracy advocates and international democracy advocates. Throw Falun Gong and others in there.

Second would be sovereignty. Taiwan is a classic case. I would say Taiwan is a top priority in terms of intelligence collection. And anything, bear in mind, it's not just a cross-Strait issue. Taiwan has relevance around the world. It's the policy the United States has toward Taiwan and cross-Strait issues in general.

Third priority would be territory and territorial integrity. That's border and coastal defense. South China Sea, East China Sea, and government policies of neighbors that affect their border and coastal defense.

To be able to pull a little bit of a thread that Peter threw out in terms of other what you call sort of "cats and dogs" priorities, on the military and technology side, in addition to what Peter mentioned about sort of directly trying to go after some crown jewels, you also have sort of leveraging a traditional dual-use technology approach where you can take advantage of key research organizations within the United States that are doing leading work on military relevant technologies. Let's say, for example, related to missile defense, at a particular university in Florida, this case about ten years ago where you can just walk in the front door and get some leading technology.

Or, let's say, for example, going back to that example of the U.S. research, a National Laboratory that does cutting edge research on additive manufacturing or 3D printing or other organizations that do key engine-related research and development. What do you do? First of all, you break into the computer systems of this particular federal organization, this laboratory. Let's say, for example, somewhere between 2009 and 2011. Then you buy a U.S. company that is considered to be doing some cutting-edge research on additive manufacturing, and then it just so happens that this particular U.S. company has significant relationship with a U.S. federal laboratory, and there are probably many examples of this sort of approach to get information by basically taking advantage of dual-use technology to be able to get access to what they need.

CHAIRMAN SHEA: Thank you.

HEARING CO-CHAIR BROOKES: Vice Chair Bartholomew.

CHAIRMAN SHEA: Did you want to say something, John?

HEARING CO-CHAIR BROOKES: Oh, okay.

MR. COSTELLO: Yeah. Just I think Peter and Mark pretty much covered it pretty well. I just want to highlight one thing. I mean practically speaking for most of its history, China has been mostly concerned with internal control, border defense, and, you know, near seas, as Mark was good to mention.

However, you know, technology and trade have brought the world into China, and China is very aware of that. And, you know, for the Communist Party, they've brought in potential sources of information, you know, channels of information to the Chinese populace, which they don't necessarily feel they can always control.

And also for energy security and economic growth, they've pushed outward, and they're continuing to push outward into strategic areas of international competition. Near seas, far seas, polar areas, space, cyber, and I think, most importantly, the information domain, and what I mean by that is international public opinion. They understand that they can't control all

sources coming into China anymore.

So instead what they're doing is, is they're pushing their narrative out into the international community so that in sort of a way so you can't control the door so you control the hallway basically. That's what China is doing. As they've done this, and as they push outward, their needs, their intelligence needs, have matured and grown and require a much greater focus on real-time operations that can guide military operations. It can preempt U.S. movement and preempt policy, policy initiatives from foreign nations that may affect them.

HEARING CO-CHAIR BROOKES: Carolyn. Vice Chair Bartholomew.

VICE CHAIRMAN BARTHOLOMEW: Thank you. Thank you. This is very interesting. Just I'm going to start out with a personal anecdote on this gathering of personal information, which is a few years ago on one of our trips to China, we were taken to a museum, not in Beijing, and I was looking at a piece of pottery, and the interlocutor who was standing next to me said it looks a lot like an American Indian design, doesn't it, and I thought, well, that's really interesting, both because it did, but also because in the 1980s, my family lived and worked on the Navajo reservation, and it's certainly nothing that I hide, but it's nothing that has been particularly salient for the past 30 years. And that was, it was a heads-up for me that people are tracking what we're doing and looking for information.

I want to go, though, two things. One is on influence operations. You know the Chinese recently posted four police officers in Rome and Milan, and it didn't get--The New York Times wrote about it, and it didn't get a lot of attention. They were there purportedly to protect Chinese tourists so, as even the article pointed out, how four people across two cities with tens of thousands of Chinese tourists could do much is a real question.

But I found myself thinking is this just an effort to get people to feel comfortable with a Chinese presence, a visible presence, and also I wondered whether it was a message to all of the tourists that you better behave yourselves and be careful of what you say as well as any dissidents who might be there? So I just wondered if you guys have heard anything about this kind of activity? Is this something where they're just kind of trying to mainstream an institutional presence that is certainly not embassy or diplomatic? That's the first thing.

And then the second thing is I have been very interested and have been following the Chinese personnel operating certainly overseas but here in the United States. One is on the tracking and targeting of dissidents and sort of how they're doing that, and then the other one, of course, is that we have had Chinese personnel coming into the United States to try to track down and I guess take people who they believe are criminals, corruption, things like that.

But I wondered if you could just, if you could just sort of start with the process of who in the Chinese system is responsible for identifying these dissidents, who is responsible for tracking what they might be saying or doing, and who is responsible for the threats that are being made to their family? Is it all the same agency? Is there some way of breaking down what parts of the intelligence community are involved in this?

Mark?

MR. STOKES: Let me let Peter have the first half because this--

VICE CHAIRMAN BARTHOLOMEW: Okay.

MR. STOKES: I would say MSS so naturally, you know--

VICE CHAIRMAN BARTHOLOMEW: Yeah.

MR. MATTIS: So quickly on the MPS abroad, there's been a tremendous amount of public dissatisfaction in China about the effort that the government expends to protect Chinese tourists abroad. If you go back over the past few years and you total it up, there are several

hundred Chinese people who have been kidnapped, killed or otherwise hurt in a lot of different places across the world. The MPS has been active, particularly since October 2011, when 13 sailors were killed on the Mekong River, that you see MPS in Southeast Asia helping hunt down the drug lord who was believed responsible. There were MPS officers who were in Angola in I think 2012 or 2013 that were responsible for helping Angolan authorities investigate a Chinese organized crime syndicate, and the MPS brought back 40 some odd people I think to China to face prosecution and jail.

There's simply been a, I think this is the issue of the Chinese government has been asked to do more by the public, and there's a sense of how do we respond and how do we try to do some of these things?

As far as who's responsible for tracking dissidents, I think one of the key features of the Chinese intelligence system is that it is competitive rather than cooperative, and so I think the Ministry of State Security and the Ministry of Public Security both have responsibilities and they overlap so that it's not simply sort of kept in one channel to push, to push forward.

The MPS has a lot of the internal surveillance databases. They're the ones that have access to border crossing information automatically. They're the ones who have sort of real-time access to hotel data when someone checks in whether it's with a passport or a household registration. And I think that one of the ways that they sort of make the system work is to ensure that there are multiple strands that are sort of following and moving, and moving along to pursue these people.

MR. STOKES: I agree with what Peter mentioned, that there are multiple organizations. I would throw one other one in, and that would be the United Front Work Department in looking and tracking Chinese dissidents overseas, particularly if they have a relationship with overseas Chinese communities in New York City, Los Angeles, San Francisco, Washington, D.C., Houston, Texas, just a whole range of organizations.

MR. MATTIS: Plus the Ministry of Education.

MR. STOKES: Yeah.

MR. MATTIS: Plus the Overseas Chinese Affairs Office.

VICE CHAIRMAN BARTHOLOMEW: Plus, plus, plus, plus, plus, plus.

MR. MATTIS: Plus, plus.

MR. STOKES: Just a whole--yeah.

MR. MATTIS: But the ones that can actually arrest you and detain you and make your life directly miserable when they show up to you face to face are the Ministry of Public Security and Ministry of State Security.

MR. STOKES: Yeah.

VICE CHAIRMAN BARTHOLOMEW: I have time for one more question, which is as the Chinese companies are moving in and purchasing assets here in the United States, including hotels and hotel chains, should we be concerned about this as it's yet another way for the Chinese intelligence community to be acquiring information? The Waldorf, the Waldorf certainly is one of them, the first and biggest examples, but, you know, chains, chains across the country, hotel chains?

MR. MATTIS: I think that goes down to my comment in response to Commissioner Fiedler's question, how do you--sorry--Commissioner Wessel's question--are we flat-footed, and I think the issue is that there are simply too many things to prioritize to give us a sound answer. Where do you put that relative to a whole host of other things because of the resources that you would need to devote to come up with a concrete answer or how, if there is a

problem, you know, does it exist, and, two, if there is a problem, then how do you start to resolve it?

HEARING CO-CHAIR BROOKES: Thank you.

We have two commissioners with questions. Perhaps I could ask Commissioners Slane and Talent to give their questions, and then let the panel answer both of them at the same time in the interest of time.

COMMISSIONER TALENT: Well, I'll just, I know we're running out of time--

HEARING CO-CHAIR BROOKES: Okay.

COMMISSIONER TALENT: --so just one quick one. Mr. Costello said that he thought the Chinese were moving more towards a Russian style or approach, fewer operations or ops, but more prioritized and longer-term.

Do the other two of you agree with that, and do you think their system, what you've described is a pretty chaotic system to me, and I'm wondering whether, whether we can have any certainty that anybody is going to be able to enforce a change like that on the system?

COMMISSIONER CLEVELAND: I like the fact that you always make him go first.

MR. STOKES: Yeah.

MR. MATTIS: I think it--

COMMISSIONER TALENT: Oh, I'm sorry. You wanted Dan's question at the same time? Mr. Chairman, you wanted Dan's question at the same time?

HEARING CO-CHAIR BROOKES: Yes, please. I'm sorry.

COMMISSIONER SLANE: Thank you. Thanks for coming, guys.

My interest is what do we recommend to Congress to deal with some of these problems? And specifically it seems to me that we need to reorganize our counterintelligence efforts here in the United States, and you know reading the materials, almost all of the CI is done domestically. Do you share a recommendation that we should do that, and do you also share the feeling that we need to throw more resources at this, and that resources have been shifted from CI to counterterrorism to the detriment of what's happening to our country?

MR. MATTIS: Very quickly to Senator Talent's question, I think the ability to control these activities exists within individual systems, but there's no way across, you know, from the top to enforce discipline on every single one of them.

The Ministry of State Security probably has done a reasonable job of preventing "amateur hour" in going after U.S. targets given that we didn't realize how important they were until the last few years. So it suggests that they've kept the Guizhou State Security Bureau from doing things in the United States and leaving it to sort of more professional parts of it to do that kind of work.

The biggest complaint--back to Commissioner Slane's question--is from former officials, including the two that you'll be hearing from in the next panel, is that the level of Chinese effort far exceeds the level of effort that we're putting against them in a counterintelligence way, and I haven't met anyone who has been in this business who thinks otherwise or who has a position that's different than that.

As far as reorganization, again, it becomes a question of what is it that we're trying to stop because there are intelligence activities, there is a completely different kind of open source effort that involves recruiting talent, to collecting information, and there's also the effort to shape perceptions and public pieces, and these are all very difficult questions that basically rely on the same sort of resources, and there hasn't necessarily been clear prioritization

other than let's try to make some cases here or there.

MR. STOKES: I'll try and address the second question particularly. The reason why I deferred over to Peter is I know both John and Peter with the expertise so I defer to them. The one area I would--I wouldn't recommend taking a closer look at is sort of the spirit of legislation that was introduced earlier this year within Congress, specifically the Information Warfare Act of 2016.

If you define intelligence in the Chinese context, somewhat differently than the way we would define it, as very closely linked with influence operations, back during the good old days, in the Soviet Union days, there was something called active measures in which U.S. Congress has significant interest in. There were annual reports on Soviet active measures that were produced. There was an entire organization that was set up, I believe as U.S. Information Agency or others that was set up to be able to counter Soviet propaganda and disinformation.

Are the Chinese any more or any less intent on being able to shape public perceptions in a covert or clandestine way than the Soviets were? I would argue not, and I would say they probably are more ambitious than the Soviets were. And so this would be an area that I would recommend taking a much closer look at is taking a look at the challenges that the Chinese influence operations, how they're connected with their intelligence collection efforts, and taking a look at what can be done to be able to counter some of their efforts at inducing misperceptions among U.S., within the U.S. populism, policymakers.

MR. COSTELLO: Regarding the sort of Russian style approach, I think a lot of us have a tendency to forget that China is an oligarchy, you know. It's not, you know, they supposedly do have an executive, but I mean honestly their state is sort of three areas. It's the government, it's the Party, and it's the military. And the Party is sort of the central component in that.

Like I say, you know, their intelligence and security apparatus does resemble a hydra, and you're not going to be able to lop off the heads, but you can tame them and you can get them in line.

The question, I think the real, the heart of your question, and I think it's a real good point to make, is that this taming is only temporary, and it depends on who's holding the whip. It fundamentally doesn't change the institutional-like framework that allows the system to be like this to begin with. So I think it's absolutely right. I mean right now we may see a sort of Russian model, but it doesn't mean if Xi Jinping were to go out of power or some other sort of, you know, major change were to happen to leadership, that that wouldn't change because the institutional safeguards aren't there.

COMMISSIONER TALENT: Systems like this tend to, the only, when somebody like Xi consolidates power, everything seems, tends to focus on what he wants to devote his time and effort into, and there's only a certain amount of time that he's got; right? In other words, I'm saying how can he do that? How does he find enough trusted subordinates without the institutional sort of protocols that we have, and it's hard enough in our system for a president to get what he wants, right, but we have, we have protocols, we have methods to implement presidential directives.

In their system, they don't, and so I'm agreeing with what you're saying now, that I would expect bursts of this to happen as he or top leaders put effort into controlling and then inertially that to run down and the system to go back to a more decentralized approach?

MR. COSTELLO: Absolutely, and I think the military reforms are particularly important in this respect. I mean having the chairmanship of the Central Military Commission

historically has been a major source of power for Chinese leaders, and I think a lot of the reforms you're seeing right now are institutionalizing that sort of--are sort of reforming the military system to institutionalize, to have an institutional level of trust that what commanders say will happen.

And sort of address your second point, I mean Peter is absolutely right. I mean we have so many intelligence priorities, it's absolutely insane. And, you know, how do you sort of balance counterterrorism against counterintel, you know? I mean you could prioritize counterintel, but then you get one terrorism incident and one terrorism scare, and it's right back the other way.

I think one thing that we can concentrate on--and I haven't seen--I have seen these complaints from the IC and outside the IC--is we don't do a good job of open source. We do not do a really good job of understanding the baseline information that's out there, and this speaks to sort of the classification problems we have in the intelligence community.

We have a lot of--I mean I was coming to the intelligence community and then coming out. I denigrated open source. I was like why are you wasting your time? Now coming out and seeing what's available out there, there are a huge number of resources that are wasted looking at classified, you know, methods and sort of techniques to get information that's already out there.

