

**ESPIONAGE THREATS AT
FEDERAL LABORATORIES:
BALANCING SCIENTIFIC COOPERATION WHILE
PROTECTING CRITICAL INFORMATION**

HEARING
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT
COMMITTEE ON SCIENCE, SPACE, AND
TECHNOLOGY
HOUSE OF REPRESENTATIVES
ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

THURSDAY, MAY 16, 2013

Serial No. 113-28

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: <http://science.house.gov>

U.S. GOVERNMENT PRINTING OFFICE

81-192PDF

WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

DANA ROHRBACHER, California	EDDIE BERNICE JOHNSON, Texas
RALPH M. HALL, Texas	ZOE LOFGREN, California
F. JAMES SENSENBRENNER, JR., Wisconsin	DANIEL LIPINSKI, Illinois
FRANK D. LUCAS, Oklahoma	DONNA F. EDWARDS, Maryland
RANDY NEUGEBAUER, Texas	FREDERICA S. WILSON, Florida
MICHAEL T. McCAUL, Texas	SUZANNE BONAMICI, Oregon
PAUL C. BROUN, Georgia	ERIC SWALWELL, California
STEVEN M. PALAZZO, Mississippi	DAN MAFFEI, New York
MO BROOKS, Alabama	ALAN GRAYSON, Florida
RANDY HULTGREN, Illinois	JOSEPH KENNEDY III, Massachusetts
LARRY BUCSHON, Indiana	SCOTT PETERS, California
STEVE STOCKMAN, Texas	DEREK KILMER, Washington
BILL POSEY, Florida	AMI BERA, California
CYNTHIA LUMMIS, Wyoming	ELIZABETH ESTY, Connecticut
DAVID SCHWEIKERT, Arizona	MARC VEASEY, Texas
THOMAS MASSIE, Kentucky	JULIA BROWNLEY, California
KEVIN CRAMER, North Dakota	MARK TAKANO, California
JIM BRIDENSTINE, Oklahoma	ROBIN KELLY, Illinois
RANDY WEBER, Texas	
CHRIS STEWART, Utah	
VACANCY	

SUBCOMMITTEE ON OVERSIGHT

HON. PAUL C. BROUN, Georgia, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin	DAN MAFFEI, New York
BILL POSEY, Florida	ERIC SWALWELL, California
DAVID SCHWEIKERT, Arizona	SCOTT PETERS, California
KEVIN CRAMER, North Dakota	EDDIE BERNICE JOHNSON, Texas
LAMAR S. SMITH, Texas	

CONTENTS

Date of Hearing

	Page
Witness List	2
Hearing Charter	3

Opening Statements

Statement by Representative Paul C. Broun, Chairman, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	9
Written Statement	10
Statement by Representative Dan Maffei, Ranking Minority Member, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	11
Written Statement	11

Witnesses:

Dr. Charles M. Vest, President, National Academy of Engineering	
Oral Statement	12
Written Statement	15
Dr. Larry Wortzel, Commissioner, U.S.-China Economic and Security Review Commission	
Oral Statement	30
Written Statement	32
Hon. Michelle Van Cleave, Senior Fellow, Homeland Security Policy Institute, George Washington University	
Oral Statement	43
Written Statement	45
Mr. David G. Major, Founder and President, The Centre for Counterintelligence and Security Studies	
Oral Statement	59
Written Statement	62
Discussion	104

Appendix I: Answers to Post-Hearing Questions

Dr. Charles M. Vest, President, National Academy of Engineering	116
Dr. Larry Wortzel, Commissioner, U.S.-China Economic and Security Review Commission	120
Hon. Michelle Van Cleave, Senior Fellow, Homeland Security Policy Institute, George Washington University	125
Mr. David G. Major, Founder and President, The Centre for Counterintelligence and Security Studies.	133

**ESPIONAGE THREATS AT FEDERAL
LABORATORIES:
BALANCING SCIENTIFIC COOPERATION
WHILE PROTECTING CRITICAL INFORMATION**

THURSDAY, MAY 16, 2013

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittee met, pursuant to call, at 3:00 p.m., in Room 2318 of the Rayburn House Office Building, Hon. Paul Broun [Chairman of the Subcommittee] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

**Congress of the United States
House of Representatives**

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371

www.science.house.gov

Subcommittee on Oversight

***Espionage Threats at Federal Laboratories: Balancing Scientific
Cooperation while Protecting Critical Information***

Thursday, May 16, 2013

2:00 p.m. to 4:00 p.m.

2318 Rayburn House Office Building

Witnesses

Dr. Charles M. Vest, President, National Academy of Engineering

Dr. Larry Wortzel, Commissioner, U.S.-China Economic and Security Review Commission

Hon. Michelle Van Cleave, Senior Fellow, Homeland Security Policy Institute, George
Washington University

Mr. David G. Major, Founder and President, The Centre for Counterintelligence and Security
Studies

**U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight**

HEARING CHARTER

*Espionage Threats at Federal Laboratories:
Balancing Scientific Cooperation while Protecting Critical Information*

Thursday, May 16, 2013
2:00 p.m. – 4:00 p.m.
2318 Rayburn House Office Building

Purpose

On May 16, 2013, the Subcommittee on Oversight will hold a hearing titled *Espionage Threats at Federal Laboratories: Balancing Scientific Cooperation while Protecting Critical Information*. The goal is to gain an understanding of how federally-owned-or-operated laboratories balance scientific openness and international cooperation with the need to protect sensitive information from espionage. This hearing will focus on identifying potential deficiencies, best practices, and to ensure sensible federal policies.

Witnesses

- Dr. Charles M. Vest, President, National Academy of Engineering;
- Dr. Larry Wortzel, Commissioner, U.S.-China Economic and Security Review Commission;
- Hon. Michelle Van Cleave, Senior Fellow, Homeland Security Policy Institute, George Washington University;
- Mr. David G. Major, Founder and President, The Centre for Counterintelligence and Security Studies.

Background

The United States has long been the world leader in higher education, science and technology and a magnet for foreign-born scholars, scientists and engineers. Unfortunately, various actors have sought to exploit our openness to steal American ingenuity and innovation. Such thefts can enable nations to save themselves billions in research and development costs and make technological advances they would be unable to make on their own to gain a competitive industrial advantage or modernize their military and other national capabilities.

Historically, restrictions focused mostly on technologies with obvious military applications such as nuclear material, cryptography and biological weapons. The goal of American counterespionage was to prevent a potential adversary from gaining such technological

advantage, and during the Cold War, it was generally clear what nations should be guarded against. However, the emergence of transnational terrorist actors and the means of communicating information, including technological innovation, via the Internet, has given rise to a far greater, more diverse and global espionage threat.

In the United States, there has long been support for a policy of not restricting publication of federally supported research results, except where classified for national security reasons. This position was best expressed in 1985 by President Ronald Reagan in National Security Decision Directive 189 (NSDD-189), which remains the government policy regarding controls on federally-funded research results. The directive asserts that “to the maximum extent possible, the products of fundamental research remain unrestricted.”¹

Fundamental research is defined within NSDD-189 as:

“...basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.”²

NSDD-189 acknowledges that there are risks associated with the open exchange of ideas within the scientific and academic communities, but it asserts that the benefits to security and other key national objectives outweigh the potential dangers.³ Nonetheless, the emergence of significant threats to national security has at times caused the pendulum to swing toward increased security and tighter controls at the cost of scientific openness and international collaboration.

Benefits of International Scientific Cooperation

Science is a worldwide endeavor. In 2008, American Association for the Advancement of Science (AAAS) Chief Executive Officer Alan I. Leshner testified before this Committee that, “Science is by definition global in scope and application - it knows no borders, is not constrained by geography, and no one country has a monopoly on it.”⁴

In March 2011, Bo Cooper, former General Counsel to the then-Immigration and Naturalization Service (INS), testified before the House Judiciary Committee that, “Throughout our history, our country has operated on the principle that the more brain power we can attract from around the

¹ White House, Executive Office of the President, “National Policy on the Transfer of Scientific, Technical, and Engineering Information,” National Security Decision Directive-189, 1985, available at: <http://www.aau.edu/WorkArea/showcontent.aspx?id=1560>; hereinafter NSDD 189.

² Ibid.

³ Ibid.

⁴ Written Testimony of Alan I. Leshner, House Committee on Science and Technology, Subcommittee on Research and Science, “The Role of Non-Governmental Organizations and Universities in International Science and Technology Cooperation,” 110th Cong., 2d sess., 2008.

world, the more creativity, invention, and growth we can achieve here at home.”⁵ A Harvard Business School study found that the number of inventions, as measured by patents, increased when H-1B visa caps were higher due to “the direct contributions of immigrant inventors.”⁶ Though the numbers have declined during the current economic downturn, immigrants with advanced degrees still comprise a considerable percentage of U.S. workers in science and engineering occupations. At the doctoral degree level, about half of U.S. workers in computer and mathematical sciences and in engineering are foreign-born.⁷

Aside from sparking innovation and entrepreneurship, foreign scholars make significant contributions to the American economy. The Association of International Educators estimates that international students and their dependents contributed approximately \$21.8 billion to the American economy during the 2011-2012 academic year. This figure is based on an analysis of tuition, enrollment figures, living expenses and other associated costs.⁸

International scientific cooperation and openness to international students also serves longstanding and important U.S. foreign policy goals by fostering communication and cooperation among nations to promote greater global peace, prosperity and stability.

Intelligence Threats to Science and Technology Community

According to the Office of the National Counterintelligence Executive, foreign economic collection and industrial espionage is a significant and growing threat. Russia and China are the most aggressive and persistent perpetrators.⁹ While China’s intrusions of U.S. computer networks has increased significantly in recent years, China’s espionage continues to operate in the physical world as well. Chinese scientists and engineers permeate U.S. academic and industrial research sectors. While most are honest, hard-working individuals, here in the U.S. for legitimate reasons, a quick review of recent economic espionage and trade-secret theft cases involving Chinese scientists and engineers show a more systemic campaign to gain American know-how:

- In November 2012, Shanshan Du and Yu Qin were convicted for conspiring to steal hybrid technology from General Motors on behalf of a Chinese competitor.

⁵ Written Testimony of Bo Cooper, House Committee on the Judiciary, Subcommittee on Immigration Policy and Enforcement, “H1B Visas: Designing a Program to Meet the Needs of the U.S. Economy and U.S. Workers,” 112th Cong., 1st sess., 2011.

⁶ William R. Kerr and William F. Lincoln, “The Supply Side of Innovation: H-1B Visa Reforms and Us Ethnic Invention,” (Working Paper 09-005, Harvard Business School, 2008), available at: <http://www.hbs.edu/faculty/Publication%20Files/09-005.pdf> (accessed May 6, 2013).

⁷ “Science and Engineering Indicators 2012,” available at: <http://www.nsf.gov/statistics/seind12/c3/c3s4.htm#s4> (accessed May 6, 2013).

⁸ NAFSA: Association of International Educators, “The Economic Benefits of International Students to the U.S. Economy Academic Year 2011 – 2012”, 2012, available at: http://www.nafsa.org/_File/_eis2012/USA.pdf (accessed May 6, 2013).

⁹ Office of the National Counterintelligence Executive, “Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011,” 2011, available at: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (accessed May 6, 2013).

- In September 2012, engineer Sixing Liu stole files detailing the guidance systems for missiles, rockets, target locators and unmanned aerial vehicles from a division of L-3 Communication.
- In March 2012, former DuPont scientist Tze Chao pleaded guilty to providing trade secrets to companies he knew were controlled by the government of China.
- In February 2010, former Rockwell and Boeing engineer Dongfan Chung was sentenced to prison for stealing restricted technology and trade secrets related to the Space Shuttle program and the Delta IV rocket.¹⁰

China is not the only threat. Former Cold War adversaries in Russia view the United States as a strategic competitor and are also aggressive and capable collectors of U.S. economic information and technology.¹¹ In his book *Comrade J: The Untold Secrets of Russia's Master Spy in America After the End of the Cold War*, Peter Earley chronicles the activities of Sergei Tretyakov, the head of political intelligence for Russia's foreign intelligence service, the SVR [the Sluzhba Vneshney Razvedki], in New York City from 1995-2000. "We often targeted academics because their job was to share knowledge and information by teaching it to others, and this made them less guarded than, say, UN diplomats," Earley quoted Tretyakov as saying.¹² Tretyakov also recounted an instance when an SVR agent provided unreleased medical data and proprietary information based on medical patents held by U.S. companies. While the underlying research reportedly cost the U.S. government \$40 million to fund, the SVR agent refused to accept any payment.¹³

Terrorists can also clandestinely acquire the advanced technological information or materials needed to build a nuclear, biological, chemical or radiological weapon. In February 2011, Khalid Ali-M Aldawsari, a Saudi student studying chemical engineering at Texas Tech University, was charged with attempting to use a weapon of mass destruction. A journal found at Aldawsari's residence described how he sought and obtained a particular scholarship because it allowed him to come directly to the United States and helped him financially, which he said "will help tremendously in providing me with the support I need for Jihad."¹⁴

¹⁰ Ibid.

¹¹ Ibid.

¹² Cited in Daniel Golden, "American Universities Infected by Foreign Spies Detected by FBI," Bloomberg, April 08, 2012, available at: <http://www.bloomberg.com/news/2012-04-08/american-universities-infected-by-foreign-spies-detected-by-fbi.html> (accessed May 6, 2013).

¹³ Peter Earley, *Comrade J: The Untold Secrets of Russia's Master Spy in America after the End of the Cold War*, (New York: G.P. Putnam's Sons, 2007), p. 274.

¹⁴ U.S. Department of Justice, Press Release: "Texas Resident Arrested on Charge of Attempted Use of Weapon of Mass Destruction," February 24, 2011.

Mechanisms for Oversight

Screening of Foreign Students and Scholars

The United States has allowed foreign students to study in U.S. institutions on temporary visas since the Immigration Act of 1924.¹⁵ Each year, hundreds of thousands of international scholars and students participate in education and exchange programs at American colleges and universities. In the 2011-2012 school year, 764,321 students from abroad were enrolled at U.S. colleges and universities.¹⁶ A visa system that is secure, timely, efficient, transparent and predictable is the first line of defense and permits both scientific exchange and enhances national security.

Export Control Regulations

The federal government controls the flow of information and materials through export control and arms trafficking regulations. Specifically, the Department of Commerce implements the Export Administration Regulations (EAR), which restrict the export of “dual-use” goods and technology – items with both civilian and military applications – found on the Commerce Control List. The Department of State implements the International Traffic in Arms Regulations (ITAR), which regulate the export of defense items and munitions enumerated on the U.S. Munitions List (USML).

Technology export controls are vital to U.S. security and competitiveness, but they have also challenged the ability of industry, laboratories and academia to engage international partners. Many have argued that the regulations are outdated and unnecessarily complicated. In 2009, former National Security Advisor Brent Scowcroft and Lockheed-Martin CEO Norm Augustine co-chaired a National Academies committee which produced a report titled “Beyond ‘Fortress America’: National Security Controls on Science and Technology in a Globalized World.” The report bluntly stated: “The national security controls that regulate access and export of science and technology are broken. As currently structured, many of these controls undermine our national and homeland security and stifle American engagement in the global economy, and in science and technology.”¹⁷

In August 2009, the Obama Administration launched a comprehensive review of the U.S. export control system with the ultimate aim of creating a unified system with one licensing agency, one control list, a single enforcement coordination agency and an integrated information technology

¹⁵ U.S. Library of Congress, Congressional Research Service, “Monitoring Foreign Students in the United States: The Student and Exchange Visitor Information System (SEVIS),” by Alison Siskin, RL32188, (Washington, DC: Office of Congressional Information and Publishing, January 14, 2005).

¹⁶ Institute of International Education, “Open Doors 2012: Report on International Educational Exchange – Fast Facts,” available at: <http://www.iie.org/en/Research-and-Publications/Open-Doors> (accessed May 6, 2013).

¹⁷ Committee on Science, Security, and Prosperity; Committee on Scientific Communication and National Security; National Research Council, “Beyond ‘Fortress America’: National Security Controls on Science and Technology in a Globalized World,” (Washington, DC: National Academies Press, 2009), p. ii.

(IT) system.¹⁸ As of April 2013, the Department of State and the Department of Commerce had issued the first set in a series of final rules that redefine how the U.S. government protects sensitive technologies and regulates exports of munitions and commercial items with military applications.¹⁹

Classification

Classification is the most appropriate mechanism when it is required that certain information be maintained in confidence in order to protect American citizens and national security. NSDD-189 states:

“It is also the policy of this Administration that, where the national security require control, the mechanism for control of information generated during federally-funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification. Each federal government agency is responsible for: a) determining whether classification is appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification procedures; b) periodically reviewing all research grants, contracts, or cooperative agreements for potential classification. No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes.”²⁰

Proper use of the established national security information classification system will allow for clear distinctions between classified and unclassified research, help eliminate uncertainties among scientists and officials responsible for enforcing regulations and better prevent the loss of sensitive information.