I think we need to do a better job of looking at open source first and having that as a baseline to which we inform our intelligence processes rather than having our classified intelligence as the baseline, and then open source is there as sort of like icing on the cake. I think that's sort of the wrong way. That would require, though, a huge paradigm shift in the way we do intelligence. And I don't even want to think about how we'd even go about doing that. Well, I would, but--

[Laughter.]

MR. COSTELLO: --it's a much longer conversation.

HEARING CO-CHAIR BROOKES: Let me just ask you to answer this one last question, and it's a sentence, and I'm going to read it to you, and then I would like you to tell me what you think:

Chinese HUMINT intelligence operations are more or less active and more or less effective against U.S. targets currently? Are they more or less active or and are they are more or less effective against U.S. targets than previously?

VICE CHAIRMAN BARTHOLOMEW: Than when?

HEARING CO-CHAIR BROOKES: Than previously, at this point.

MR. MATTIS: More active and potentially more effective.

HEARING CO-CHAIR BROOKES: Potentially more effective. Okay. Because we know about cyber a lot. So I wanted to focus on HUMINT. I know--okay.

MR. STOKES: HUMINT broadly defined I would argue the Chinese are more active and more effective than we are.

HEARING CO-CHAIR BROOKES: Not than we are. Against U.S. targets. I mean are they more active?

MR. STOKES: Yeah.

HEARING CO-CHAIR BROOKES: Okay.

MR. COSTELLO: Regarding HUMINT specifically, I would defer to both Mark and Peter.

HEARING CO-CHAIR BROOKES: Okay. Because I want to differentiate

because we see so much cyber activity. Are they moving away from HUMINT towards cyber? You know, that sort of thing. So are they more active? That's--

MR. STOKES: Oh, they're symbiotic.

HEARING CO-CHAIR BROOKES: You think they're--

MR. COSTELLO: I think they're symbi--I think you got to, like cyber, HUMINT and open source are this symbiotic triangle that is just, that has turned into this sort of beautiful engine of intelligence for China.

MR. STOKES: I'd say SIGINT broader than cyber--your phone calls.

MR. MATTIS: And SIGINT is and cyber is the crutch of the shortcomings of the HUMINT system. It's answering questions that the HUMINT system can't answer right now and it's adapting to try to answer.

HEARING CO-CHAIR BROOKES: Okay. Good. Thank you very much.

Thank you very much for your rich and thoughtful testimony, and we'll conclude this panel and move on to the next one. Thank you.

[Applause.]

HEARING CO-CHAIR BROOKES: Ten minute break. Is that right? Yeah.

Clapping.

PANEL II INTRODUCTION BY SENATOR BYRON DORGAN

HEARING CO-CHAIR DORGAN: We'll ask people to be seated and begin the second panel. Thank you very much.

In the first panel, we described and discussed the structure, reforms, and capabilities of Chinese intelligence services, and this panel is a panel that will discuss Chinese intelligence collection operations and the implications for U.S. national security.

We will investigate China's espionage operations against the U.S. both in our country and abroad, and our panelists, two panelists, will consider the implications of these operations for U.S. security.

Michelle Van Cleave was appointed by President George W. Bush in 2003 to be the first person to serve as National Counterintelligence Executive, the statutory head of the U.S. counterintelligence. She was responsible for leading and integrating the counterintelligence activities of the FBI, CIA, the military services, and other federal organizations. Good luck as I think as I read these things.

MS. VAN CLEAVE: Fair enough.

[Laughter.]

HEARING CO-CHAIR DORGAN: But it was a very significant job, and Michelle Van Cleave was the first to serve in that very important position.

Upon leaving office, she joined the faculty of the National Defense University where she served until 2011, teaching a core course in homeland security. She's currently a Senior Fellow at the Center for Cyber and Homeland Security at GW University and a principal with the Jack Kemp Foundation, and I can't help but say that I served with Jack Kemp, and he remains in my memory one of the really terrific members of Congress that I had the pleasure of serving with, and I know you worked with him.

MS. VAN CLEAVE: Thank you, Senator. We share that view in common.

HEARING CO-CHAIR DORGAN: In addition, we have David Major with us today. Mr. Major is the founder and president of the Centre for Counterintelligence and Security Studies, which provides counterintelligence, counterterrorism, and security training for the government and the corporate sector.

He's a retired FBI Supervisory Special Agent and was the First Director of Counterintelligence, Intelligence, and Security Programs at the National Security Council at the White House. From 1988 until retirement in 1994, he was the FBI's principal representative in the national intelligence policy formulation process.

Both of you have had very, very significant posts at the top of our government in the issues that we care about. We appreciate your taking the time to spend some time this morning with us. We ask that you keep your remarks to seven minutes, and we also ask that--we understand that some people in the room have had difficulty hearing. We don't have a microphone. If you would speak up, we'd appreciate it very much. And Ms. Van Cleave, we'll start with you.

COMMISSIONER FIEDLER: We have microphones. Loud speakers is what we don't have.

HEARING CO-CHAIR DORGAN: Loud speakers is what I meant.

**OPENING STATEMENT OF MS. MICHELLE VAN CLEAVE
FORMER NATIONAL COUNTERINTELLIGENCE EXECUTIVE**

MS. VAN CLEAVE: Thank you for inviting me to be here with you this morning. You've asked me to address a number of questions about Chinese intelligence operations in the United States. I've prepared a written statement, which I hope has been distributed to you all, in an attempt to answer some of these questions. I would like to use my time with you this morning to talk about what, in my opinion, needs to be done. This Commission certainly is no stranger to Chinese intelligence operations, and as you all know--we read the papers, and hardly a week goes by without picking up yet another story about an export control violation or trade secret violation, most of these cases involving Chinese sources, and frankly with no end in sight.

It is worth reminding ourselves that the sweeping compromise of all U.S. nuclear weapons design information, back in the 1990s, remains unsolved to this day. We still don't know how it is that the Chinese were able to acquire all of that incredibly sensitive information.

There have been a number of major espionage cases involving China, but the one I would single out for your attention is the Katrina Leung "Parlor Maid" case. The damage assessment was done on my watch as the new head of counterintelligence. We were responsible for doing all damage assessments on espionage cases, and I can confirm that "Parlor Maid" was one of the most devastating espionage cases in U.S. history, that Ms. Leung's FBI handler for some 20 years was a conduit to giving her insight into virtually every significant U.S. intelligence operation against China.

Think about what the implications of that means, that the breadth and the depth of all the things that U.S. has done against the Chinese target are in question. At a minimum, U.S. intelligence needs to be wary of how China is using that understanding of our intelligence effort against them to hide what they are doing or to mislead us about their activities today.

More recently, I would note the arrest of a U.S. naval lieutenant commander, a SIGINT officer, in September of last year. His arraignment just last month on three counts of espionage and lesser charges is a reminder of this continuing threat.

And, of course, in addition to these espionage operations are the seemingly ubiquitous Chinese cyber operations against the United States. All of our weapons laboratories, Pentagon computers, communication systems, other sensitive networks are regularly targeted. And as you know, China has a policy of economic espionage against the U.S. by which it is feeding off our S&T base.

Your report last year took the U.S. government to task for its ineffective response to China's cyber operations, citing in particular the reach into OPM's computer records. The compromise of personnel information for 22 million people, mine among them, many of yours perhaps as well, or some seven percent of the U.S. population, is a rather staggering attack, and I would suggest that we have yet to face the full repercussions of this particular loss.

And why is that? Because OPM really is the lodestar. OPM is the lodestar because it is the keeper of all the personnel files containing all the detailed information on virtually everyone in the U.S. who has access to classified information. Those files contain all of their financial information, their employment history, their residences over the years, interviews with their friends and neighbors and colleagues, all kinds of insights into their health records, where they've traveled, who they know, on and on and on, all captured in those files. For any intelligence service, that is gold.

That information is gold for intelligence services looking for opportunities to

recruit, to identify potential people of interest, to find their vulnerabilities, and to exploit them., In addition, since these files also include records of movements, travel, connections abroad, there is concern, and for good reason, that by exploiting what can be pieced together from these files that U.S. intelligence operations abroad could be in jeopardy.

The bottom line is this. Chinese espionage in the United States is about to get much worse. And I would urge the members of this Commission to take this warning to heart and to engage your energy and creativity and talent to decide what in your considered opinion should be done. Much like war being too important to be left to the generals, the strategic counterintelligence question, what to do about Chinese operations against us, is, I would suggest, too important to be left to the intelligence community alone to answer.

Our different counterintelligence agencies -- the formidable work of the FBI in catching spies, and the work of CIA, and the work of our military services -- all have a tactical focus to achieve the mission that they have been assigned. Together they are not charged with answering the question: what are the threats to the United States government, to the United States as a nation and to our interests, and what should we do about it? That's not their job.

And I would suggest that national security planners, for the most part, have ignored this dimension of state power. When they think about strategy, in my experience, they just don't consider counterintelligence as a tool of statecraft, and yet I would suggest to you that it is, and it should be, and it should be considered that way when we think about what to do.

Now I would hold out a caveat, that in wartime, the enemy's intelligence capabilities are, in fact, factored into national planning, but not so much when it comes to broad national strategy. And I think that needs to change because it's not enough for the United States to be chasing individual spies case by case. The real national security challenge is how to put together a strategic counterintelligence program, one team, one plan, one goal, to degrade the capabilities of hostile intelligence services that are directed against us.

Now that may sound straightforward, but that is not how the U.S. counterintelligence enterprise is set up to work. It has three operating arms, as I've mentioned: the FBI, the CIA, and the military services. They have different missions and those are vital missions, but there is no common operating picture of what the adversary is doing. There is no common guiding doctrine to guide their work.

There is a lot of bilateral cooperation, but there is no national orchestration of U.S. counterintelligence effort against the adversary. The creation of the National Counterintelligence Executive, the position that I held in government, was created in part to address these kinds of deficiencies.

And when I served in that position, my office did a top-to-bottom review of in the resources, programs and activities across the U.S. counterintelligence community. We concluded that the U.S. counterintelligence enterprise needed to be reconfigured in order to be able to go on the offense strategically, to exploit where we can, and interdict where we must, with the purpose of degrading adversary intelligence operations against us.

President Bush issued a national strategy with this proactive reorientation at its heart. But I must report with regret that we were not able to make much progress in executing that strategy. The principal problem was this: while creating a national head of counterintelligence, the law that created the position that I held did not create a strategic counterintelligence program, the means by which this orchestration and integration of our counterintelligence activities could be accomplished.

And it's not because we don't have enough money. While, in my opinion, funding

for counterintelligence is puny relative to the cost imposed by these actions against us, that is not the core problem. We are getting about as much as we can out of our current counterintelligence enterprise. The problem is that we don't have a way of moving from working defensively at home case-by-case to taking the fight, as you might put it, to the adversary abroad. If we were to execute an offensive counterintelligence strategy, it would, in fact, begin with working the target abroad to understand how they're resourced, how they're positioned, how they're targeted, how they're used, what their vulnerabilities are, and how those vulnerabilities can be exploited.

And at home a similar kind of coordinated and community-wide effort would be involved in forestalling the inevitable penetrations of the U.S. government and working against the systematic targeting of our science and technology.

This is also true when it comes to cyber space attack. The most effective cyber space defense is likely to be a good offense. From a counterintelligence perspective, again, such an approach would mean getting inside of the attacker's intelligence operations to find out what they are doing in order to stop them or confuse them or otherwise misdirect them.

I would add that the Chinese clearly understand the advantages of linking cyber to human operations, as the last panel was discussing in its closing minutes, and our response needs to be equally agile.

But, again, to emphasize, the missing element here is a national program in counterintelligence to enable the integrated planning, orchestration and execution of strategic CI operations. I think that this kind of a mission would be a sharp departure, as I have described, from the way we usually do business, but there is no question in my mind that our nation's very talented CI professionals can do this job provided the leadership sets the right course.

**PREPARED STATEMENT OF MS. MICHELLE VAN CLEAVE
FORMER NATIONAL COUNTERINTELLIGENCE EXECUTIVE**

**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

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."

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.

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 students⁵ and academicians, all potentially extend the reach of Chinese intelligence into the core structures of

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/>

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, 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,

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>

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, 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

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

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

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 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 --

¹⁴ <http://www.zdnet.com/article/linkedin-serves-up-resumes-of-27000-us-intelligence-personnel/>

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,

to acquire the controlled technologies they want, 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?

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.

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>

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 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 home²⁵, where our CI effort has been concentrated on counterespionage investigations, (*i.e.*, on violations of criminal statutes against espionage and

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.

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.

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-

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.

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.

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

³⁰ <https://www.ncsc.gov/publications/strategy/docs/FinalCIStrategyforWebMarch21.pdf>

³¹ <https://www.dni.gov/files/documents/ICD/ICD750.pdf>

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 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.*

³²<file:///C:/Users/Michelle/Documents/Documents/Earhart%20Project/Vignettes%20research/The%20Farewell%20Dossier%20-%20Weiss.htm>

* 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.*

**OPENING STATEMENT OF MR. DAVID MAJOR
FOUNDER AND PRESIDENT, CI CENTRE**

MR. MAJOR: Thank you, Senator and Commissioners.

I'm very happy to be here to talk about one of my favorite topics. From a background standpoint, I've been looking at China for at least 45 years, and I know I don't look that old, and thank you for recognizing that. But I've been looking at the development of our program and trying to deal with China from a very long period of time.

First of all, I couldn't agree more with what Michelle said. I was at the White House when she was at the White House. That's where we first met, and we were talking about needing a strategy back then, and this was during the Reagan administration so this is not a new argument, but it's one that's been very difficult to sell.

One of the things in the counterintelligence world, which is always important but often forgotten, is this is one discipline, which is a strategic weapon, but you cannot not do counterintelligence, and sometimes we try not to do that. We try to put it away.

China is a good example of that. China has always been an enigma for American counterintelligence. We have a much better handle today with what China does, but from the time when the PRC became a country in 1949, we had no sources in China, we didn't know what they were doing, and they went through so much turmoil, internal turmoil, the entire Western community was blind as it related to China.

China never even began to open up to this until 1972, and that's when they went to the United Nations. At that time, the FBI started looking at China. We had no idea of how China operated, and we look, took an approach towards China which blinded us for a long time, and that is we took the Western view. We looked at--we thought they might spy the way Russia does. They still don't spy the way Russia does. They spy completely different than another service. So whether we're talking about operating in the United States or Canada or Europe, all the countries today are becoming very concerned about China because they have become more aggressive, and they will become more aggressive.

It wasn't until 1979 that when we finally established diplomatic relations with the Chinese that we began to get some handle. But we continued to look at China operating in the Western model. So we would look at intelligence officers, trying to find them in embassies to have meetings, and they weren't doing it.

We now know that they were doing it in China to some degree, but they weren't aggressive at that timeframe. It was in the 1980s, it was the mid-1980s, when the 863 Program was established to steal technology, which really began to drive them, that we saw, began to see a systemic change inside of what China was doing.

Now from 1949 until the year 2000, we only identified five cases in the United States that you could say were Chinese espionage. Now I say "that you could say" because it's difficult sometimes to find the footprint of the government in China cases because we may see their intelligence service, the MSS, but they also spy two other ways: (a) they use illegals, just the way the Russians do, like the show "The Americans." They do that. They call them bottom-sinking fish, which is an interesting term.

We have some cases like that where they send people to be here to integrate into our society but in a way that's a lifetime commitment. Come here and maybe you can go into the second generation of doing it. There's a great book on this called Daughter of China that explains this process. This young woman who was a lieutenant in the PLA talks about this

process and how she was being recruited to do that. So they do have illegals.

They do have some people working out of embassies, but they're not targeting, assessing and recruiting the way the Europeans do or the way the United States does it. What they have is building relationships. If they can, those relationships are culminated or expanded in China where it takes place. One person said in the first panel there's no dead drops. That's true. The tradecraft of China is a couch, usually a couch in China. That's what it looks like when you do it, but they still do recruitment.

Now for a long time there was a theory in counterintelligence community that China was stealing sand one pebble at a time. You probably heard that lecture. That's turning out not to be true. They may have done that because we didn't know what they were doing, but as they become more aggressive, we now know that while we only had five cases, it is the number one target of American counterintelligence with China, and the number now is up to 160 and counting.

So since the year 2000 until today, there's been 154 American cases. Now sometimes I can't say that's the MSS that's doing it or the PLA, their intelligence service, because it's hard to say. And one thing we do know about China intelligence is they will steal anything. And if you look around at the cases, they will steal anything of value.

And you're talking about, well, now that they spent this money to do this, how are they going to exploit it? I believe that they get it and say, well, can we use this? So they will steal technology, they will steal information, they will steal classified information, corporate information. Most of the cases we've seen are in the corporate world. What is interesting because in the corporate world, the expansion is going into like biomedics and a variety of other different kinds of information that's not military related.

But one of the great cases, recent cases, I think, is the stealing of corn in China and the rice that took place in the United States. That's interesting. Think about that. China wants to steal rice, but they were doing it for the peptides. It was all about science. So you probably know that case.

Someone made a comment in the first session about Duffie, Glenn Michael Duffie. Actually that's a very disturbing case for the people in our business because if you pay \$70,000 for nothing, \$70,000 just to try to get inside American intelligence, that has all kinds of implications if Duffie wasn't going to go to the CIA and have polygraph.

Now he wasn't caught because of the polygraph. It was a way to catch him, but it wasn't the way they caught him. There's a different nuance there. They obviously knew he was a spy when he went in to take the polygraph, but the fact is that if they'll do that for \$70,000, what about all the other Duffies of the world who get approached?

That's why the Bureau made a wonderful video, "The Game of Pawns," trying to educate students. Someone asked a question in the first session: why don't we go to talk to academia and warn them? I've been trying to do that for years. And they don't want to hear it. When I was in Baltimore as a supervisor, I had a dean tell Chinese students when they arrived in Johns Hopkins University, the FBI may come and talk to you, you have no obligation to talk to them, and I will stop them from talking to you.

Well, when I found out about that, I went out and had a "come to Jesus" meeting with the dean because I said, Dean, you can say that, but I'm still going to try to talk to your Chinese students whether you say it or not. But that's the kind of response we had. Then later Johns Hopkins sends some professors to China, and they were targeted, and they tried to recruit them there. We wanted to brief the professors going there, and we weren't allowed to brief the

professors there.

So we set ourselves up for compromise in these kinds of policies we set up if we don't take it serious. Now today we are--China, as I say, is the number one target of the counterintelligence community. Everybody is now talking about China, and they should talk about it because it is a great concern for us.

A couple other comments, if I could, based on the first session, and I'll stop. Someone asked about contractors is a problem. Contractors are no more or less of a problem than anybody else. In classified area, of all the people who have been charged with a crime relating to the compromise of classified information, only nine percent of them are contractors. 91 percent of them are govies-- people that were charged with. That's a fact that you should know.

And my paper talks a lot about Taiwan, and you made a great comment as it relates to Taiwan, and if I have a chance in your questions, I'd like to talk some more about Taiwan and how successful they've been and why they're successful there. I don't believe we should stop selling to them, but I do think that--I didn't understand what you were saying.

COMMISSIONER FIEDLER: That wasn't my question. It was whether we should trust them?

MR. MAJOR: Yeah. We should trust them--no. But the fact is that what they've been doing as the underbelly for us against Taiwan is a great concern because we have sent them classified projects. Ask people from Lockheed Martin, which had a major program which was compromised by them. But they have 54 spies out of ROC, and they're very, very senior people, and I listed them to you in the paper that I've given to you and what the positions were.

So with that, we can open up the questions.

**PREPARED STATEMENT OF MR. DAVID MAJOR
FOUNDER AND PRESIDENT, CI CENTRE**

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

Hearing on Chinese Intelligence Services and Espionage Operations

June 9, 2016

Mr. David Major

Founder and President, CI Centre

What intelligence collection operations with national security implications for the United States is China running outside of the United States, and how effective are these operations?

1. What types of intelligence collection operations targeting the United States does China run in foreign countries?

Understanding and discussing Chinese intelligence collection operations requires a broad and in-depth explanation. The CI Centre has a three to five day, 8 hours a day seminar to explore this complicated issue. Accordingly, it is problematic to even begin to try to answer this question in a satisfactory manner in a short briefing. Since the establishment of the Peoples' Republic of China (PRC) in October 1, 1949, Western intelligence and counterintelligence services have been working to answer this question. Only recently has a model emerged that begins to provide a satisfactory picture of PRC intelligence operations. The PRC conducts worldwide intelligence operations, both in the United States and outside China in a similar manner, but different than the USA and European model of intelligence collections. China has an extensive CYBER, SIGINT and IMINT collections capability that is land, sea and space based. The Western intelligence human intelligence models involve professional intelligence services who employ professional intelligence personnel who are centrally controlled and directed. The intelligence services establish collection needs and information requirements and dispatches the intelligence professionals under diplomatic cover to foreign countries to target this information. Intelligence Services also dispatch intelligence professionals with no diplomatic projection to established cover in foreign countries to meet collection requirements. These types of collection platforms are called "Non-Official Cover officers" NOCs, or illegals but the PRC refer to them as "bottom sinking fish", and they may be dispatched for the person's life time.

In a "normal" espionage world, nations use their intelligence services to collect information based on tasking requirements. If successful the collector then delivers the information to the tasking consumer.

The PRC, however, may or may not use its intelligence services to collect targeted information. In the PRC model collection can be conducted by the consumer so if no intelligence service is used,

three important characteristics emerge. The consumer becomes the collector, a “relationship” is developed with the information holder and the collection-consumer. This is an overt, sometimes social relationship which can be used for intelligence collection without the efforts of the intelligence services and is not centrally controlled.

Targeting of the Republic of China (ROC), (aka Taiwan, Formosa) is an exception to most of the “rules” of Chinese intelligence. This target is essentially the area of operation exclusively of the Ministry of State Security and the PLA and intelligence is not privatized or decentralized. Since 1979 when the PRC opened up to the West and allowed its citizens to travel outside China and foreign nationals to visit the PRC, extensive contacts have been established between PRC nationals and the West. These contacts are all used by PRC intelligence collectors to target potential sources and establish relationships that may be exploited for intelligence collections. PRC intelligence will target and exploit PRC college students overseas and foreign students studying in China, trade and cultural delegations, and attempt to first identify any ethnic Chinese (Han) that may be in the position to “help” China.

Obligations, roles, and relationships are central issues used by Chinese intelligence collectors in most Chinese intelligence espionage operations. Human collection operations will in general be very slow in developing and visitation to China is almost always seen. It is in China that targets are “pitched”, followed by tasking and debriefing of sources. The approach or pitch in the majority of the cases is “can you help China?” just a little. Unlike other services that are looking for “bad people” to do “bad things”, China is looking for “good people” to do “bad things”.

PRC operations tend to have preferences and prejudices toward ethnic Chinese (Han) to target for recruitment and a Xenophobic attitude towards foreigners. Thus, searching out Han within foreign countries is one of the first steps in the PRC collection process. The approach taken is to appeal to the pride the target may have in Chinese history and accomplishments, coupled with an articulated duty to help the “Ancestral Lands”. The emphasis is to appeal to the target’s pride in China and its history. The appeal is that the PRC is not a 3rd World or second-rate country or not a “tin pot village”. The approach is not necessarily pride in the PRC, but pride in China.

Three important concepts are observable in essentially every PRC human collection operation targeting Han. They are guanxi, face, and shame vs guilty. These are not seen in the USA/European intelligence model. China is a shame culture not guilty culture. The West is a guilty culture. Guanxi is paramount and essentially means all relationships are about obligations. If a Han person has a relationship with someone, that person will have an obligation to help the other individual in the relationship. To refuse an obligatory request is to lose face and to lose face is to be shamed. Guanxi is the engine that drives PRC intelligence operations and thus the best intelligence is personal; friendship based on transaction contacts with a network of contacts. Thus personal contacts are the best mechanism to solve problems or collect information. It is about not standing in line but going through the back door through relationships. The concept of “Face” requires one to honor obligations. Failure to try to meet those obligations results in loss of face. Loss of face brings dishonor to the family and not the

individual resulting in shame. This the obligation to help is evoked in operations. Shame is an external motivator and the context can be more important than content. Simply put “A sin unrevealed is two thirds revealed.”

Li Fengzhi, a former Intelligence Officer of the Chinese Communist Party’s (CCP) Ministry of State Security and defector to the USA advised publicly that the “CCP/MSS has spared no manpower and resources, to send many agents to the West and develop informers”. He has advised that “the CCP uses members of overseas Chinese communities, and Chinese students and scholar associations to work for the regime—in the name of serving the Chinese nation.” Li also said that “there is a written principle in the Ministry of State Security that says agents are allowed to appear to be anti-CCP as long as their goals are to protect the CCP’s greater interests.” Overseas Chinese is a term that means anyone who is ethnically “Han” and happen to not live in China. Culturally China will still see these Han as Chinese even if they have lived in China.

The backbone of today’s PRC strategic intelligence collection program is the “863 Program” initiated in March 1986 following four Chinese scientists' suggestion that aimed at making breakthroughs in some sophisticated fields of science and technology to which late PRC leader Deng Xiaoping had given his nod. The 863 program or State High-Tech Development Plan is a program funded and administered by the government of the People's Republic of China intended to stimulate the development of advanced technologies in a wide range of fields for the purpose of rendering China independent of financial obligations for foreign technologies. This long term program was to reduce the PRC technology gaps by targeting and combining military use with civilian use. The essence of the program was to use other countries’ technologies to reduce its own manpower and other resources. A key figure in pushing for the establishment of this strategy was Tsien Hsue-shen, founder of the Chinese ballistic missile industry, father of the Chinese aerospace industry, and builder of the Chinese nuclear industry. The backbone of today’s PRC experts were trained by Tsien after they finished their education. He coached, advised and goaded them to do their best. He was like a demigod, an aloof and awesome figure in China, as he was a “U.S. trained” expert. He taught others how to scrutinize American research journals and other open literature to estimate the level of aeronautical developments in the U.S. defense industry. He changed educational philosophy in military circles to “study the book and read English”. On October 16, 1991 Tsien was awarded the “State Scientist of Outstanding Contribution”, the highest honor for a scientist in PRC.

Today’s collection operations emanating from the PRC have been aggressive in many technological areas. Classic national intelligence “espionage” cases, economic espionage, trade secret theft cases, and technology cases have been identified and lead to legal action in the USA against 160 individuals. It should be noted that 154 of these cases have all surfaced since 2001 (the last 16 years). Numerous Western countries have followed suit with the USA and characterize the PRC as the most aggressive intelligence collector from HUMINT and CYBER attacks.

2. Outside the United States, which U.S. government national security decision making bodies; defense industrial actors; weapons, platforms, and systems; and operations and planning

centers does China target or seek to target with espionage operations?

PRC strategy of “Unrestricted Warfare”

In 1999 two PLA Air Force Colonels and Political Officers published a PRC strategy of “Unrestricted Warfare”. This eventually became public and it is informative to address this question. Some have argued the book was not a blueprint for a “dirty war” against the West but a call for innovative thinking on future warfare. Others have set forth the premise that this was a call for the doctrine of total war. It outlined the strategy that the PRC is preparing to confront the United States and its allies by conducting “asymmetrical” or multidimensional attacks on almost every aspect of our social, economic and political life. This new PRC form of warfare borrows from the ancient wisdom of Sun Tzu and his doctrines of surprise and deception. It also employs civilian technology as military weapons “without morality” and with “no limits” in order to break the will of democratic societies. The 12 targets of this strategy are:

1. Financial Warfare which means entering and subverting banking and stock markets and manipulating the value of a targeted currency.
2. Smuggling Warfare which means sabotaging a rival country’s economy by flooding its markets with illegal goods and jeopardizing a local economy by flooding the market with pirated products.
3. Cultural Warfare which means influencing the cultural biases of a targeted country by imposing your own cultural viewpoints.
4. Drug Warfare which means flooding illicit drugs across national borders and breaking down the fabric of a society through their use.
5. Media and Fabrication Warfare which means manipulating foreign media, either by compromising or intimidating journalists or getting access to another country’s airwaves and imposing your own national perspectives.
6. Technological Warfare which means gaining control of or having an edge in particular vital technologies that can be used in both peace and wartime.
7. Resources Warfare which means gaining control of scarce natural resources and being able to control or manipulate their access and market value.
8. Psychological Warfare which means imposing one’s national interest by dominating a rival nation’s perception of its own strengths and weaknesses.
9. Network Warfare which means dominating or subverting transnational information systems.
10. International Law Warfare which means joining international or multinational organizations in order to subvert their policies and the interpretation of legal ruling.

11. Environmental Warfare which means weakening or subjugating a rival nation by despoiling or altering its national environment.