¹⁸ U.S. Library of Congress, Congressional Research Service, “The U.S. Export Control System and the President’s Reform Initiative,” by Ian F. Ferguson and Paul K. Kerr, R41916, (Washington, DC: Office of Congressional Information and Publishing, January 11, 2013).

¹⁹ Department of State, “Export Control Reform: First Final Rules Mark Major Milestone,” available at: <http://www.state.gov/r/pa/prs/ps/2013/04/207597.htm> (accessed May 10, 2013).

²⁰ NSDD 189, *supra*, note 1.

Chairman BROUN. The Subcommittee on Oversight will come to order. Good afternoon, everyone. I appreciate you all's patience. Every now and then we have votes that come into play that interfere with our schedule and we appreciate everybody's patience.

In front of you are packets containing the written testimony, biographies, and the truth-in-testimony disclosures for today's witnesses. I now recognize myself for five minutes for an opening statement.

The title for today's hearing is, "Espionage Threats at Federal Laboratories: Balancing Scientific Cooperation while Protecting Critical Information." I would like to extend a particularly warm welcome to our witnesses and to thank you all for joining us here today, and we are looking forward to your testimony.

This hearing focuses on the intersection of two very important issues: one, ensuring that the United States remains the world's leader in scientific research and technological innovation; and protecting our national security on the other hand. Both are extremely important.

Finding the appropriate balance between scientific openness and security concerns is not new. But it is critical that we have this type of public discussion regularly so as to maintain open lines of communication and, if necessary, recalibrate our strategies to respond to new threats.

Science is a global endeavor. International cooperation on science and technology and the open exchange of ideas has led to countless significant breakthroughs that have benefited all of mankind. Here in the United States, visiting foreign scientists and scholars sparks innovation and entrepreneurship. They make critical contributions to our economy, and they learn firsthand about American culture and values. But, we cannot afford to close our eyes to the reality that there are nefarious actors—scheming insiders, business rivals, criminals, even terrorists and foreign intelligence services—who exploit our free and open society to steal the results of American ingenuity and innovation.

Russia and China have regularly topped the intelligence and law enforcement community's list of the most aggressive and persistent thieves of our scientific and technological information that is very sensitive. Russia views the United States as a strategic competitor and its intelligence services are very capable and just as prolific as ever.

And China continues efforts to gain access to advanced technology to fuel its military modernization program, according to the Pentagon's latest report on the capabilities of the Chinese military. The report says China operates a large, well-organized network of companies and research institutes with both military and civilian R&D functions that enable the Chinese military to access sensitive and dual-use technologies or knowledgeable experts under the guise of legitimate civilian R&D. This raises the question: are American taxpayers' dollars subsidizing the modernization of China's military? Just last week, Chinese media reported that their military is ready to test-fly an armed stealth drone which looks remarkably like some American stealth aircraft.

In addition to foreign intelligence services, terrorists could clandestinely acquire the advanced technological information or mate-

rials needed to build a nuclear, biological, chemical, or radiological weapon. What if the Boston bombers had used their university ties to acquire radiological material to turn their bombs into dirty bombs?

Our goal today is to gain a better understanding of how Federal laboratories and their partners in the broader academic and scientific communities balance international scientific cooperation with the need to protect sensitive information. I don't have any prescriptions to put before you. As a doctor, I wish I did. But, I look instead to our witnesses to identify best security practices and sensible Federal policies that don't allow the pendulum to swing too far in either direction.

Thank you.

Now, I recognize the Ranking Member, the gentleman from New York, Mr. Maffei, for an opening statement. My friend, you are recognized for five minutes.

[The prepared statement of Mr. Broun follows:]

PREPARED STATEMENT OF CHAIRMAN PAUL C. BROUN

Good afternoon and welcome everyone to this Subcommittee on Oversight hearing titled "Espionage Threats at Federal Laboratories: Balancing Scientific Cooperation while Protecting Critical Information." I would like to extend a particularly warm welcome to our witnesses and thank them all for joining us here today.

Today's hearing focuses on the intersection of two very important issues—ensuring that the United States remains the world leader in scientific research and technical innovation, and protecting our national security.

Finding the appropriate balance between scientific openness and security concerns is not new. But it is critical that we have this type of public discussion regularly, so as to maintain open lines of communication, and if necessary, recalibrate our strategies to respond to new threats.

Science is a global endeavor. International cooperation on science and technology and the open exchange of ideas has led to countless significant breakthroughs that have benefitted all of mankind. Here in the United States, visiting foreign scientists and scholars spark innovation and entrepreneurship, make critical contributions to the economy and learn first-hand about American culture and values.

But we can't afford to close our eyes to the reality that there are nefarious actors—scheming insiders, business rivals, criminals, terrorists, and foreign intelligence services—who exploit our free and open society to steal the results of American ingenuity and innovation.

Russia and China have regularly topped the intelligence and law enforcement community's lists of the most aggressive and persistent thieves of sensitive scientific and technical information.

Russia views the United States as a strategic competitor and its intelligence services are very capable and just as prolific as ever.

And China continues efforts to gain access to advanced technology to fuel its military modernization program, according to the Pentagon's latest report on the capabilities of the Chinese military. The report says China operates a large, well-organized network of companies and research institutes with both military and civilian R&D functions that enable the Chinese military to access sensitive and dual-use technologies or knowledgeable experts under the guise of legitimate civilian R&D. This raises the question, are American taxpayer dollars subsidizing the modernization of China's military? Just last week, Chinese media reported that their military is ready to test-fly an armed, stealth drone which looks remarkably like the American MQ-9 Reaper.

In addition to foreign intelligence services, terrorists could clandestinely acquire the advanced technological information or materials needed to build a nuclear, biological, chemical or radiological weapon. What if the Boston bombers had used their university ties to acquire radiological material to turn their bombs into dirty bombs?

Our goal today is to gain a better understanding of how federal laboratories and their partners in the broader academic and scientific communities balance international scientific cooperation with the need to protect sensitive information. I don't have any prescriptions to put before you, but look instead to our witnesses to iden-

tify best security practices and sensible federal policies that don't allow the pendulum to swing too far in either direction.

Mr. MAFFEI. I want to thank the Chairman of the Committee and I want to thank particularly the witnesses and audience today for your patience given these—the voting schedule and the logistics of getting back here.

I want to associate myself with the comments of the distinguished Chairman from Georgia and I would only add that the challenge at our national labs and our scientific facilities is controlling access to information and innovations that are truly highly sensitive without obstructing the positive interaction that occurs between scientists.

So, as we see on a routine basis, other nations and foreign corporations regularly are attempting to steal, siphon, or subtly acquire U.S. Government secrets or other kinds of proprietary data that has highly technical and scientific value for the economy or national security. So identifying specific espionage threats, developing safeguards against them, and warning American scientists about them is certainly an important task. But it is a task that has to be balanced against the cost of overreacting and inhibiting the advance of scientific understanding and positive international cooperation.

So this hearing will help illuminate those tradeoffs. And I am very grateful to the Chairman for calling it. I look forward to hearing from our witnesses today about how to strike the right balance between these both very necessary goods. And I hope that our witnesses can offer key and, if possible, specific recommendations that could be followed by us in Congress and the Federal Government as a whole, as well as inform action by our universities, private corporations, and the laboratories.

I yield back the balance of my time.

[The prepared statement of Mr. Maffei follows:]

PREPARED STATEMENT OF RANKING MEMBER DAN MAFFEI

Thank you Chairman Broun for holding this hearing today.

The challenge at our national labs and other facilities is controlling access to the information and inventions that are truly deemed to be highly sensitive without obstructing the positive interaction that occurs between scientists. Still, as we see on a routine basis, other nations and foreign corporations regularly attempt to steal, siphon or subtly acquire U.S. government secrets or proprietary data that has high technological and scientific value for their economy or national security.

Identifying specific espionage threats, developing safeguards against them and forewarning American scientists about these expanding and evolving threats is an important task. But it is a task that has to be balanced against the costs of overreacting and unnecessarily inhibiting the advance of scientific understanding. This hearing will help illuminate the tradeoffs.

I look forward to hearing from our witnesses today about how to strike the right balance between international scientific cooperation and ensuring the protection of critical key data or research. I hope that our witnesses can offer key recommendations that could be followed by the Federal government as well as inform actions by our Universities and private corporations.

Yield back.

Chairman BROUN. Thank you, Mr. Maffei. We have these huge problems with cyber attacks upon business and national labs and cyber security should be at the forefront of what all of us here in Congress focus upon because we have a tremendous potential of

economic espionage and scientific espionage, and thank you so much for your opening remarks.

If there are any other Members who wish to submit additional opening statements, your statements will be added to the record at this point.