12. Economic Aid Warfare which means controlling a targeted country through aid dependency.

Chinese Soft Power in Africa

During the Cold War, the USSR and USA were both heavily invested in the Africa Continent as a number of civil wars of independence served as surrogate for the communist or Western nation's competition. Intelligence collection and covert actions by both countries and their allies were rampant throughout the region. When the Soviet Union collapsed in 1991, both countries withdrew much of their diplomatic and intelligence commitments to the continent. The PRC, which had always had a presence in the region, did not withdraw their presence. The past 25 years has seen a rise of soft power on the African Continent. Unlike the USA, whose strategic goal was to spread democracy in the African emergent countries and the Soviets who wanted to spread communism, PRC wanted to win influence. "Soft Power" refers to a nation winning influence abroad by persuasion and appeal rather than by threats or military force. Simply put, China deploys soft power in Africa very prudently. China projects soft power by building visible infrastructure projects on the continent not by trying to control the form of government in the countries. The PRC has invested in projects such as the `Uhuru` Tanzam Railway project, that links Zambia to the Indian Ocean, and to building for free the African Union's new gleaming skyscraper headquarters complex in the Ethiopian capital of Addis Ababa. Some of these countries have no espionage laws which provides a "free fire zone" for espionage collection by the PRC. In Angola the PRC has granted the country a 5 billion dollar investment to expand and diversify the economy. Reconstruction finance mainly benefits Chinese companies who are engaged in at least 70% of Chinese- financed reconstruction work in Angola. Accordingly, the security service in many of these countries are reluctant to examine PRC intelligence collection and influence in their country.

Chinese Soft Power in Latin America

Soft Power is also a concern in Latin American as set forth in the Council on Hemispheric Affairs July 20, 2015 report entitle "Big Dragon on Campus: China's Soft Power-play in Academia." As set forth in this report:

"Over 400 Confucius Institutes established in schools across 115 countries. Officially, the Confucius Institute (CI) is a non-profit educational initiative which partners with schools across the globe to provide Chinese language instruction, scholarships for students to study in China, and to promote greater understanding and appreciation of Chinese culture. However, the organization's close ties with China's communist government, the sometimes ideological nature of its lessons and its efforts to enforce China's political positions, have raised concerns that the organization's intentions may be less about promoting Chinese language and culture and more about expanding

China's political influence globally and spreading the Chinese Communist Party's (CCP) ideology."

"The CIs' trend of promoting the CCP's positions on major political issues to students should also be of concern in Latin America and the Caribbean.... The Confucius Institutes, headed by incumbent politicians, are not apolitical organizations. Their goal is to expand China's soft power and present a positive, sanitized image of China, or as one professor put it, one of "pandas and chopsticks." The nature of the CCP's rule and the censorship and political repression it practices should not be overlooked, especially in education. Thus, greater scrutiny should be applied to the institute's practices in the region"

An example of China's soft power success occurred in Panama when the National Assembly has based a bill making the teaching of Mandarin compulsory in all schools in recognition of China's growing importance in the world economy.

3. How does China's infiltration of the governments and or defense industry of U.S. allies and partners, such as Taiwan, Japan, South Korea and Australia, affect U.S. national security? How does China's infiltration of the systems of U.S. allies and partners, such as Taiwan, Japan, and Australia, have a direct or indirect effect on U.S. national security?

As set forth in Question 1, targeting of the Republic of China (ROC), (aka Taiwan, Formosa) is an exception to most of the "rules" of Chinese intelligence. This target is essentially the area of operation exclusively of the Ministry of State Security and the PLA and intelligence has not been privatized or decentralized. Taiwan is the "third rail" for the PRC, both politically and for intelligence collection. A reflection of this was admitted by the former ROC Premier Wu Den-yih that "Taiwan and China are engaged in a war without gunfire." According to the National Council on Foreign Relations:

"Beijing and Taipei sharply disagree on the island's status. The PRC asserts that there is only "One China" and that Taiwan is an inalienable part of it. Beijing says Taiwan is bound by an understanding reached in 1992 between representatives of the Chinese Communist Party (CCP) and the Kuomintang (KMT) political party then ruling Taiwan. Referred to as the 1992 Consensus, it states that there is only one China, but with differing interpretations, allowing both Beijing and Taipei to agree that Taiwan belongs to China, while the two still disagree on which is China's legitimate governing body. The tacit agreement underlying the 1992 Consensus is that Taiwan will not seek independence. "

One of the USA manufacture classified command and control programs code named "Broad Victory" illustrates the vulnerability of USA defense industry to PRC exploitation and impact on US national security. The following are the events surrounding this compromise.

The ROC defense strategy to protect the country from the PRC changed in 2000 when the Democratic Progressive Party (DPP) beat the long-ruling Kuomintang (KMT) to become leader of the Republic of China (ROC). The DPP inherited an army-centric military that had been designed over nearly 50 years of KMT rule to focus on the defense of the island's physical territory. The DPP feared this focus would turn Taiwan's densely populated cities into urban combat zones if conflict with China ever came, and instead decided to pursue "decisive offshore operations" and carry the fight to the Taiwan Strait that would employ air and naval power to carry the fight into the Taiwan Strait and, if necessary, to the mainland. The immediate obstacle for this strategy was Washington's reluctance to sell Taipei the types of advanced weapons systems necessary for such a defensive strategy after the U.S. promised to reduce its sales to Taiwan in a 1982 Sino-American joint communiqué. In the recent time period Taiwan pushed the USA hard for the release of new F-16 fighter aircraft and is awaiting delivery of Patriot PAC-3 air defense missile systems and P-3C Orion maritime patrol aircraft. All these technologies are targets of the mainland Chinese.

A major element of the new defense strategy was enhancement to command and control that the USA could provide. The Po Sheng ("Broad Victory") program was initiated, an umbrella project to modernize Taiwan's C4ISR capabilities, a system to integrate ground, naval and air forces with command centers that is being sold to Taiwan by Lockheed Martin. Po Sheng would give Taiwan its first national-level joint command and control capability to deal to deal with aircraft, maritime surface and land targets. It enables those platforms equipped with data-link terminals to share near real-time information and engage a target in a timely and effective manner. This program was compromised by both the MSS and PLA in Taiwan and in the USA by multiple high level espionage operations. ROC Army officer LO Hsien-che was recruited in Thailand where he was a military attaché. He was later promoted to Major General and placed in charge of the Po Sheng program which he compromised to the PRC. He was arrested in 2011 found guilty and given a life sentence in prison. It came out the MSS paid him over 1 million dollars for this technology. The Po Sheng program was also compromised by the PLA in the USA based espionage network run by PLA Intelligence Officer LIN Hong involving 9 individuals who were arrested. The nine arrested were: Chi Mak who worked as a defense contractor L3 Power Paragon and three members of his family, Greg Chung who worked for Rockwell International / Boeing, US Citizen Tai Shen Kuo and his PRC paramour Yu Xin Kang, Greg W. Bergersen an analyst with Defense Security Co-operation Agency and retired US Air Force LT Col. James Wilbur Fondren, Jr.

The PRC focus on the Po Sheng program shows its intense interest and progress in developing the capability to disrupt Taiwanese communications ahead of an attack. Taiwan's penetration by China affected what types of arms the U.S. was willing to sell to Taiwan, according to a former deputy defense minister.

The proven success the PRC has had publicly to penetrate Taiwan's military and intelligence community agencies has serious implication for US national security. Between 2002 and 2016, 56 individuals have been charged in Taiwan as clandestine agents of the MSS or PLA. There have been 23 espionage plots of which all but 6 involve more than one individual. Five (5) of the

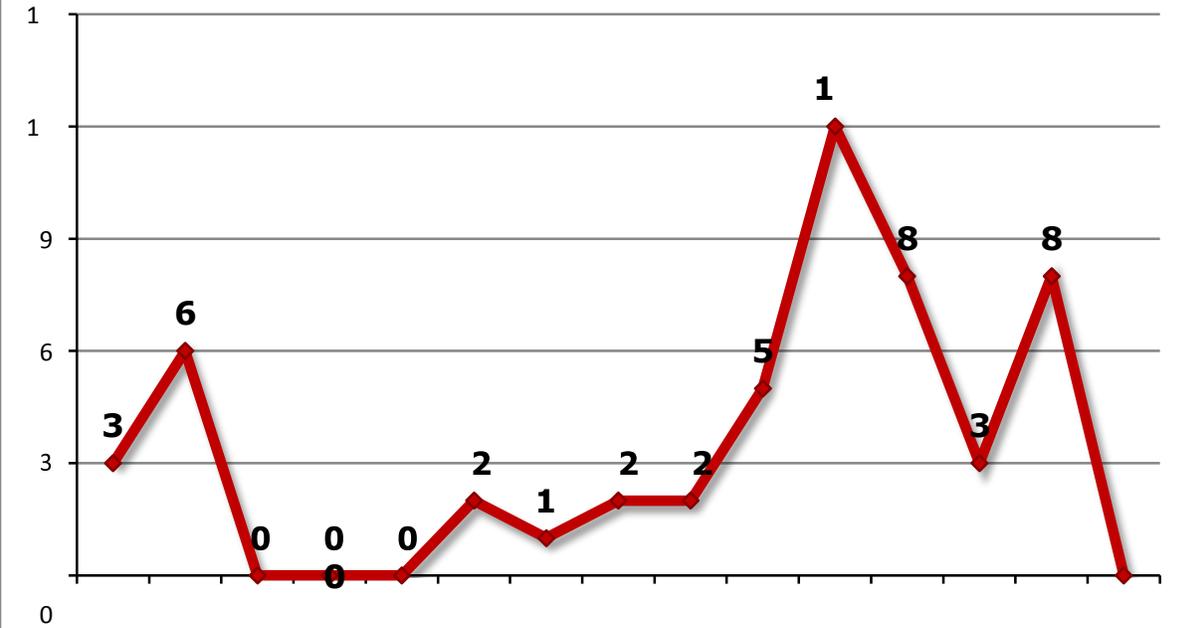
individuals arrested are flag officers. An additional 17 are officers in the Army, Navy, Air Force or Marine Corp and 15 are members of one of three ROC intelligence services.

As set forth by Jamestown Foundation China Brief November 7, 2014 Conclusions:

“The seemingly universal presence of a Taiwanese businessman or retired official with interests on the mainland suggests Chinese intelligence focuses on people who can serve as bridges to the intelligence target. These are people whose economic livelihoods and careers depend upon China, making the threat implicit when intelligence officers approach them.”

We have been able to identify 15 of the individuals recruited in PRC by the MSS or PLA when the Taiwanese national was working or visiting the mainland. Recruitment in third countries is rare, with one each recruited in Thailand, Bali, Philippines, and Shanghai. The PRC intelligence service relies heavily on their recruited Taiwan agents recruiting sub-agents and creating networks. At least 50% (26) individuals were recruited into espionage for the PRC by a co-worker, friends, family members or relatives. Interestingly, this matches what the USA counterintelligence community has observed with 42% of espionage subjects being recruited by co-workers, friends, and family members or relatives.

56 Agents of the PRC Identified in Taiwan



- a) How does China’s infiltration of the systems of U.S. allies and partners affect U.S. alliance stability?
- b) How does China’s infiltration of the systems of U.S. allies and partners affect U.S. willingness to transfer advanced defense technologies to these countries?
- c) Describe unilateral U.S. efforts and joint efforts by the United States and allies and partners to deter, track, prevent, or mitigate the impact of Chinese espionage in allied and partner countries. How effective are these efforts? Provide examples if possible.

There have been 56 Taiwanese nationals arrested in the past 14 years (2002 to 2016) that were involved with 23 PRC espionage plots to accrue the most significant technology and intelligence from the ROC’s military and all three intelligence services. Much of this technology was developed by the US defense community in the United States and sold to Taiwan. Justifiable concerns about the security of U.S. defense systems sold to Taiwan is a byproduct of this espionage activity. It is noted however that during the period 2001 to 2016 154 individuals arrested in the USA were involved in providing sensitive information and/or technology to entities in China. Thus PRC “espionage” is a problem and reality for both the ROC, the USA and the world as a whole. Taiwan has made efforts to improve security—including trip reporting and

routine polygraphs for personnel with sensitive access as well as boosting its counterintelligence staff. It is hoped that both countries are openly sharing damage assessments to help make way for improved U.S.-Taiwan counterintelligence cooperation. Knowing the degree of severity of Taiwan's espionage losses, the U.S. government will assume the worst case in spite of the many questions that could be raised about how much damage each spy did, such as whether technical information was transferred via documents or orally. If the USA begins to slowdown or stop the transfer of needed technology and information with Taiwan for fear of espionage loss then the PRC wins and Taiwan is doomed.

History has repeatedly validated the known counterintelligence truth that security/countermeasures do not stop espionage, it just slows it down. The continuation of an aggressive effort to penetrate the PRC collection capabilities and successfully run human source is the key to success. Innovation and risk taking operations will lead to successful operations like the ones set forth below

4. How effective are U.S. actors in deterring, tracking, preventing, and mitigating the impact of these espionage operations? Provide examples if possible.

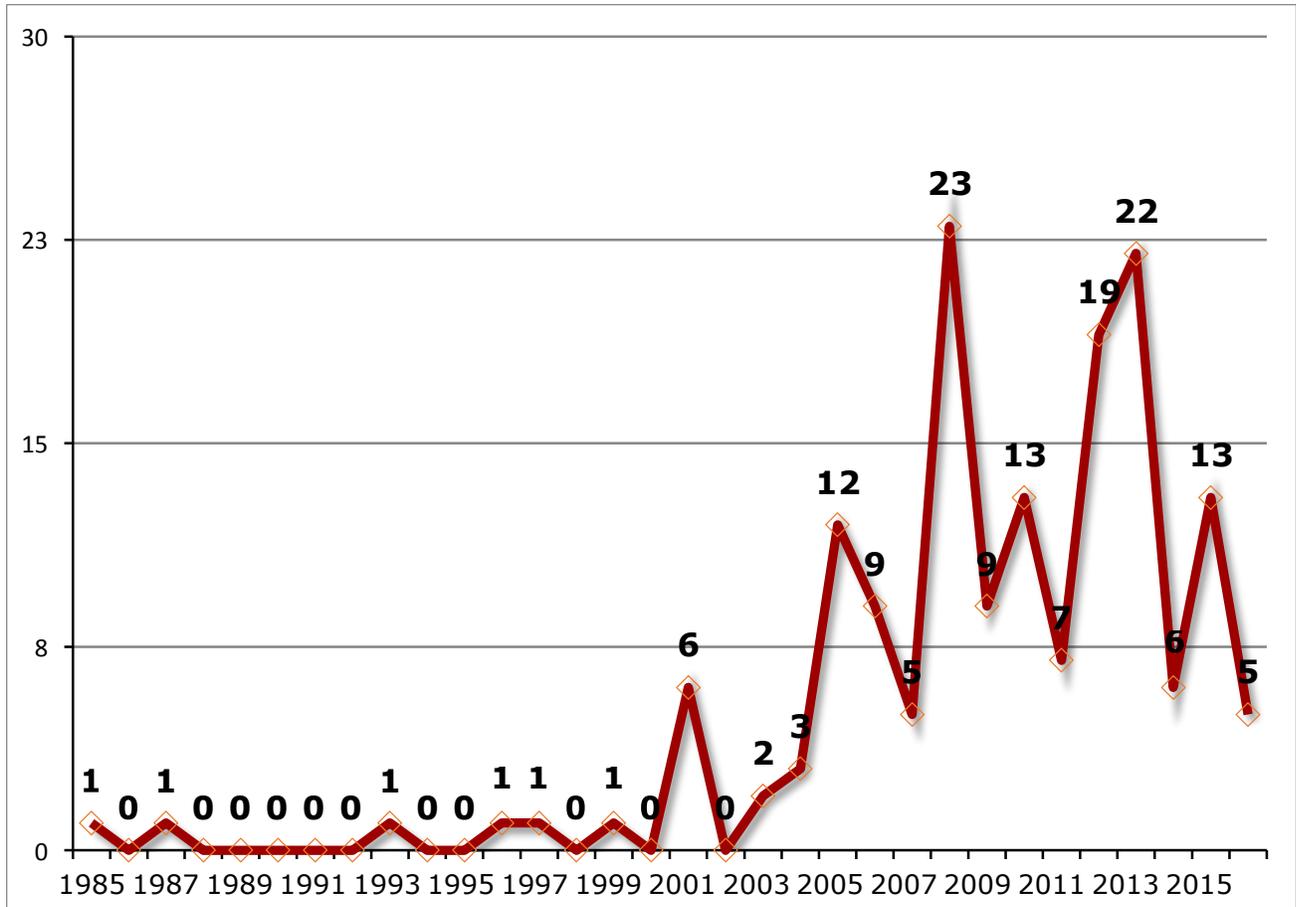
The PRC intelligence services were an enigma for the West and USA counterintelligence communities since the formation of the PRC on October 1, 1949. China was closed to the West's intelligence community until the PRC was recognized to represent China in the United Nations in 1972 and opened to the West with diplomatic normalcy with the USA in 1979. The West approached the PRC looking for the Western intelligence model; active intelligence officers under diplomatic cover targeting, assessing, recruiting, and handling recruited agents. Since this is not the method used by the PRCIS, USA failed in the mission to deterring, tracking, preventing, and mitigating the impact of PRC espionage operations. In 1981 this began to change when in Beijing a PRC MSP officer Yu Qiangsheng initiated contact with the US Embassy in what was an MSP approved recruitment operation against a CIA Officer assigned to US Embassy in Beijing. Yu used this as cover for action and in fact volunteered to provide secret information to the CIA. This was the first penetration of the PRCIS (the MSP will be renamed to the MSS). He was assigned the code name "Planesman" and provided the lead to identification of the longest run espionage in USA history CIA employee Larry Wu-Tai Chin. Yu defected to the USA in October 1985. With the implementation of the PRC 863 program in 1986 the Chinese became more aggressive and the Western counterintelligence service began to understand how the PRCIS operated. With the collapse of the USSR and end of the Cold War, the PRC moved from the second CI priority target of USA to number one. During the years 1985 to 2000 only 6 individuals were arrested for being involved in Intel collection for China. In October 11, 1996 the USA Congress passed the Economic Espionage Act of 1996 which provided a new tool to investigate and neutralize the intelligence activities of the PRC. PRC is currently the most aggressive intelligence collector and 154 individuals have been charged with intelligence collective.

In June 2012 it became public that in early 2012 an MSS Private aide (private secretary) to the Second Vice-Minister of MSS Lu Zhongwei was arrested for being an agent of the West. Lu

Zhongwei is one of the most senior MSS officials in the PRC. The aide's name has yet to be made public. Sources have indicated that the aide revealed information on China's espionage network in the United States, including the names of numerous Chinese agents. Chinese media reported the arrest is part of the highest-level spy case involving the two countries since Yu Qiangsheng defected to the United States in 1985. This aide case may have been the source to identify the 56 nationals of Taiwan arrested as PRC agents between 2002 and 2016.

In 2014 PRC National Ling Wancheng defected to the USA when his brother became the target of a security investigation in the PRC. Publically Ling is considered the most valuable Chinese defector to flee to the USA. He is the brother of Ling Jihua, ex-chief of staff to former president Hu Jintao, who was formally detained on suspicion of "serious violations" of Communist party rules in December 2014. It is reported that Ling Jihua had stolen thousands of classified documents and handed them over to his brother, Ling Wancheng. Ling Wancheng is reported to have revealed to US details on Chinese procedures for launching nuclear weapons, personal lives of China's leaders, arrangements for leadership security and security protection leadership compound in central Beijing.

160 AGENTS OF PRC ENTITIES IDENTIFIED IN USA 1985-2016



In addition to the efforts of the USA to penetrate the PRC intelligence collection community, the three Taiwanese intelligence services (National Security Bureau, Military Intelligence Branch, and Ministry of Justice Investigative Bureau) have also had success in human operation. The intelligence from these sources has also been exchanged with the USIC. The following are examples of significant ROC penetration of the PRC:

- 1999 2 PLA officers were court-martialed and executed as agents of the ROC from 1992-1999
 - Major General Liu Liankun who was head of the ordnance department of the General Logistics Department in the People's Liberation Army (PLA) for six years.
 - He provided important information to Taiwan including the locations of mainland missiles over a seven-year period.

- He was assisted by Senior Colonel Shao Zhengzhong
- 2003 PLA Major General Liu Guangzhi and a former president of the Beijing-based Air Force Command College was arrested
 - Liu was reportedly recruited by a former colleague surnamed JIA, at the Air Force Command College.
 - JIA worked for Taiwan after he left the PLA and joined a company owned by a Taiwanese named Li Yun-pu, a former colonel in Taiwan's MIB.
 - It was reported Liu turned over significant information to Taiwan about missile deployment, training and other key facts.
- In 2004 the PRC announced that it had detained 24 Taiwanese nationals in the PRC and 19 mainlanders as spies for the ROC and all had confessed. Very little detailed information is available to validate this report or identify the individuals detained.
- 2005 WO Weihand and GUO Wanjun were arrested in the PRC as spies for the ROC and both were executed in November 2008. WO was born a PRC national, became a medical doctor and citizen of Austria. He was recruited by the ROC MIB in 1989 and recruited sub-agent GUO in China. GUO was a PRC missile expert and provide WO information about China's strategic missile program.

5. Please rank China as an intelligence threat to the United States.

The PRC today is the most aggressive intelligence threat facing the United States. Their combination of technical cyber-attacks and exploitation coupled with a philosophy to use human intelligence to steal national defense information from the US Government, economic and trade secrets from the private sector and technology diversion to steal "anything of value" is a significant counterintelligence challenge. In the wake of the USA success in the Gulf war of 1991 the PRC observed the US dominance of the digital domain and embarked on a cyber warfare and collection strategy to dominate this venue in the future. Investing billions of dollars and a vast commitment of manpower the PRC has become the greatest threat to the USA in the digital world. Senior USA officials have declared that today there are two types of Government and private entities, "those that have been penetrated by the PRC or those that have been penetrated and do not know it." This aggressive collection posture is enhanced by a human "espionage" capability that has both a centralized collection strategy using their professional intelligence services (MSS and PLA) and an authorized decentralized nonprofessional cadre. PRC aggressively exploits academia in the USA and overseas using visiting scholars and PRC national students to identify and assess potential sources of information. In addition, the Chinese MSS and PLA aggressively targets students, scholars and businessmen visiting the PRC. This is

complicated by the willingness to use large sums of money to potential sources to apply for employment in the US Government. This technique surfaced in 2010 with the arrested in the USA of Glenn Shriver who was paid \$70,000 just to apply to the US State Department and CIA. This has significant implications and is unprecedented in the “espionage collection” process to pay a source for just trying to join and organization.

The long term approach of the PRC intelligence collection strategy was set forth by former PRC Deng Xiaoping, “observe calmly; secure our position; cope with affairs calmly; hide our capacities and bide our time; be good at maintaining a low profile; and never claim leadership.”

6. The Commission is mandated to make policy recommendations to Congress based on its hearings and research. What are your recommendations for congressional action related to the topic of this hearing?

The creation of a risk mitigation assessment center is essential if it has not already been established. A true axiom of the “spy business” is that the worst situation is to have no sources but the second worst situation is to have a successful source penetration. The reason is that when you have a good penetration you have to be taken advantage of the actionable information being provided but not to compromise the fact that you have actionable intelligence. This takes effectively and sufficient well trained personnel and management to recognize clues to penetrations, analyze available information and the ability to take actions to test these hypothesis and mount sophisticated actions to mitigate the threats. In budget reduction environment budget it is a simple solution to cut training and analysis. Organizations must fight the instinct to try to “buy” counterintelligence on the cheap.

The PRC must pay the price for an aggressive collection program by ensuring the West has the will to call out the PRC on its espionage, active measure and soft power initiative. Self-Censorship is an instinct that education can overcome. As set forth in the Council on Hemispheric Affairs July 20, 2015 report entitled “Big Dragon on Campus: China’s Soft Power-play in Academia”:

“The administrations of many universities hosting Confucius Institutes across the globe have self-censored their activities to keep from offending China. In 2009, North Carolina State University cancelled a visit by the Dalai Lama, after the director of the school’s Confucius Institute warned that hosting the Tibetan leader would disrupt ‘strong relationships we were developing with China.’ Sydney University in Australia also cancelled a lecture by the Dalai Lama in 2013. Australian politicians and activists charged that the university withdrew its support for the event ‘to avoid damaging its ties with China’ and to secure ‘funding for its cultural Confucius Institute.’ New South Wales MP John Kaye accused the University of selling off its “internal integrity” to ‘maintain close financial ties with the Chinese government.’ The university relented after protest and controversy. Also, in 2009 a district court in Tel Aviv, Israel, ordered the city’s university to reopen an art exhibit made by practitioners of Falun Gong, after the exhibit’s organizers sued. Falun Gong is a religious sect banned in China in 1999 and whose practitioners are still actively persecuted by authorities. The court found that the university’s dean closed the exhibit under orders from the Chinese Embassy. Judge Amiram Benyamini, who presided over the case said that the evidence did not support the dean’s claim that the

embassy's remonstrance did not influence his decision to close the exhibit. Judge Benyamini concluded that based on the evidence provided by the plaintiffs, the dean shut down the exhibit solely for fear of losing the university's CI and the associated funding. Russell explained that many universities see China as a 'sugar daddy' and regard partnering with it and establishing CIs as a 'pragmatic way of getting more funding.' The United Nations identified under-funded schools as one of the major 'overarching block' to proper education in Latin America and the Caribbean. With schools in the region in need of funding and the generous amounts of funding provided by Hanban, it should be taken into concern how much influence the CIs will have over their hosts in the region, and how likely it will be for students to receive an objective and realistic view of China and the CCP.

The US Government should consider offering first class advanced counterintelligence training to the three ROC intelligence agencies. This would include training on targeting and recruitment operations.

TAIWAN CASES		Arrested or Indicted	Conspirators	Rank	Branch	
2002	LIU	Chen-kuo	June 05 2002	Liu ring	Retired Captain	Army
2002	LIU	Yueh-lun	June 05 2002	Liu ring	Petty Officer First Class	Navy
2002	Wife of LIU Chen-kuo		September 26 2002	Liu ring	Civilian	Civilian
2003	HUANG	Cheng-an	August 06 2003	CSIST ring	Retired Major	Air Force/Chung Shan Institute of Science and Technology
2003	LIN	Wei	Sometime in 2003	CSIST ring	Civilian	Civilian
2003	YEH	Yu-chen	August 06 2003	CSIST ring	Civilian	Civilian
2003	HSY	Hsi-cheh	August 06 2003	CSIST ring	Civilian	Civilian
2003	TSENG	Chao-wen	November 11 2003	CHEN Hui-chiung	Retired Colonel	Military Intelligence Bureau
2003	CHEN	Hui-chiung	November 11 2003	TSENG Chao-wen	Lieutenant Colonel	Military Intelligence Bureau
2007	CHEN	Chih-kao	September 23 2007	LIN Yu-nung	Retired Special Agent	Ministry of Justice Investigation Bureau
2007	LIN	Yu-nung	September 23 2007	CHEN Chih-kao	Special Agent	Ministry of Justice Investigation Bureau
2008	WANG	Hui-hsien	June 20 2008		Retired Colonel	Military Intelligence Bureau
2009	WANG	Ren-bing	January 15 2009		Civilian	Presidential Office advisor
2009	CHEN	Pin-jen	January 15 2009		Civilian	Legislative assistant
2010	LO	Chi-cheng	November 1 2010	LO Ping	Colonel	Military Intelligence Bureau
2010	LO	Ping	November 1 2010	LO Chi-Cheng	Agent	Military Intelligence Bureau
2011	LIN	Po-hung	October 14 2011	WU ring	civilian	National Police Bureau
2011	WU	Tung-lin	October 14 2011	WU ring	civilian	National Police Bureau
2011	WU	Chang-yu	October 14 2011	WU ring	civilian	Central Police University
2011	LO	Hsien-che	January 25 2011		Major General	Army
2011	LAI	Kun-chieh	May 31 2011		Civilian	Civilian
2012	TSAI	Kuo-hsien	April 16 2012	WANG Wei-ya	Retired Captain	National Security Bureau
2012	WANG	Wei-ya	April 16 2012	TSAI Kuo-hsien	Retired Colonel	Ministry of Defense
2012	YUAN	Hsiao-feng	sometime in 2012	CHEN Wen-jen	Retired Lieutenant Colonel	Air Force
2012	CHEN	Wen-jen	sometime in 2012	YUAN Hsiao-feng	Retired Lieutenant	Air Force
2012	CHENG	Min-chun	April 18 2012		Left when he married PRC National	Military Intelligence Bureau
2012	CHENG	Lin-feng	July 11 2012	TSAI Teng-han	Retired Lieutenant Colonel	Army
2012	TSAI	Teng-han	July 11 2012	CHENG Lin-feng	Civilian	Civilian
2012	CHANG	Chih-hsin	sometime in 2012	CHANG ring	Retired Commander	Navy