Now, at this time I would like to introduce our panel of witnesses. Our first witness is Dr. Charles Vest, President of the National Academy of Engineering and President Emeritus of the Massachusetts Institute of Technology.

Our second witness is Dr. Larry Wortzel, the Commissioner of the U.S.-China Economic and Security Review Commission. Dr. Wortzel is a former Army Counterintelligence Special Agent. Thank you for your service in the Army, sir. I am a Marine and I appreciate your service. You are a former Marine, too? Oorah.

Our third witness is Ms. Michelle Van Cleave, Senior Fellow at the Homeland Security Policy Institute at the George Washington University. Ms. Van Cleave is also the first national counterintelligence executive and has previously served as counsel on this Committee. Welcome back. We are glad to have you. Welcome, Ms. Van Cleave.

Our final witness is Mr. David Major, Founder and President of the Centre for Counterintelligence and Security Studies. Mr. Major is a veteran FBI Special Agent and experienced counterintelligence educator.

As our witnesses should know, spoken testimony is limited to five minutes each if you could please try to restrain yourselves. I know this is a big topic, but if you can, please keep it within the five minutes. I am not going to gavel you down if you go over, but if you could, please limit it to five minutes and after which the Members of the Committee will have five minutes each to ask questions. Your written testimony will be included in the record of the hearing.

Now, it is the practice of this Subcommittee on Oversight to receive testimony under oath. If you would all please stand. I should ask you, do any of you have an objection to taking an oath?

Okay. Let the record reflect that all of the witnesses indicated they have no objection to taking the oath.

Now, if you would raise your right hand.

Do you solemnly swear or affirm to tell the whole truth and nothing but the truth, so help you God?

Thank you. You may be seated. Let the record reflect that all the witnesses participating have taken the oath.

Now, I recognize our first witness, Dr. Vest, for five minutes. You are on, sir.

**TESTIMONY OF DR. CHARLES M. VEST, PRESIDENT,
NATIONAL ACADEMY OF ENGINEERING**

Dr. VEST. Openness of research and education accelerates discovery, contributes to worldwide advancement of knowledge and technology, and enhances American leadership, economy, diversity, and values. I also understand the importance of security. I served on the independent Intelligence and Weapons of Mass Destruction

Commission appointed by President George W. Bush, and I am a trustee of In-Q-Tel.

Here are three things I believe in: the “Leaky Bucket Theorem.” It is far more important to keep filling our bucket of science and technology than it is to obsessively plug every little leak; second, high fences around the small areas of scientific results and technology that truly must be denied to others through classification; and finally, competing and cooperating with other nations and institutions.

Export control and visa policy remain somewhat rooted in the Cold War when we had a single enemy. Our dominant security asset was technology superiority; the Soviet Union’s was a huge military. Secrets were more easily maintained and military technologies were mostly separate from consumer products. That ended in 1989. Today, we face diffuse threats like terrorism. We no longer singularly dominate the world’s science and technology. We are subject to the instant and open communications of the Internet and the World Wide Web. Our military and intelligence agencies are very dependent on commercial products, our companies have global supply chains, open innovation, manufacturing facilities, customers, suppliers, and research laboratories all over the world.

In 1982, Executive Order 12356 broadened the government’s authority to classify defense-relevant information that stated basic research information not clearly related to national security may not be classified. However, the government soon forced last-minute withdrawal of the 150 technical conference papers on the subject of cryptography.

President Ronald Reagan responded to the resulting vigorous debate by issuing National Security Decision Directive 189 that stated, “It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted.”

The horrific 9/11 attacks raised new questions about our openness. Globalization of modern industries complicated these questions. Visas denied to many foreign students, visitors, and conference participants in the United States reflected legitimate concerns, overreaction, bureaucratic foibles, risk aversion, antiquated systems, good intentions, bad policies, heart-rending personal experiences, and, finally, slow-but-steady improvement.

My views on scientific technological and educational openness are based on five considerations: America’s traditional values and strengths, the nature of basic science and technology, U.S. science and engineering workforce, the value of a well-educated world, and national security writ large. America’s economic and military strength and leadership are made possible by our unique combination of democracy, market economy, investment in research and advanced education, and diversity. There is no longer a singular threat like the Soviet Union or an economically surging Japan, and our world is integrated by digital communication and expanding talent base from new markets everywhere, so we must compete and cooperate.

Here is a specific example. In 2011, the U.S. and Chinese Academies of Engineering held a joint meeting of experts to discuss the future of the Global Navigational Satellite Systems. We discussed

applications to consumer products, transportation, agriculture, and science. It was noted that the codes enabling civilians to use the U.S. GPS signals are openly published whereas the codes for the non-defense new Chinese system called Compass are closed and unavailable. If both systems could be used, accuracy, coverage, reliability, and safety would be improved for all.

The CEO of one of our largest U.S. GPS companies explained that in our country, the government launches and maintains the satellites and provides open codes for their use. Entrepreneurs then bring useful applications to market. Soon after this joint meeting, the Chinese made the codes for Compass openly available. Perhaps we contributed to this decision by cooperating as well as competing.

In summary, openness is very important to the United States in the 21st century, but our policies have a long and continuing history of sometimes getting unnecessarily in the way. When this occurs, there are three simple guidelines my colleagues and I follow at MIT: one, obey the law; two, reject grants or contracts incompatible with institutional values; three, analyze and give voice to needed reforms in Federal policy or its implementation.

Finally, I commend to you our 2009 National Academies report titled "Beyond Fortress America: National Security Controls on Science and Technology in a Globalized World," that was authored by a highly experienced committee co-chaired by retired General Brent Scowcroft and Stanford University President John Hennessy.

Mr. Chairman, I would be pleased to respond to questions. Thank you.

[The prepared statement of Dr. Vest follows:]

Testimony of

Charles M. Vest
President, National Academy of Engineering
The National Academies

before the

Committee on Science, Space, and Technology
Subcommittee on Oversight
U.S. House of Representatives
"Espionage Threats at Federal Laboratories: Balancing Scientific Cooperation while
Protecting Critical Information"

May 16, 2013

Chairman Broun, Ranking Member Maffei, I am Charles Vest, president of the National Academy of Engineering (NAE) and president emeritus of the Massachusetts Institute of Technology (MIT). I have spent my career in higher education and research, and have served on the boards of major corporations. I am a proponent of openness in education and research, and I hope to explain the value of such openness.

I also understand the importance of security, having served on the independent Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction appointed by President George W. Bush, and I am a trustee of In-Q-Tel, that identifies, adapts, and delivers innovative technologies to support the missions of the CIA and the broader intelligence community.

I believe in openness of education and research to accelerate discovery, contribute to the worldwide advancement of knowledge and technology, and to enhance America's leadership, economy, diversity, and values.

My views support what is called in the vernacular "the Leaky Bucket Theorem," that when it comes to research and technology, it is far more important to keep filling our bucket than it is to obsessively plug leaks. I also believe in high fences around the small area of scientific results and technology that truly must be denied to others, i.e. critically important secrets should be classified, and we should minimize security mission creep and the bureaucracy that wastes time on over-classification and grey areas such as so-called Sensitive but Unclassified Research.

Openness is highly valued throughout the science and technology communities; it has three major dimensions:

1. Open flow of ideas, i.e. scientific and engineering knowledge;
2. Open flow of people, i.e. international students, faculty, and employees; and
3. Open flow of technology products and devices.

These three flows are frequently stemmed by counterproductive or unduly applied policies that many believe will harm our national security, technological leadership, and our economic competitiveness in the long run.

HISTORICAL POLICY CONTEXT

The basic point is this: Our policies regarding export controls and visas are rooted in the Cold War when two superpowers faced off against each other. The dominant security asset of the U.S. was our technological superiority; that of the Soviet Union was a huge military. It was more or less possible to maintain secrets from each other, and military technologies were more or less separate from consumer products.

The Cold War ended in 1989. Today, a quarter century later, we face very different diffuse threats such as terrorism; we no longer singularly dominate the world's science and technology; we are subject to the instant and open communications of the Internet and World Wide Web; our military and intelligence agencies are very dependent on commercial products; and our companies have global supply chains, open innovation, manufacturing facilities, customers, suppliers, and research laboratories all over the world.

Three world-changing events have driven the development or reexamination of U.S. policies regarding the flow of scientific and technical knowledge, non-U.S. citizens, and commerce:

1. The Cold War,
2. The advance of Japanese consumer manufacturing, and
3. Post 9/11 terrorism.

The Cold War Era

Cold War policy regarding the balance between openness and security began soon after the end of World War II. Even in that early context, in 1947, President Truman's Scientific Research Board stated:

Strict military security in the narrow sense is not entirely consistent with the broader requirements of national security. To be secure as a Nation we must maintain a climate conducive to the full flowering of free inquiry. However important secrecy about military weapons may be, the fundamental discoveries of researchers must circulate freely to have full beneficial effect. Security regulations therefore should be applied only when strictly necessary and then limited to specific instruments, machines or processes. They should not attempt to cover basic principles of fundamental knowledge.