TAIWAN CASES			Arrested or Indicted	Conspirators	Rank	Branch
2012	ZHANG	Xin	sometime in 2012	CHANG ring	Military officer unknown rank	Navy
2012	CHIEN	Ching-kuo	sometime in 2012	CHANG ring	Retired Lieutenant	Navy
2012	LU	Chun-chun	sometime in 2012	CHANG ring	Retired	Missile Command (retired)
2013	HSU	Chung-hua	February 4, 2013	CHANG ring	Admiral	Commander of Attack Squad
2012	CHIANG	unknown	Jan-12		Captain	Air Force
2013	CHEN	Chu-fan	February 28 2013	CHEN Shu-lung	Retired Lieutenant General	Air Force former Vice chief of Military Police command
2013	CHEN	Shu-lung	February 28 2013	CHEN Chu-fan	Retired Major	Military Intelligence Bureau
2013	KO	Cheng-sheng	March 13 ,2013	SHEN Ping-kang	Retired Vice Admiral	Navy Former Deputy Commander of ROC Navy
2013	SHEN	Ping-kang	March 13, 2013	KO Cheng-sheng	civilian	Australian Businessman
2013	HAO	Chih-hsiung	September 13, 2013	Hao Chih-hsiung Ring	Major	Air Force compromised ROC E-2 Hawkeye
2013	WANG	Han-liang	September 1, 2013	Hao Chih-hsiung Ring	civilian	Civilian Fugitive hiding in China
2013	WAN	Tsung-lin	September 1, 2013	Hao Chih-hsiung Ring	civilian	Civilian Karaoke Club owner
2014	LIAO	Yi-Tsung	March 10 2014	HU Kuang-tai	Col. (retired)	Marine Corps
2014	HU	Kuang-tai	March 10 2014	LIAO Yi-Tsung	Officer (unclear)	Marine Corps
2014	Unknown	Kuo	February 10 2014		N/A Focus Taiwan News Channel Journalist	N/A
2015	WANG	Tsung-wu	March 4 2015	LIN Han	Major (retired)	Military Intelligence Bureau
2015	LIN	Han	March 4 2015	WANG Tsung-wu	Colonel (retired)	Military Intelligence Bureau
2014	ZHEN	Xiaojiang	September 24, 2014			Fomer PLA Officer arrested in ROC
2014	HSU	Nai-chuan	November 2, 2014	ZHEN Xiaojiang	Major General (retired)	Army
2014	CHOU	Chih-Li	September 24 2014	ZHEN Xiaojiang	Col	Air Force
2014	SUNG	Chia-lu	November 2, 2014	ZHEN Xiaojiang	Pilot	Air Force
2014	YANG	Jung-hua	November 2, 2014	ZHEN Xiaojiang	Official	Air Force
2014	LEE	Huan-yu	November 2, 2014	ZHEN Xiaojiang	Businessman	Kaohsiung nightclub operator
2014	MA	Po-Le	November 2, 2014	ZHEN Xiaojiang	Pilot (retired)	Air Force
2014	CHAO	Tai-chi	November 2, 2014	ZHEN Xiaojiang	Major General (retired)	Unclear
2015	KE	unknown	April 10 2015	ZHEN Xiaojiang	Retired Air Force Officer unknown rank	Air Force
2015	LOU	unknown	April 10 2015	ZHEN Xiaojiang	Lieutenant Colonel	Air Force

PANEL II QUESTION AND ANSWER

HEARING CO-CHAIR DORGAN: Mr. Major, thank you very much.

Ms. Van Cleave, you mentioned the issue of globalization creating easy access to sophisticated technologies, and then you also in your paper talked about the lack of post-employment restrictions on senior government officials going to work for a, for example, a Chinese company or a Russian company, a global company but that is either Chinese or Russian. You didn't use those countries as an example, but I understand you, in fact, I think you described a press report of a senior official from the Department of Homeland Security or--yeah, I think it was Homeland Security, who went to work for a significant global enterprise, a Chinese telecommunications firm.

How would, how would you recommend, and perhaps Mr. Major, as well, how would you recommend addressing those issues? If someone, a senior person, does go to work for a foreign company, in this case, a Chinese company, they are still, of course, under the penalties of a law, you know, prevented from disclosing classified information and so on, but you're raising the specter of difficulty nonetheless of that kind of movement.

So how would you go about dealing with that?

MS. VAN CLEAVE: So, Senator, I don't recall putting that in my statement. However, I'm happy to speak to the question that you pose. The matter of post-employment restrictions is one that has equities on both sides. We have no wish to have talented people find themselves unemployable once they leave government service, but as you rightly point out, there are restrictions on what they can and cannot share and draw upon.

But to be sure, people who have access and understanding of sensitive matters are going to be interesting targets for recruitment for the access that they might be able to provide to others who may still be in place. So I think that as David alluded, it might be helpful if the FBI had an opportunity to provide awareness, counseling to individuals perhaps as they are leaving government about the extent to which they might be of interest to foreign governments for reasons other than their good looks.

So I think it could be useful to have that kind of sensitivity training for employees and contractor personnel as they are leaving government service.

HEARING CO-CHAIR DORGAN: Thank you. I found that on page 12 of the report, and it--

HEARING CO-CHAIR BROOKES: Testimony.

HEARING CO-CHAIR DORGAN: It was testimony you had given previously. Sorry.

MS. VAN CLEAVE: Oh, previous testimony.

HEARING CO-CHAIR DORGAN: That I read through.

MS. VAN CLEAVE: I'm sorry, sir. Yes, yes.

HEARING CO-CHAIR DORGAN: But it raises an interesting question, and also you raised the question of the whole globalization approach providing easier access to sophisticated technology--

MS. VAN CLEAVE: Right.

HEARING CO-CHAIR DORGAN: --which I'm sure is the case, but no one is going to march back globalization.

MS. VAN CLEAVE: No, nor would we want to.

HEARING CO-CHAIR DORGAN: Right.

MS. VAN CLEAVE: I think the benefits of what we call globalization are tremendous. At the same time, it is descriptive of an environment where we have to be thinking differently perhaps than we did in times past when there was less interaction. We looked at the old Soviet target, for example, and the interaction was rather controlled and limited. The world is not like that now, thank God.

HEARING CO-CHAIR DORGAN: Uh-huh.

MS. VAN CLEAVE: . . . But we need to appreciate that the environment that has resulted provides opportunity for a lot of movement, which gives U.S. intelligence broader opportunity as well let me hasten to add.

HEARING CO-CHAIR DORGAN: Right.

MS. VAN CLEAVE: Because of that, because of that kind of interaction. But also it means we need to be thinking more proactively about the way we understand foreign intelligence threats and what we're willing and able and ready to do about them.

As I have suggested, historically we haven't taken this on as a national mission, to our detriment. I think that, I hope that the time has come for a new national policy perspective that says, look, these kinds of foreign intelligence activities are harming us today, threaten to do more harm in the future, and we need to take them seriously, We would have an ability to better protect ourselves if we pull together key CI resources in a proactive national program to degrade foreign intelligence capabilities directed against us.

HEARING CO-CHAIR DORGAN: Commissioner Brookes.

HEARING CO-CHAIR BROOKES: Thank you.

David, what are the current trends in your mind in Chinese intelligence collection? I mean where are we going from where we are, from where we are today?

MR. MAJOR: Well, first of all, as we've talked about, I think they're getting more aggressive. They were, seemed to be handcuffed. They didn't care--they didn't want to be embarrassed, which is a part of the culture. But they don't seem to be worried about that anymore. So you see these cases that illustrate that there's almost a green light to run technology.

As I said, though, they will steal anything of value, and primarily what they're doing both here and in Canada and in Europe, they are targeting Hun people, people who are ethnically Chinese. There's a term in the Chinese culture which says a tree can grow to a thousand feet, but its leaves still fall to its roots, and they look and target people, first generation people. That's part of going back to China and being assessed when they're there. So these are the increases we're seeing in their activities, and that's something we have to address.

One comment about the last question if I might. You also could have a follow-up program for these people who have these jobs and have a friendly discussion with them after they left the government. They should be friendly about it, and the government come back in and talk to them and maybe kind of say what have you seen? And anybody ask anything? And if I knew that was coming, I would probably be reticent if someone came and tried to talk to me.

But I think it's not a bad approach to take that, but I do see it's increasing. As I said, the one thing that I'm struck with as we study this is that the targeting of anything of value is coming. One of the interesting trends is the targeting of technology. We understand that cyber is such a big problem, but we understand that 30 percent of all the economic espionage cases are targeting communication or technology. So you go inside the wall to steal how you're protecting it. Then you give it to the people outside the wall to use that to attack from the outside.

So if you coordinate those two issues, the person using the cyber attack with someone on the inside acquiring how they're protecting it, and you put those together, it makes it easy to attack, and that's 30 percent of all the cases we've seen, is that kind of information being targeted primarily by the Chinese.

HEARING CO-CHAIR BROOKES: Michelle, you said, you made a statement saying that you expected that the Chinese intelligence threat to become much worse. Could you expand on that a little bit?

MS. VAN CLEAVE: I think the threat will grow as a result of their successes against us, both in the cyber realm but also as David was saying, because of the integration of those cyber successes and their human espionage capabilities. I'm looking at what was lost through the OPM breach, Peter, and I'm saying this is, this is staggering. This is staggering. The current NCIX was given the responsibility to try to do a damage assessment of what has been compromised. I wouldn't know where to start. When you have that kind of detailed information on 22 million people with access to U.S. classified information, any intelligence service could sit back and use that as a road map to fuel an explosion of operational activity.

HEARING CO-CHAIR BROOKES: Do you expect them to become more aggressive, especially in their HUMINT collection?

MS. VAN CLEAVE: Yes.

HEARING CO-CHAIR BROOKES: Or recruitment I mean outside of China? Do we expect--I mean what do--

MS. VAN CLEAVE: Yes.

HEARING CO-CHAIR BROOKES: --where do you see those?

MS. VAN CLEAVE: Yes and yes.

HEARING CO-CHAIR BROOKES: That's why I was asking David where do we see those trends going because we know what we've seen in the past. Where do you see this going, having that access to that sort of information in terms of their recruitment process?

MS. VAN CLEAVE: So this is where national strategy and operations in the intelligence world come together. What are China's priorities from a military strategy point of view, from a diplomatic or foreign policy point of view? Those priorities --and their economic interests-- will direct the way that they engage their intelligence resources to support their goals, right, like any other nation state. They're going to use it that way.

The United States is their biggest concern, their biggest target always, always, whether it's in gaining advantage or in gaining insight into what we're doing, from strategic objectives such as keeping us out of the South China Sea to a tactical operations like buzzing our aircraft. Whatever it is, the U.S. is going to be their biggest concern, and the access to these files, the ability to recruit inside the U.S. government, the ability to gain insight into what the United States is doing and how we're doing it, that is where I would expect to see them pushing their advantage wherever they, wherever they find it.

So this is why I'm so concerned about this loss. When you put that together with the cyber attacks, you kind of scratch your head and you say why? Why the attacks on these health insurance companies? Why are we seeing them going after records of airline companies where people have traveled? Or financial records?

This is all a part of an opportunity to build a matrix that says, okay, here's a possibility. This is an interesting individual. As David was saying, and a big lesson I got out of going into this business, is that it's always about people. It always comes down to people. Yes, IT has changed everything. The Information Revolution has changed the espionage business

because of the portability of data, because of its ubiquity and the use of metadata analysis and collection. Intelligence work has changed in many, many ways, but it still comes down to people. So this is why I'm so concerned about what it is going to happen now.

MR. MAJOR: I'm not sure if you're familiar with an organization called IC Watch. Their mission is to watch the watchers, and they're young people in their 20s who are mad at the United States intelligence community because of Snowden.

So they put together a database called "Transparent Kit," and you can go on that database, and you can--what they've done is they've pulled people from LinkedIn and what people have said about what they had access to and the programs that are involved, and then they match that with Facebook, and you can go in and search this database. Everybody who has an SCI clearance, anybody who has access to this program, and you go in and search it, and they got thousands and thousands of names. You can go today onto IC Watch, and it's a targeting base, who to go after.

Now, you take that information, which is readily available to anybody, well, it was set up by some kids out of, who went to Boston University. Any intelligence community in the world will use that to target the U.S. intelligence community. Take that with the OPM information, and you got, you've got a great starting point. Here's Joe Johnson. He's got access to these programs. He lives here. Here's everything you want to know about him. And, oh, by--here's some more information about him. So it would be a lot easier.

I as a humaner who targeted people to recruit them would have had to work very hard to get the information that they've got in OPM. I can't tell you what a treasure trove that would be as a starting point because I usually would start with a diplomat that I would be targeting and all I have is name and date of birth. But this information is incredible, and you can't stop that. By the way, I've been compromised with it. I'm sure you have too. I got the letter.

So, yes, you know it's there. This is a challenge to make sure we educate our people, that it's not just that it's been compromised, but the ability to mount an operation, a human operation against Americans. We've always said we were a soft target. We're a very soft target because of this--very soft.

HEARING CO-CHAIR BROOKES: Okay. Thank you. That's all.

HEARING CO-CHAIR DORGAN: Commissioner Fiedler.

COMMISSIONER FIEDLER: I couldn't agree with you more. I mean we were all targets. I'm less worried myself at my age, okay, because I'm not as valuable since the probability of my life ending is higher at this age than that young lady back there. And so the algorithms that can be written to mine that data, which we do everyday for algorithms for voters, for who will buy soap, and the Chinese can figure out how to write algorithms as well, and I would imagine they're targeting mostly not just for immediate recruitment, but for long-term penetration so that the young population in that OPM database is the one that we should worry about most.

I am--I'm not--I don't begrudge the Chinese anything in terms of gathering intelligence. We do it; they do it. They should do it. So it's a counterintelligence problem to me. Your description of the inability of our, and I'm presuming, both our political leadership and our career civil servant leadership to think strategically is not--so there's two problems that I have with that. Some people are just incapable of doing that anyway. Some individuals.

But then the other problem is the constant chasing. I think you're referring to tactical. So I would refer to it as putting out fire on a constant basis, and you consume your time,

you think you're busy, you're accomplishing something, but you're neglecting the strategic.

That solution to that thought process problem is not purely educational. It exists all over the place. What do you think that solution--I mean you clearly are admitting that you failed in your job to inculcate that into the people you are working for or to have them grab it and understand it. So you failed once. How is the next guy going to succeed? What do you think has to be done?

MS. VAN CLEAVE: So it's not an education failure although education always helps. In this case, it is a lack of an institutional means by which to carry out and achieve a strategic end.

COMMISSIONER FIEDLER: Okay. Now let me stop you a second.

MS. VAN CLEAVE: Yes.

COMMISSIONER FIEDLER: So you don't think it's the shortcomings in the sort of everything that's being thrown at people. It's just that there's no part within the system where there was a vehicle to--

MS. VAN CLEAVE: No. So let me step back a little bit. As we know, since 1947, when the National Security Act was created, there has been a head of U.S. intelligence; right?

COMMISSIONER FIEDLER: Yeah.

MS. VAN CLEAVE: And it was the DCI, then it became a DNI.

COMMISSIONER FIEDLER: Yeah.

MS. VAN CLEAVE: There's always been a recognition of the urgency and the need of integrating what we do from an intelligence perspective.

COMMISSIONER FIEDLER: The stovepiping problem.

MS. VAN CLEAVE: Yeah, pieces. The pieces are put together so you have a whole. Counterintelligence never had a head. Counterintelligence grew up always, always, always as a subordinate mission within different entities.

COMMISSIONER FIEDLER: And it had some bad history with--other stuff--

MS. VAN CLEAVE: Well, there is that history also.

COMMISSIONER FIEDLER: Yeah.

MS. VAN CLEAVE: But no one ever sat back and said who's worrying about the foreign intelligence threats against the United States? Who's got the job of saying here are these threats and here is what we need to do about them?

COMMISSIONER FIEDLER: Well, let me go to the here--because you go in your oral testimony to us to that next step--

MS. VAN CLEAVE: Yes.

COMMISSIONER FIEDLER: --which is advocacy of disruptive operations--

MS. VAN CLEAVE: Yes.

COMMISSIONER FIEDLER: --is what I would characterize that as.

MS. VAN CLEAVE: Fair. That's fair.

COMMISSIONER FIEDLER: Okay?

MS. VAN CLEAVE: Yes.

COMMISSIONER FIEDLER: And there are two aspects to those operations that are currently in debate among people anyway. One, and there are two levels in my view of difficulty. One, foreign operations, disruptive foreign operations, which are easier to do, and then disruptive domestic operations, which in the counterintelligence context seems to me to be the greater problem and the greater obstacle that you're facing.

In other words, we want to disrupt their activities in the United States. And I agree with that. Yeah, I actually agree with that. But how to do it--

MS. VAN CLEAVE: Right.

COMMISSIONER FIEDLER: --becomes very, very difficult and problematic in our current environment.

MS. VAN CLEAVE: I may ask David to speak to this, but let me say that something he said a moment ago made me smile because he was saying a foreign intelligence officer would come to the United States, maybe in a diplomatic posting, and he's at the FBI, and he looks at the jacket behind this individual, to read up on what we know about this person, only it's empty. You got a name. Maybe you know where he was posted last, but that's about it.

COMMISSIONER FIEDLER: Yeah.

MS. VAN CLEAVE: What I'm saying is that for the FBI, for the people who are assigned the job of working against foreign intelligence operations within the United States, we've asked them to start at our own goal line, just start when those people show up here, to start with virtually nothing. I'm saying we need to have a more integrated approach to how we think about the operations of intelligence services within the United States that starts by saying let's figure out who these people are--

COMMISSIONER FIEDLER: As a matter of targeting.

MS. VAN CLEAVE: --what they're doing, what they're up to.

COMMISSIONER FIEDLER: Yeah.

MS. VAN CLEAVE: Before they get here.

COMMISSIONER FIEDLER: Before they get here.

MS. VAN CLEAVE: Yeah. Right.

MR. MAJOR: We actually were somewhat successful in the Bureau--

COMMISSIONER FIEDLER: So we should be stealing their OPM stuff as much as we can.

MR. MAJOR: If we could. If we could. Absolutely, we should.

COMMISSIONER FIEDLER: I mean if they're using Microsoft--if--

MR. MAJOR: Make sure NSA does that.

COMMISSIONER FIEDLER: If they're using Microsoft stuff, they don't--that's pirated--they don't have any security so we should be getting it.

MR. MAJOR: One of the things that Michelle is saying is that what I would work--when I'm working to target country, I know what I know here, and I know what they've done here.

COMMISSIONER FIEDLER: I understand what you're saying.

MR. MAJOR: But what the CIA does against that country is someplace else. We may or may not know depending on how friendly I am with my buddies in the CIA.

COMMISSIONER FIEDLER: That also is a tasking and a resource problem that you said you didn't have. You sort of downplayed the resource problem, which I disagreed with because I suspect that our resources, I mean we certainly have enough money. It's an allocation question.

MS. VAN CLEAVE: Uh-huh.

COMMISSIONER FIEDLER: Okay.

MS. VAN CLEAVE: Sure.

COMMISSIONER FIEDLER: Okay. But so it's an allocation of resources. I don't think that enough is devoted to counterintelligence by any means.

MS. VAN CLEAVE: I'm not arguing with you on that one. Not arguing.

COMMISSIONER FIEDLER: By any means.

MR. MAJOR: Let me throw this--and Michelle wouldn't say this, but I'm going to say it. I've looked at all these NCIXes. They would come in. The one problem--they were never given, they were given the authority, but they weren't given the power, and she couldn't make people do things. And it's a small staff, and you can't make some--and Washington is all about money. If you don't have the power, money, control money, you can't make anybody do anything.

And so she'd want the FBI to do something or the Army to do something, we'd come up and write papers about it, and people would ignore them, and they'd be papers that no one would read. So they were good work, but you had to give her the authority or that position to actually run a national program.

MS. VAN CLEAVE: Right. On the other hand--

MR. MAJOR: And that hasn't happened.

MS. VAN CLEAVE: On the other hand, the FBI and everybody else doesn't need to be told how to do what they already know--

MR. MAJOR: Exactly.

MS. VAN CLEAVE: --how to do, what to do, and how to do it within their spheres. What I am saying is at a national level, there needs to be a strategic effort that draws some of these resources, not all of them, but some of these resources together, and that orients them against the target strategically, and we don't have that today.

HEARING CO-CHAIR DORGAN: Commissioner Tobin.

COMMISSIONER TOBIN: Mr. Chair, I want to explore the same thing touched on by Commissioner Fiedler. Before you spoke about CI being a tool of statecraft. I know what you mean by that. But as we work toward preparing our report, could you give us, more information, expand on that so we can consider perhaps a recommendation for Congress.

MS. VAN CLEAVE: Well, I think back to my academic career, and I had a master's degree in international relations, and the way that international relations was taught back then, the tools of statecraft were a part of what you understood--diplomacy and economics and the military tool--and then later to the table came the question of intelligence and how intelligence is used as a part of state power to accomplish ends.

I am suggesting that countering the intelligence activities of an adversary or a competitor is also a tool of statecraft. , When we come into the National Security Council, and the president has convened the policymakers around the table, and they're trying to assess what needs to be done with respect to China or any other concern, say what it is we're doing in the South China Sea and what does this mean and what should our policy be, I am suggesting that counterintelligence have a seat, in essence, as an advisor at that table that says, Mr. President, , here's what we understand about their intelligence operations supporting what they're doing in the South China Sea.

Here are the opportunities that we see to divert them or to stop them from gaining the kinds of insights that they require in order to achieve their objectives. Counterintelligence from that perspective has a place in the policy discussions to give a full understanding of the range of options available to the United States in how we pursue our objectives.

COMMISSIONER TOBIN: And you mention in National Security Council--

MS. VAN CLEAVE: Yes.

COMMISSIONER TOBIN: --other places? Can you name other places that you

would like to see it?

MS. VAN CLEAVE: Well, that's the venue where all of the departments and agencies come together to provide recommendations going forward to the president, and one of the things that my office was invited to do back when we first started this NCIX operation was to bring those kinds of options to the policy table so that the National Security Council, its staff and membership, would have them as part of their discussions. Whether that continues until today, I don't know.

COMMISSIONER TOBIN: Thank you.

MR. MAJOR: It can work. I can tell you because when I went to the White House, I was the first FBI agent ever sent to the White House to put counterintelligence on the policy table, and I had an ally--that was Ronald Reagan--who understood it. So I was there when things came up, and I have a number of examples by because we were at the table, we were able to affect policy on issues that were being ignored in the past. So it can be there.

And one of them was China, for example, opening up a country, opening up cities, certain cities. Do we want to do that? Do we want to give them a consulate there? What do we have in China? And by being, having a voice there on these big decisions can make a big difference. I don't think they have that position anymore. But I was there for--I was there for awhile. We were successful.

COMMISSIONER TOBIN: Do you think that will be hard to sell.

MS. VAN CLEAVE: No.

COMMISSIONER TOBIN: --like a difficult step.

MS. VAN CLEAVE: --If I said it was hard to sell, let me correct myself. I don't think that it's hard to sell to national security policy people because every time I've had this conversation with people who come with a policy mind-set, their reaction is yes, of course, that makes a good deal of sense, a lot of sense. Where it hasn't resulted in much change is within U.S. intelligence or counterintelligence, and there I think that there is a selling job that needs to be done. There's a job that needs to be done where everyone signs on to say, yes, the strategic counterintelligence mission makes sense.

It's not coming at the expense of doing the day-to-day counterintelligence job that our professionals do so well, but it is beyond that, the next thing that needs also to happen. So that's where I think the education needs to take place among the professionals. If a program, or at least a pilot program, were to get created and assigned to the Director of National Intelligence, go forth and do this, see how it goes, then let's try it out, the proof would be in the doing.

Can we pull the resources together to do the strategic planning across the community that says this is what we have in place, this is what we understand about the environment, and here's what we propose doing about it? The execution can be distributed, but the planning needs to be centralized. In fact, that's how we think about counterterrorism; right? We think about from an NCTC perspective the way that terrorist organizations are operating. Strategic planning is done at a national level and the execution is done as required by different parts of the national security community.

COMMISSIONER TOBIN: Thank you. On a second round, I might ask further questions.

HEARING CO-CHAIR DORGAN: Thank you.
Commissioner Slane.

COMMISSIONER SLANE: Thank you.

Michelle, I'm trying to understand your recommendations and how we can

recommend to Congress that they approach the intelligence agencies and suggest that these things be done? In an earlier life, I worked for an intelligence agency, and it was the defectors that came to us with the names of Americans who were spying for those foreign governments.

And when you talk about being proactive, are you suggesting that we direct the CI overseas to target these people as one mechanism or am I missing something here? I mean what, and how do we get over the hump of recommending to Congress and then Congress telling the intelligence agencies how to do their job?

MS. VAN CLEAVE: So two questions. Let me take the easy one first. Congress has the opportunity of creating or directing, beyond suggesting. Congress can say tell me, to the president, to the DNI, tell me what a strategic counterintelligence program consists of, what are the elements, what are the billets that you require, how do you set out the objectives, how do you measure success, and what are the resources that you need?

Design that program and then go forth and try it out and see how this works because it's a different way of doing business so I wouldn't say let's, you know, overnight flip a switch and you're done. No, we've got to work our way into doing this. So a pilot program is what I would think the Congress, the oversight committees in a classified appropriate arena would be where they would entertain the thought of doing something, directing something like this.

So then to the second part of your question, what would that consist of? Overseas resources would be targeted through all the means of collection that are available to the U.S. intelligence community against the foreign intelligence service as a target of interest. So I want to know with more particularity who are these people and where are they trained?

What does their training consist of? What are their liaison relationships? How are they tasked by their governments? Where do they go? What are the logistics arrangements? All of the things by which this service operates gives insight into what their vulnerabilities might be to exploitation, to recruitment, to whatever the opening might be.

In return for that, we have an opportunity to mislead them, to stop them, to degrade their operations in a variety of different ways. This is the heart and soul of the statutory definition of what counterintelligence is, but we do it case-by-case today. I am suggesting let's think not of individual cases alone but of the service as a whole and go after them in that way.

So think about what we know about how the Chinese collect science and technology, industrial information, trade secret information in the United States. We know that they have, they use front companies. We know that they've got entities in the United States that keep track of who's going where and who's got what and is dealing with tasking because it's not just everything under the sun, it's specific things that they're going to be interested in, particularly when it comes to dual-use technologies that are going to be of value to their military modernization.

So this kind of a system that enables tasking may also enable ways of diverting the collectors, the Chinese collectors, from achieving their objectives. This is not something that is alien to U.S. intelligence. For those who are unaware of the Farewell case against the Soviet Union, this was an insight into KGB operations --provided by a source in place--Vetrov the man's name was. He provided to French intelligence a blueprint, if you will, of all the technologies that the Soviets were interested in acquiring. And once we had that, we were able to run operations that were diverting Soviet collectors and misleading them, and it was a very, very effective program once we had that kind of insight.

I am suggesting that making that kind of an effort against China is more than

called for in today's environment. Does that answer your question?

COMMISSIONER SLANE: Yes, uh-huh. Thank you.

David, anything to add?

MR. MAJOR: Time has run out.

COMMISSIONER SLANE: Okay. Thank you.

HEARING CO-CHAIR DORGAN: Commissioner Wessel.

COMMISSIONER WESSEL: Thank you, both, and many, many questions, and appreciate all your good work over many years, and also want to echo Senator Dorgan's comments about Jack Kemp. Having had the opportunity to work with him many years ago as well, we need more people like him in Congress to try and bridge some of the divide that exists.

Let me ask if you if I can turn this a little bit to some of the vectors that exist for all of these problems. And as we all know, cyber is one of the main vectors that they've used, the Chinese have used to harvest some of the gains.

We have supply chain issues, and understanding we're not going to put the globalization genie back in the bottle, at the same time, it seems that we are losing sight of some of the vectors that are being used, and ideology may be creating additional pressures on policymakers not to act, and I'm specifically referring, although there are many things with Huawei, ZTE, et cetera. And Huawei, and it may have been under your, both of your watches, the last parts of your watch, where tier one suppliers were essentially told that utilizing Huawei equipment on their networks might create some risks that should not be accepted.

We had Congress produce a report. Huawei has been continuing to be active in the U.S. market, not just in handsets, but as we know in tier two and tier three telecom suppliers, many of which are around critical infrastructure, whether it's military or chemical facilities, et cetera. Several weeks ago, there was an article about a directive that the Air Force had given to its contractors to stop procuring Lenovo computers and to actually remove the Lenovo equipment from certain networks. It was being used up at Tobyhanna, which is a C4ISR center, et cetera.

Huawei has, last or two years ago, sponsored the former members of Congress dinner, spending a lot of money to do that. They've been spending millions of dollars to lobby here in town. How should we be looking at the supply chain issues right now? Should we, is the horse out of the barn, that, you know, it's so global that we can't do anything about it? Or should we with, again, with regard to some entities like Huawei, ZTE, continue to be vigilant and try and make sure that their equipment is not utilized on some of our critical systems?