In 1982 Executive Order 12356 broadened the authority of the government to classify defense-relevant information, but the order stated that *Basic scientific research information not clearly related to national security may not be classified*. There was much debate about the interpretation of this sentence, and great uncertainty about how it would be applied. An answer soon came. As an optics researcher, I attended a meeting of the Society of Photo-Optical Instrumentation Engineers, in San Diego in August 1982. Under government pressure, and with less than ten days notice, scientists and engineers withdrew presentation of more than 150 technical papers on the subject of cryptography.

The vigorous debate that was launched by the quashing of basic cryptography papers was more or less settled in September 1985 when President Ronald Reagan issued National Security Decision Directive 189 (NSDD 189) that stated:

It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. ... that where the national security requires control, the mechanism for control of information generated

during federally funded fundamental research in science, technology, and engineering at colleges, universities and laboratories is classification.

Each federal government agency is responsible for: a) determining whether classification is appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification procedures; b) periodically reviewing all research grants, contracts, or cooperative agreements for potential classification.

No restrictions may be placed upon the conduct or reporting of federally funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes."

Japanese Competition

The issues of export controls and visa policy gained currency again in the very late 1980s and the 1990s. This time around, the issues were even more complicated because they were driven as much by industrial competitiveness as they were by traditional military security issues. The rise of Japan in particular as a major economic power was driven by their sudden dominance in high-quality, high-throughput manufacturing of consumer products such as electronics and automobiles.

There were strong pushes to bar international students from university research programs because it was believed by many that foreign countries, especially Japan, would send students and visitors to our universities and laboratories to master our technology in order to return home and use it against us economically. It certainly is true that during this period the Japanese created a playing field that was unfairly tilted by their import restrictions. But they also completely outpaced us through their quality movement and through their advantage of building new "greenfield" manufacturing facilities. However, the fundamental problem was that much of American industry had become fat and lazy through the days in which we totally dominated. Eventually, they woke up and did the

terribly hard but effective work to become competitive again. This coupled with a huge thrust forward of American entrepreneurship in new fields like information technology and biotechnology got our economy moving again. I conjecture that our manufacturing sector gained more value from learning about high-quality production from the Japanese than they gained from learning about our technology. I also am confident that U.S. openness to foreign citizens and the open flow of information were, and are, dominant forces in our success as high tech entrepreneurs.

Post 9/11 Terrorism

The horrific attacks on our nation on 9/11 quite naturally raised many new questions and perspectives about our traditional openness to those from other nations and about the open flow of scientific and technological knowledge. This was compounded by the rising realities of the Internet and World Wide Web, and by the globalization of modern industries and their supply chains. It accelerated after the dot-com economic bubble burst, and a national paranoia about leaking technological knowledge and mild xenophobia recurred. This played out particularly in the blocking of visas to foreign students, visitors, and participants in conferences held in the U.S. Since 9/11, this has been a complicated mixture of legitimate concerns, overreaction, bureaucratic foibles, risk aversion, antiquated systems, good intentions, bad policies, heart-rending personal experiences, and, finally slow but steady improvement. During this period, in November 2001, then National Security Advisor Condoleezza Rice, acting on behalf of the President, stated that pending further review and updating of export control policies, "... the policy on the transfer of scientific, technical, and information set forth in NSDD-189 shall remain in effect, and we will ensure that this policy is followed." Unfortunately, at the working level, this statement frequently did not appear to be implemented.

Starting in the late 1990s, universities began to be told that the conduct of basic scientific research that utilized satellite systems, and in some cases computer systems, were off-limits to foreign students and to collaborative efforts with other countries, even close friends like Japan. If non-U.S. citizens worked on projects and came into contact with

certain specialized equipment, the knowledge they gained was considered a *deemed export* of sensitive technology and they were either barred from the contact, or required to pass certain security reviews. Quiet, but essentially fruitless, discussions between university leaders and federal officials ensued, and in several instances universities turned down such contracts rather than accept restrictions on their students.

In my view, the application at the working level of policies regarding visas and deemed exports were and are, cases of policy schizophrenia. Both before and after 9/11, the dominant reason for rejecting students applying for visas to study in the U.S. appears to have been *immigrant intent*, i.e. the government was afraid that these prospective students would stay in the U.S. after they completed their studies. On the other hand, many policy makers simultaneously decried the fact that increasing numbers of international students who had studied here were returning to their countries of origin to contribute to the development of their economies and universities rather than to ours.

The traditional American welcome mat was withdrawn after 9/11. Although the situation has slowly improved, damage has been done and continues. The matters discussed here, together with larger geopolitical considerations, have created a far less favorable opinion of the United States in much of the world than that to which we are accustomed. For example, in 2005, the Pew Research Center asked 17,000 people from 16 countries “Suppose a young person who wanted to leave this country asked you to recommend where to go to lead a good life – what country would you recommend?” In only one of the 16 countries (India) was the U.S. the most frequently recommended country.

WHY OPENNESS IS OF GREAT NATIONAL VALUE

My views on the critically important value to U.S. national interests of maximizing the flow of scientific and technological knowledge and people are driven by five considerations:

1. America’s traditional values and strengths,

2. The nature of basic science and technology,
3. U.S. science and engineering workforce,
4. The value of a well-educated world, and
5. National Security writ large.

It is my belief that America's modern economic and military strength and leadership have been made possible by our unique combination of democracy, market economy, investment in research and advanced education, and diversity. As fundamental as these factors are, they are threatened or damaged by bureaucratic restrictions on openness beyond those classified areas that truly must be maintained as national secrets. Simultaneously, we are disinvesting in the research universities and scientific infrastructures that make our success possible, even as many other countries have learned from us and are implementing the policies and making the investments in which we used to lead. As I noted at the beginning of this testimony, it is more important to keep filling our scientific and technological bucket than to obsessively plug the leaks.

Here is an example of what our openness has brought to America: At MIT we are very proud of the Nobel Laureates who teach and work on our campus. Those who received their Nobel Prizes in recent decades were born in the United States, India, Germany, Italy, Mexico, and Japan. Similarly, the recent Laureates from the University of California were born in the United States, Taiwan, Poland, France, Hungary, Germany, Austria, and Norway.

These scientists, as well as countless others, came to the U.S. because of our openness and investments, and because American colleagues understand that science thrives in unfettered communication among scientists everywhere. Indeed, the conduct of science requires criticism and testing of the repeatability of experiments by other scientists. Scholarly pursuits more broadly require access to knowledge and artifacts, and are strengthened by criticism and exploration from different vantage points. One need only look back to the history of the Soviet Union to understand that science, even science practiced by brilliant and well-educated scholars, cannot flourish in isolation. In a similar

vein, advancing and improving commercial technology benefits by open discussion and pre-competitive cooperation.

Let me turn to my deep concern about the future of the U.S. engineering workforce. This is the Knowledge Age, and to be able to compete and lead in the global marketplace, we need people with knowledge – especially engineering knowledge. But here is the reality: Across Asia, more than 21 percent of university graduates today are engineers. Across Europe, about 12.5 percent of university graduates are engineers. In the United States, only 4.5 percent of our university graduates are engineers. The primary reason that we haven't already been economically steamrollered is obvious: we import engineering talent. Talented immigrants now comprise a large percentage of our engineering and scientific faculties, and just over 50 percent of our engineering PhD students are non-U.S. citizens. And in 1998, Chinese and Indian CEOs alone were running around one quarter of the companies in Silicon Valley, accounting for \$16.8 billion in sales and more than 58,000 jobs. In 2005, immigrants founded 25 percent of U.S. startups and the fraction of immigrant-founded Silicon Valley startups was 52.4 percent. These figures are now declining as individuals find improving opportunities in other countries and as we squeeze our institutions. From 2009 through 2012, the number of applications to U.S. graduate schools from overseas increased about 10 percent annually; for 2012-13, these applications grew by less than 2 percent. And from 2009 through 2012, the number of applications to U.S. graduate schools from China increased about 20 percent annually; for 2012-13, these applications declined by about 5 percent.

These warning signs about our future engineering and technical workforce must be taken seriously. They reflect many things, particularly the deep problems of STEM education in our K-12 system and a popular culture that broadly does not value science and engineering. But they also reflect the impact of policy and negative perception about declining openness and opportunity at a time when opportunity is rising elsewhere in the world. In the long run, if these trends continue, it is likely that loss of scientific leadership and decline in the talent base available to us will cause serious economic and security damage.

Another important topic regarding openness is education, not only on our campuses, but also through the Internet and World Wide Web. As I have indicated, damaging restrictions on access to our universities and research institutions were threatened or implemented in the 1990s. Post 9/11, pressures for restriction on foreign students and scholars intensified, and discussions in Washington considered barring non-U.S. citizens from even studying certain subjects in our universities. Fortunately, many of these pressures and considerations subsided. Today, initiatives such as MIT's OpenCourseWare and MOOCs (Massively Open Online Courses) offered by both non-profit and for-profit university consortia like edX and Coursera represent another form of openness valued by the academic community.

In many ways, these movements were initiated by MIT's OpenCourseWare program that makes the basic course materials such as detailed lecture notes, course syllabi, reading lists, problems sets, examinations, etc. available on the web at no cost for anyone who wishes to use them. They have been used by millions of teachers and self-learners all over both the developed and developing worlds. The materials can be used in whole or in part, added to or modified, and tuned to local needs and contexts. This and other open courseware programs have brought value to students and teachers around the world and have created very positive images of the United States as a generous nation.

MOOCs and other advanced on-line learning tools are in their infancy. But already it is clear that they reach very large numbers of students throughout the world and directly provide actual education to them, often with mechanisms for feedback on homework assignments and exams. While these initiatives and organizations deliver aspects of what is best in American higher education to massive numbers of students who might or might not be able to come to the U.S., most of us believe that a well-educated world is a better world in the long run. They reflect U.S. leadership despite the fact that they contribute knowledge, learning, and opportunity to those who will compete with us in the future.

Our national security is no longer a straightforward matter of dominance in weapons technology over a well-defined threat such as the Soviet Union during the Cold War. Our national security now and in the future is primarily a matter of science- and technology-driven economic strength in a highly competitive and thoroughly integrated world economy. While recognizing that a narrow segment of truly critical technologies needs to be protected by well-enforced classification, I believe our national security generally is best served by maximizing openness of scientific discourse and knowledge, pre-competitive technologies, and education.

COMPETING AND COOPERATING: THE 21ST CENTURY REALITY

Finding the right balance between openness and security of our citizens and institutions is not always easy. And it plays out as much, or perhaps even more, in the industrial and economic domains than in traditional national security domains. Just as there no longer is a singular military threat from the Soviet Union, there also is not a singular economic threat such as a surging Japan. The world and its institutions are now connected and integrated by instant digital communication, readily shared knowledge, an expanding talent base, and the accelerating emergence of new markets in every corner of the world.

Just as there is a modest slice of technology secrets that must be classified, so too must industry expect effective patent systems to protect truly valuable intellectual property. But in general, the response of our companies to this new age has been to become far more open. First, in recognition of growing markets and capabilities, they have moved many of their operations to countries where the new consumer bases and talent are. No matter where they produce goods or deliver services, their supply chains are now global networks. For example, it is reported that the new Boeing 787 is assembled from 132,000 engineered parts manufactured in 545 locations around the globe. Furthermore, companies have moved dramatically to Open Innovation, i.e. they no longer do everything themselves; rather, they acquire technology from wherever it is found in the world, including sometimes from their own competitors. These interactions have also led to situations in which some intellectual property (IP) is not held as closely as in the past.

Some elements of IP are readily shared and frequently even given away. In other words, the world of business and industry is becoming more open, and what have emerged are new balances in which companies, and indeed nations both compete and cooperate.

A powerful example of global openness by businesses is found with Apple's development of the iPad. By openly sharing the necessary information about its computational codes and promulgating standards, Apple created a worldwide industry of "App" developers, most of them creative young individual entrepreneurs.

So in many ways, competition and cooperation are the yin and yang of the 21st century. We must do both, and federal policy surely affects our ability to do so

Let me give a specific example: In 2011, the U.S. National Academy of Engineering (NAE) and the Chinese Academy of Engineering (CAE) held a joint meeting of experts in Shanghai to discuss the future of Global Navigational Satellite Systems (GNSS). This is the system of satellites and ground-based facilities that make possible the GPS systems on which we are very dependent today. The Chinese are building a navigational satellite system called *Compass* that will be their equivalent to the U.S. GPS system. The NAE brought a delegation of our top experts from universities, business, DOD, and the State Department, including the individual who led our original project to deploy the GPS system. The Chinese delegation was equivalent in stature and included the government official in charge of *Compass*. Unfortunately, experts from NASA had to withdraw from our meeting at the last minute because of Congressionally imposed restrictions on NASA interactions with the Chinese.

In our meetings, we discussed applications to consumer products, transportation, agriculture, and science. It was noted in particular that the codes that enable civilians to access and use the non-defense U.S. GPS signals are openly published and available to anyone, whereas the Chinese codes that would make possible similar uses of COMPASS were closed and unavailable. If we could make commercial and scientific use of both the U.S. and Chinese systems, the redundancy would improve accuracy, coverage, reliability,

and safety for all. A highlight of the meeting was when the founder and CEO of one of our largest GPS companies explained that in the U.S. the role of the government is to launch and maintain the satellite system and provide open codes for its use. Entrepreneurs and others in the private sector then find useful applications and bring them to market. I believe that such open discussion and cooperation, as well as market-based competition, should characterize interactions in the 21st century.

Although I have no basis to claim direct cause and effect, soon after this joint meeting, the Chinese made the codes for *Compass* openly available. This is what I mean by both competing and cooperating.

CLOSING COMMENTS

It has been my intent to present a case for maximizing openness in science, technology, and education, as well as to present both historical and current policies that sometimes get in the way. How should universities and other research institutions respond to outdated or misapplied federal policies? I believe the answer has three simple parts, and my colleagues and I tried in my years as MIT's president to follow them:

1. Obey the law.
2. Reject grants or contracts incompatible with institutional values.
3. Analyze and give voice to needed reforms in federal policy or its implementation.

The views I have expressed here are mine, but they are very consistent with recent work by the National Academies. In particular, I commend to you our 2009 report, *Beyond Fortress America: National Security Controls on Science and Technology in a Globalized World*. The highly experienced committee that drafted that report was co-chaired by Gen. (ret) Brent Scowcroft and Stanford president John Hennessy. Its opening passage makes its general findings clear:

The export controls and visa regulations that were crafted to meet conditions the United States faced over five decades ago now quietly undermine our national security and our national economic well-being. The entire system of export controls needs to be restructured and the visa controls on credentialed foreign scientists and engineers should be further streamlined to serve the nation's current economic and security challenges.

Beyond Fortress America, presents four specific findings and three recommendations, each with several specific action items that would be required for its implementation. The recommendations themselves are:

Recommendation 1. *The President should restructure the export control process within the federal government so that the balancing of interests can be achieved more efficiently and harm can be prevented to the nation's security and technology base, in addition to promoting U.S. economic competitiveness.*

Recommendation 2. *The President should direct that executive authorities under the Arms Export Control Act and the Export Administration Act be administered to assure the scientific and technological competitiveness of the United States, which is a prerequisite for both national security and economic prosperity.*

Recommendation 3. *The President should maintain and enhance access to the reservoir of human talent from foreign sources to strengthen the U.S. science and technology base.*

As I noted, the Scowcroft-Hennessy report contains details of many specific actions to implement these broad recommendations.

Mr. Chairman, thank you for the opportunity to present this testimony. I would be pleased to entertain questions.

Charles M. Vest

Charles M. Vest is President of the National Academy of Engineering and President Emeritus of the Massachusetts Institute of Technology.

Dr. Vest earned a BS in mechanical engineering from West Virginia University in 1963 and MSE and PhD degrees in mechanical engineering from the University of Michigan in 1964 and 1967 respectively. In 1968, he joined the faculty of the University of Michigan as an assistant professor; he taught in the areas of heat transfer, thermodynamics, and fluid mechanics, and conducted research in heat transfer and engineering applications of laser optics and holography. He and his graduate students developed techniques for making quantitative measurements of various properties and motions from holographic interferograms, especially the measurement of three-dimensional temperature and density fields using computer tomography. He became an associate professor in 1972 and a full professor in 1977. In 1981, he turned much of his attention to academic administration, and served as the university's associate dean of engineering (1981–1986) and dean of engineering (1986–1989) before becoming provost and vice president for academic affairs.