Do you want to start, Ms. Van Cleave?

MS. VAN CLEAVE: I think that the obvious answer is the latter. One needs to continue to be vigilant. Is the horse out of the barn? Well, we were talking about globalization a minute ago; right. The market is global, but the critical systems that are at least critical within the U.S. government, we can and some do, maybe not as effectively as we might want, but we can have screenings that condition acquisition and procurement to validated components that are not going to pose the kinds of risks that an open market might pose.

Now I will tell you one of the problems is having the insight into the companies that are actually the suppliers to know whether or not they do pose a risk. The CFIUS, which reviews these large investments in the United States, thinks about that problem in a similar vein. What is it about the positioning of these large companies in U.S. markets or acquiring U.S. entities?

COMMISSIONER WESSEL: But that's an acquisition, not a sale of equipment.

So Huawei if they were to acquire Three Leaf or, you know, some of the others.

MS. VAN CLEAVE: Right. Yes.

COMMISSIONER WESSEL: But supplying equipment, again, as was the case in the past, to tier one would not be a CFIUS. That would be Team Telecom or one of the other entities, I assume.

MS. VAN CLEAVE: Okay. I guess I was stepping back, tried to think about more of the global--

COMMISSIONER WESSEL: Yeah, okay. Global. Okay.

MS. VAN CLEAVE: --question, but--but the supply chain reviews that go in internally within the intelligence community, within DoD, I mean somehow, and I don't have the magic answer, but somehow that needs to be more rigorous, but in order to be more rigorous, where I was about to go with this is that we need better insight into who some of the subcontractors are or the other companies in order to be able to say whether or not they do pose a risk.

COMMISSIONER WESSEL: Right.

MS. VAN CLEAVE: And some of these supply chain insights, intelligence assessments of potential suppliers got moved under my office when I was the NCIX, and the question the procurement officer wants answered is, tell us is this a risk or not a risk. So I go to the drawer where the information is supposed to be about this particular entity, and we don't have anything. Why? Because we haven't been collecting against it.

So how do I give them an assessment of whether it's a risk or not? It all comes back to having done systematically the collection, the requirements levied against collection, which are limited, and analysis, also limited, in order to understand where the real risks are. So maybe this is manageable. It's a risk. It's a cost-benefit assessment but manageable within the government.

When you step back and say what of the whole of our society? What about the reliance that our critical infrastructures have on components that might be supplied by companies that are under the control of governments that look at this as a way of gaining power over the United States? What about the vulnerabilities of our critical infrastructures? What do we do about that?

Let's not make it easy on them. Let's not open the gates if we don't have to. But to a large extent the gates have been open. So what does that say? What does that say from a planning perspective, from a policy perspective for the United States? This is probably beyond the reach of what we're here to talk about today, but there is a premium, I think, on national security emergency preparedness planning that enables a thin line of reconstitution and recovery in the event critical infrastructures go down in time of crisis that needs a refreshment and a reinvigoration in the recognition that we have these vulnerabilities that are not going to be easily, if ever, corrected.

MR. MAJOR: The acquisition cycle, I'm not sure if this problem has been solved, but I know that one, my interface with DARPA was the fact that the microchip production, that it's all being done in Asia, and they said we don't have the capability to know whether those microchips have been, have some software that could be activated at some time.

So at some particular time when we're going to defend Taiwan, and they say, you know, you can't shoot that missile because if you do, it will shoot your own area, that will be a real problem. I don't know if that problem has been solved, but it's an acquisition one. It's not the company. It's the fact that all the chips are being made in Asia, and we used to make our

own, and then we closed our own chip manufacturing capability. It's never made any sense to me at all.

That problem may have been solved, but I don't think it has. And it's an acquisition problem that goes beyond the company.

COMMISSIONER SLANE: The problems got worse.

MR. MAJOR: That's what I figured.

COMMISSIONER SLANE: Yeah.

MR. MAJOR: That's what I figured.

COMMISSIONER WESSEL: Thank you.

MR. MAJOR: And that's a real Achilles heel, a real Achilles heel.

HEARING CO-CHAIR DORGAN: Commissioner Bartholomew.

VICE CHAIRMAN BARTHOLOMEW: Yes. Thank you very much. Thank you to both of you, both for your service to our country and for your testimony today.

I think that this is a difficult topic for reasons other than some of the difficulties that we've been going through, and, you know, the U.S. is a country that's been built on the contributions of immigrants, and I think it's really important to emphasize here that the vast, vast majority of Chinese Americans are people who are patriotic, who have many have been here for generations. They serve on our military. They're the backbone of communities.

It's an infinitesimal portion of the Chinese American population that we are talking about here, and I just wonder since I believe that it's un-American to equate ethnicity with risk, how the U.S. government can and should balance concerns about intelligence gathering in communities in the United States with sort of the basic freedoms and principles that this country is built on?

MR. MAJOR: Can I try to address that problem? That comes up in almost every class I teach and how do you do this? It's always been a problem in the counterintelligence community. One way to look at it, if I might, is the fact that it's not how we look at ethnicity; it's how the collector looks at ethnicity. The Chinese intelligence services specifically target people who are Hun. They go after them to do it. So it's their decision to do it. It's not our decision to say these are people that can't be targeted.

They are people that have a higher probability of being targeted because of what the targeter's world view is, not the counterintelligence world view is. So that's the only way you can explain that to people because, yes, there's a higher probability that you are going to be targeted because of this. That doesn't have anything to do with whether we trust you or not.

And that's, by the way, this has been with us for a hundred years, and it goes back to World War I when the Nazis--or at that time the Germans were targeting Irish-Americans on the docks to put bombs in there because they were Irish-Americans, because the Irish hated the Brits. And so this is a problem we've always had. Every time we've ever done any kind of policy in counterintelligence, this always surfaces.

And the only way to look at it is we're not questioning anybody's loyalty. We're questioning the methodology used by those who will target them. And it cut across the board with all kinds of ethnicity. Russians will target Russians first, you know. So all the services have this problem.

VICE CHAIRMAN BARTHOLOMEW: Yeah. I'm concerned. I mean you raise the issue of World War I, but, you know, we have a number of instances in our own history of having done it wrong, and I'm thinking particularly of the Japanese internment, but there are a number of other incidents, and I guess what I'm concerned about even just with the conversation

that we've been having today is that it somehow leaves people with the impression that there is a presumption of guilt or risk on Chinese Americans, and, you know, so I understand the distinction that you're making, but in practice people have to implement and how, how does that implementation take place in this country by U.S. government agencies without essentially profiling an entire community?

MR. MAJOR: Because you don't start a case like that. Never go after a case and say, oh, that's a person that I don't trust because of their ethnicity, I'm going to investigate them. That's not how counterintelligence and security works at all. What it does is it starts with some facts, some justification, for looking at an individual that I can articulate and make clear. So it never starts that way. I've never worked a case simply to say, well, let's see, this person is Chinese, let's investigate them. Or this person is whatever the nationality is. It's just not how we do it and never have done it that way.

But there's a perception that's how we do it, and that's often used as a defense when a case surfaces. They say, oh, look at the Wen Ho Lee case, I mean, you targeted him because he was Chinese. No, because we had evidence that he might be the person. So it's a way of articulating the predication. But people who don't know how the system works believe that that's how you predicate cases.

VICE CHAIRMAN BARTHOLOMEW: Ms. Van Cleave, anything to add?

MS. VAN CLEAVE: I think David makes a good point that that really is not how it works, and yet I understand your concern, that there is that perception, but what I would hope to convey to you is that counterintelligence as a profession in the United States is really not about or shouldn't be considered to be about finding the traitors among us so much as it is understanding how an adversary uses intelligence against us.

That's what I am inviting you to think about. It is how do the Chinese use their intelligence services, their human intelligences, their cyber collection, their SIGINT services? How do they use them in ways that are going to advance their interests and harm us? And is there something we can do about that so that we don't get hurt?

MR. MAJOR: Let me just add one thing. What makes us distinctly different in our society is that when we do counterintelligence, we target the collector to find out who is the betrayer. We don't target potential betrayers, people that they might target. We don't target them. We go from the collector to the betrayer. That's not true in other societies. Other societies see people in that society as potential betrayers for them.

Russians did this all the time. Make three trips to the United States. They're going to target you. But we've never done that, and that's not often understood. So we go from, as I say repeating myself, from collector to betrayer, and we don't start with betrayer.

VICE CHAIRMAN BARTHOLOMEW: Thank you.

HEARING CO-CHAIR DORGAN: Commissioner Shea.

CHAIRMAN SHEA: Thank you, both, for being here. This has been very, very fascinating.

I'm just going to direct my question to Mr. Major. I was reading your written testimony, and I guess the staff asked you to respond to a series of questions, and one of the questions was: Outside the United States, which U.S. government national security decision-making bodies, defense industrial actors, weapons, platforms, and systems, and operations does China target or seek to target with espionage operations?

And then your response was to refer to something called the strategy of "Unrestricted Warfare," developed by two PLA colonels, and outlines 12 areas targets of the

strategy that range from financial warfare, to drug warfare, which struck me as particularly interesting, cultural warfare, and I'm just wondering is this--in your assessment, is this the operational concept behind Chinese operation? I was just wondering why you started there? Why did you even raise this?

MR. MAJOR: Well, I went from there--I think I went from there to Taiwan.

CHAIRMAN SHEA: Yeah.

MR. MAJOR: But--which is the real Achilles heel in that question. That unconventional, Unrestricted Warfare is a controversial paper written by two PLA colonels in their effort to say here's how you beat the United States, and one belief is that, well, it's just a think piece. This is really not a strategy. This is just going to put this out as a placeholder for other--there's another belief that says, no, this really was what their strategy is and they may still use part of that.

So anyone who looks at China I think should be aware of the existence of that book and that strategy, and it's a starting off point for what they might be doing. I don't know if you have any view on that book because I have mixed views on the book.

HEARING CO-CHAIR BROOKES: It's almost 20 years old, though; right?

MR. MAJOR: 1999.

HEARING CO-CHAIR BROOKES: Yeah, that's what I say.

MR. MAJOR: Yeah.

HEARING CO-CHAIR BROOKES: So it's a long time ago.

MR. MAJOR: Well, yeah. In the counterintelligence business, that's not a long time.

[Laughter.]

CHAIRMAN SHEA: Yeah, right. But is this something you feel forms, is real, actually forms the basis of their thinking?

MR. MAJOR: I think it has a basis in fact for some of the collections we see. Maybe not all 12 of them, but I see it as part of it.

CHAIRMAN SHEA: So they're collecting to serve that strategy, to meet that.

MR. MAJOR: The strategy might be being served as to what their strategic goals are. It would be a starting point, not the end point, as I see it.

MS. VAN CLEAVE: But on that point, wouldn't it be nice if we had fidelity on what in fact their strategy is? If we had the reach inside their operations to know what that strategy is and what their tasking genuinely is, it would give us such an advantage in trying to stop them or degrade them.

CHAIRMAN SHEA: Thank you.

HEARING CO-CHAIR BROOKES: Do we have a national counterintelligence center like the NCTC?

MS. VAN CLEAVE: Yes, the Office of the National Counterintelligence Executive.

HEARING CO-CHAIR BROOKES: That's it.

MS. VAN CLEAVE: Uh-huh.

HEARING CO-CHAIR BROOKES: Is it on the same level in terms of resources as NCTC?

MS. VAN CLEAVE: It's not nearly as large, but in the hierarchy of the org chart of the Office of the DNI, it's one of the three centers that the DNI operates. The third being Counterproliferation.

HEARING CO-CHAIR BROOKES: Okay.

MR. MAJOR: Let me ask, follow up on your question. One of the things that all your questions relate to is how much insight do we have on what China is doing? And the only way we're going to get this insight is primarily two ways. You're going to get it through, maybe you might get it through signals intelligence, but you're also getting it through human intelligence. And so one of the questions you asked was how successful have we been in penetrating them, and I articulated in the paper I wrote a couple of or three very good successes we had.

It wasn't until 1981 that the entire Western world never had a human source inside China, and that first source came to us by "Planesman." Planesman was a game changer for us. He volunteered to us, was operated in place until 1985. He gave us Chin--

MS. VAN CLEAVE: Larry Wu-Tai Chin.

MR. MAJOR: Larry Wu-Tai Chin. He gave us that case, but since that time, there's this other case that you can, if you look at charts like this--this is something from the CI--this should tell you something immediately. Only way you can identify spies is there's got to be a source on the inside. The idea comes up with something else. From the real world there's always a source.

So when you start finding sources, you start finding spies, it means you've been successful in making penetrations somehow, and you can almost dovetail this and our success with the arrest of the Special Assistant to the Vice Chairman of the MSS, which took place in January of 2012 and became public in June of 2012.

And if you dovetail that information that's come out and then look at these cases, they begin to make sense because, if you notice, the arrest was made in 2012. They had 12 arrests in Taiwan. That's because the source has been compromised. Therefore, I can take action on it.

In our business, one of the things you have to remember is the worst thing is to not have a source, but the next worst thing is to have a source because you got to take action based on the source and protect your source. And all of this discussion is how many sources you have.

And now, right now, we're dealing with a major defector. There's been some publicity on it that they talk about. That's a success for our intelligence community. So when you look at this, all the answers are based on how many human sources can we get, and we've have some success in that.

MS. VAN CLEAVE: One slight amendment.

MR. MAJOR: Yeah.

MS. VAN CLEAVE: I think the worst thing is to have a source that's actually not your source--

MR. MAJOR: Well, that's--

MS. VAN CLEAVE: But rather controlled by the other side--

MR. MAJOR: Make that number three. And the worse thing is--and a bad source.

[Laughter.]

HEARING CO-CHAIR DORGAN: Well, the Commission wants to thank both of you today. You both have a wealth of knowledge with which you've made a significant deposit with us today, and it is very much appreciated.

The Commission is going to hold a roundtable now at 1:30 so we will take a break

until 1:30. I will necessarily be absent I've indicated to Peter. I'm hoping to return before the end of the roundtable, but, in any event, Mr. Wessel has agreed to fill the chair.

And with that, then we will have about a one hour recess and then reconvene for a roundtable.

CHAIRMAN SHEA: The roundtable is private.

HEARING CO-CHAIR DORGAN: The roundtable is going to be private. But again let me thank Ms. Van Cleave and Mr. Major, really a terrific job. Thank you very much.

HEARING CO-CHAIR BROOKES: Thank you. Thank you very much.

MS. VAN CLEAVE: Thank you.

MR. MAJOR: Thanks.