In 1990, Dr. Vest was elected president of the Massachusetts Institute of Technology (MIT) and served in that position until December 2004, when he became professor and president emeritus. As president of MIT, he was active in science, technology, and innovation policy; building partnerships among academia, government, and industry; and championing the importance of open, global scientific communication, travel, and sharing of intellectual resources. During his tenure, MIT launched its OpenCourseWare (OCW) initiative; cofounded the Alliance for Global Sustainability; enhanced the racial, gender, and cultural diversity of its students and faculty; established major new institutes in neuroscience and genomic medicine; and redeveloped much of its campus.

In 2007, Dr. Vest was elected to serve as president of the US National Academy of Engineering (NAE) for six years. Under his leadership, the NAE promoted the Grand Challenges for Engineering, a set of 14 critical challenges for engineers in the 21st century, which, if achieved, will improve the quality of life for humankind. This effort spawned a number of Grand Challenges Summits at universities around the United States and has contributed to improved public understanding of the value and importance of engineering advances to the well-being of the nation and the world.

Dr. Vest presided over the international expansion of the NAE's Frontiers of Engineering (FOE) program to include partnerships with China and the European Union. In 2009, he launched the annual NAE Frontiers of Engineering Education symposium series, aimed at identifying and propagating innovative approaches to engineering teaching and learning. He also initiated a major new NAE effort to understand and address changes in global manufacturing-design-innovation value chains and their implications for US employment, education, and competitiveness. And under his leadership, the NAE in 2011 undertook a novel partnership with the US Institute of Peace to consider how the application of technology and of knowledge and methods from engineering and science can serve the goals of conflict prevention, peacemaking, and peacekeeping.

In addition to strengthening and augmenting the strategic programs of the NAE, Dr. Vest exercised his visibility as NAE president to great effect during his tenure, playing a prominent role nationally and internationally in illuminating forces reshaping the landscape of engineering research, practice, and education, and in defining the attributes future engineers will require to compete and lead in the emerging global economy.

Dr. Vest was a director of DuPont for 14 years and of IBM for 13 years, and vice chair of the US Council on Competitiveness for 8 years. He also served on various federal committees and commissions, including the President's Committee of Advisors on Science and Technology (PCAST) during the Clinton and Bush administrations, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, the Secretary of Education's Commission on the Future of Higher Education, the Secretary of State's Advisory Committee on Transformational Diplomacy, and the Rice-Chertoff Secure Borders and Open Doors Advisory Committee. He serves on the boards of several nonprofit organizations and foundations devoted to education, science, and technology. He has authored a book on holographic interferometry and two books on higher education. He has received honorary doctoral degrees from 17 universities. He was awarded the 2006 National Medal of Technology by President Bush and received the 2011 Vannevar Bush Award from the National Science Board.

Chairman BROUN. Thank you, Dr. Vest. I appreciate your testimony.

Now, I will go to my fellow Marine. We can talk about why you left the best service to go to the Army later on offline. But now, Dr. Wortzel, you are recognized for five minutes.

**TESTIMONY OF DR. LARRY M. WORTZEL, COMMISSIONER,
U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION**

Dr. WORTZEL. Chairman Broun, Ranking Member Maffei, Members of the Committee, thanks for the opportunity to appear before you today.

China is putting in somewhere in the area of \$1.5 trillion in its 2006 Medium to Long-Term Plan for the Development of Science and Technology, and the expenditure will go from 1.7 percent of GDP to about 2-1/2 percent of GDP by 2020. That is still less than we spend.

But for the purpose of this hearing, it really doesn't matter what they are spending. We should be focusing on the fact that China is saving an incalculable amount of time, money, and research effort through espionage and intellectual property theft. And that science and technology cooperation programs certainly are vital to China and help foster better cooperation between China and the United States, but there remains a substantial espionage threat posed by Chinese nationals that are working at U.S. labs.

The U.S.-China Economic and Security Review Commission in its annual reports have reviewed how China acquires foreign technology through traditional espionage and through cyber espionage, and we have recommended that Congress provide additional funding and emphasis on export control enforcement and counterintelligence efforts to detect and prevent espionage.

I have to say there is sort of a natural tension between maintaining scientific openness and preventing espionage. Dr. Vest talked about National Security Decision Directive 189 and that was in 1985, but in 2010 and 2012, the Office of the Secretary of Defense in two other reviews really reaffirmed that decision, that fundamental research, basic and applied research has to remain open, and anything else is probably going to cripple our universities, cripple our companies, and cripple our graduate education.

So if there is one place you might focus, it is on this dividing line between fundamental research and applied technology development. Where is that? It is a little opaque to me. And second, you might look at specific new or emerging technologies that require additional protection. The Army argues that developments in biological agent research, robotics, information and cyber systems, nanotechnology, and explosives or energetics should get a little bit more attention. And other services want to look at integrated circuit technology, new materials and processes. So I think there is room for that.

I also think there is a lot of room for better education in the labs and in universities because you have to know what the cover organizations are that these researchers come in under. Some of them—almost all of the intelligence collection organizations I have

had familiarity with in China have cover organizations, and most people don't know them, including a number of new FBI agents.

The other thing to think about when you look at China is you really have to consider the political environment in the home country of a particular researcher. You are dealing with a citizen of an authoritarian state that is ruled by a single party. The Chinese Communist Party runs the country, runs the police, the intelligence agencies, and the judiciary. They are all members of the Communist Party. And any resident that applies to study overseas or for a visa is essentially a potential hostage to party dictates. And that is in a country that has no rule of law.

People in China that apply for these passports are often interviewed by the security services. Their future employment, where their relatives live, their relatives' employment is subject to a great deal of pressure. So—and there is no right of refusal for citizens of China if a government asks them to gather information.

Thank you for the opportunity to make this testimony and I am happy to answer any questions you have.

[The prepared statement of Dr. Wortzel follows:]

**“Espionage Threats at Federal Laboratories: Balancing Scientific Cooperation while
Protecting Critical Information”**

Testimony of Larry M. Wortzel

before the House of Representatives

**Committee on Science, Space and Technology Subcommittee on Investigations and
Oversight**

May 16, 2013

Chairman Broun, Ranking Member Maffei, members of the sub-committee, thank you for the opportunity to testify today. I will discuss balancing scientific cooperation, the protection of critical information, and the espionage threat from China. As a member of the U.S.-China Economic and Security Review Commission, I will present some of the Commission’s findings on China’s science and technology policy and its goals, priorities and strategies with respect to the United States. The views I present today, however, are my own.

A report prepared for the U.S.-China Economic and Security Review Commission makes it clear that China’s *2006 Medium to Long-term Plan for the Development of Science and Technology* sets goals “of becoming an innovative nation by 2020 and a global scientific power by 2050.”¹ In order to achieve this goal, the Chinese government has invested a great deal of money and effort in subsidizing industry, insisting on transfers of science and technology to China when approving foreign investment, and funding over fifty nationally directed science and technology parks.² It looks as though China will invest about \$1.5 trillion in strategic emerging sectors in the next five years with research and development spending expected to increase from 1.7 percent of GDP in 2007 to 2.5 percent of GDP by 2020. For the purposes of this hearing,

however, we should be focused on the fact that China saves incalculable amounts of time, money and research effort through espionage and intellectual property theft.

The Chinese Academy of Sciences operates 100 research institutes and there are more than 45,000 other research institutes and laboratories in China responsive to Beijing's direction and planning.³ This nationally directed infrastructure seeks to obtain technology from foreign firms in key scientific areas that often have military application. Many of China's researchers and scientists have trained at U.S. institutions or have worked in U.S. firms, also adding to the transfer of American technology.

Science and technology cooperation programs are vital to China's own long-term goals, but they also help foster bilateral cooperation between China and the United States. However, there also is a substantial espionage threat posed by the large number of Chinese nationals working at U.S. laboratories and academic institutions. The counterintelligence education web site maintained by the Federal Bureau of Investigation highlights the "insider threats" posed by foreign intelligence collection to research, technologies, and intellectual property ostensibly protected by export controls.⁴ Indeed, of the ten incidents of "insider threat" espionage cited by the FBI, six cases are related to China. Three former U.S. officials, Mike McConnell, former Director of National Intelligence; Michael Chertoff, former Secretary of Homeland Security; and William Lynn, former Deputy Secretary of Defense, said in a January 27, 2012 *Wall Street Journal* opinion piece that: "The Chinese government has a national policy of espionage in cyberspace, pointing out that "it is more efficient for the Chinese to steal innovations and intellectual property than to incur the cost and time of creating their own." This cyber espionage takes place alongside or in conjunction with other forms of espionage.

The U.S.-China Economic and Security Review Commission's annual report of 2007 reviews how China acquires foreign equipment and technology to support its defense industrial base and documents six espionage prosecutions related to China.⁵ That annual report recommended that Congress provide additional funding and emphasis on export control enforcement and counterintelligence efforts to detect and prevent espionage. In 2009, the Commission's annual report to Congress addressed espionage conducted by Chinese state-controlled research institutes and commercial entities.⁶ In 2012, the Commission recommended that Congress ask the National Academy of Sciences for an assessment of Chinese strategies to acquire technology and to identify the extent to which industrial espionage has been used as a tool to advance China's interests.

According to the National Counterintelligence Executive, "of the seven cases that were adjudicated under the Economic Espionage Act (18 USC 1831 and 1832) in Fiscal Year 2010, six involved China." An article in a March 2012 manufacturing newsletter notes that "there have been at least 58 defendants charged in federal court related to Chinese espionage since 2008."⁷ China's targets have included are stealth technology, naval propulsion systems, electronic warfare systems for our ships and aircraft, and nuclear weapons.

There is a certain natural tension between the goal of preventing espionage by China (or any other country) and maintaining scientific openness. National Security Decision Directive 189 (NSDD 189), of September 21, 1985, makes it clear that U.S. national policy is that "to the maximum extent possible, the products of fundamental research remain unrestricted;" when restrictions are needed, the answer is that the products be classified as national security information according to U.S. statute.⁸ The directive went on to define "fundamental research" as "basic and applied research, the results of which ordinarily are published and shared broadly

within the scientific community, as distinguished from proprietary research from industrial design, production, and product utilization, the results of which are restricted for proprietary or national security reasons.” In a 2010 memorandum to defense agency heads and military department secretaries, then Under Secretary of Defense for Acquisition, Technology and Logistics Ashton B. Carter restated Department of Defense policy on fundamental research to ensure that it followed NSDD 189. He also instructed the Department of Defense that where controls are needed, classification of the product is the “only appropriate mechanism.”⁹

This tension between what needs to be protected for national security and openness in scientific research is not new. In 1984, when I was a credentialed counterintelligence special agent for the Army and an investigator for the Counterintelligence and Security Policy Directorate of the Office of the Secretary of Defense, I had personal experience with this issue. In the interest of scientific cooperation and openness, a U.S. government computer data base containing oceanographic data such as bathymetric readings, undersea currents, and salinity was linked to computers in the Academy of Sciences of the Union of Soviet Socialist Republics. Some of these data were collected by U.S. Navy oceanographic research ships. The Department of the Navy approached the Office of the Secretary of Defense and the National Security Council expressing concern that although the information was fundamental research, sharing it with Moscow presented a national security concern. According to the Navy, the stored data sets provided a great deal of information critical for submarine navigation and could support the launch of ballistic missiles from submarines. Members of Congress got quite upset about Navy and DOD attempts to restrict fundamental research and I was called upon to testify before the Oceanography subcommittee of the House Committee on Merchant Marine and Fisheries about the entire matter.¹⁰ Ultimately, research results that needed protection had to be classified. Now

here we are, thirty years later, still wrestling with the potential national security implications of foreign access to fundamental research.

I can suggest a few approaches that our nation might take. Obviously, perhaps it is time to once more evaluate the distinctions among basic, applied research and advanced technology development. What was true in 1985 may need to be updated to remain true today. To be candid, however, I think the scientific community and the country would come down in about the same place. A report on basic scientific research by the Defense Science Board last year did not suggest more controls on research, but instead recommended that the Department of Defense develop a technology strategy and remain involved in cutting edge basic research.¹¹ There are many threats to our security today, China included, but if we could live with open fundamental research during the Cold War, we can probably live with it today. After all, U.S.-China relations are substantially different than were U.S.-Soviet relations.

Instead of trying to restrict scientific research and experimentation, we ought to look more carefully at the institutions where research is being conducted and who is involved in the research. Also, some types of research may require more controls. In his May 24, 2010 memorandum on fundamental research, then Under Secretary Carter said that “there will be compelling reasons for DOD to place controls on some research that is performed on campus at a university, but such occasions should be rare and each must be scrutinized.”¹²

If laboratories or academic institutions are engaged in fundamental research and at the same time are involved in research on proprietary, export-controlled or classified matters, it is incumbent on the government or industry to ensure that foreign nationals do not get unauthorized access to export controlled or classified research. Also, the information systems of institutions

involved in controlled or classified research should be separate from those that are open to all researchers.

If a strong case can be made that there are some new or emerging technologies that require additional protection, that argument must stand up to public and scientific scrutiny. Leaders of the U.S. Army are most worried about developments in the areas of biological agent research, robotics, information and cyber warfare systems, nano-technology, and explosives or energetics. Other military services expand this list to include directed energy systems, chip and integrated circuit technology, and new materials and processes. At what point does research on these issues move from basic or applied research, which is “fundamental,” to research that requires export controls or classification? And does that standard of open fundamental research apply to every country in the world?

The FBI and the Defense Security Service, which administers the Defense Industrial Security Program, make the point that foreign nationals from some countries seem to have a higher track record of engaging in espionage. But they don’t give academia a list of those countries.

When you look at China, you must consider the political environment in the home country of a particular researcher. You are dealing with a citizen of an authoritarian state that is ruled by a single political party. The Chinese Communist Party runs the country, the police, intelligence agencies, the university heads, as well as members of the judiciary, who are all members of the Communist Party. All residents are potential hostages to party dictates in a nation that has no rule of law. People in China applying for passports and permission to study or conduct research overseas may be interviewed by the security services. The future employment of these individuals, their place or residence, and the residences and employment of their family

or loved ones is subject to Party dictates. A foreign national from China, or a state like China, is vulnerable to coercion and to having his or her loved ones held hostage. And there is no right of refusal for citizens of these states when the government asks them to gather information.

No policy on fundamental research will resolve this problem, however. It is up to American government security services and the FBI to appropriately administer programs that involve classified or export controlled information. And it is up to the government to ensure that foreign nationals do not get access to information that should not be disclosed to them.

In my personal view, Congress should direct the executive branch to maintain a classified list of countries, people and companies that pose a serious espionage threat to our government and industry. Such a listing could be validated across the intelligence community. When nationals from those countries are involved in research at places that also have programs involving classified or export-controlled information, it is up to the government to develop security and risk mitigations measures.

In 2012, a news article in *Bloomberg* used the attention-grabbing headline “American Universities Infected by Foreign Spies.”¹³ The story here is compelling, but the headline may be a little exaggerated. Certainly there are cases of foreign researchers attempting to gather export-controlled information or even engaging in economic espionage. But the infection is not a fatal one, nor is it so serious that we need to completely revise how we understand fundamental research. If we attempted to do that, we would probably cripple undergraduate and graduate education in the United States. However, some of the examples cited in this article are instructive. A Chinese researcher, Yu Xiaohong, allegedly attempted to conceal her academic background and make a visit to a researcher on celestial bodies and navigation at the University of Michigan. It turned out that she was from a Chinese People’s Liberation Army advanced

educational and research institution and had written an earlier paper on anti-satellite warfare. The U.S. professor she wanted to visit became suspicious of her intentions and stopped the exchange. In other cases, Chinese researchers have engaged in economic espionage or have taken trade secrets. The FBI has been pretty successful at prosecuting such cases. This suggests that Congress might provide more resources to the FBI and other federal agencies charged with protecting classified and export-controlled information to conduct more investigations and to increase education about the foreign intelligence collection threat. It is fair to assume that most of the researchers who apply for and undertake scientific and technical research for the government have the best interests of the United States at heart. If trained to be observant, they may report suspicious activity.

There is probably some utility to asking scientists to further develop concepts of the distinctions between applied fundamental research and developmental research. My sense is that the distinction is a little opaque, like the definition of “national security.”¹⁴ Executive Order 13526 or December 29, 2009, “Classified National Security Information,” says that “scientific technological, or economic matters relating to the national security” may be classified, and it goes on to define national security as “the national defense or foreign relations of the United States.”¹⁵ That still is rather ambiguous. It is clear, however, that if a university or laboratory is conducting research for the government, it is up to the government to set the standards for who may have access to the research, how the research is to be protected (if at all), and how fundamental research is to be segregated from developmental research with national security applications.

Those distinctions cannot be left to the security or intelligence community alone, because generally the experts there are not involved in advanced scientific research. Any effort at

determining when or if to restrict access to scientific research must involve members of the scientific community and industry. Some things, however, may be self-evident. We probably might want to take a harder look at graduate students from Iran or North Korea working on advanced explosive research or applied nuclear physics.

One example for ways to better-identify potential espionage threats to our national security and to screen nationals of the countries posing such threats is provided by some of the language in S. 884, the “Deter Cyber Theft Act.” In this bill, the Director of National Intelligence is directed to compile and report to Congress a list of foreign countries that engage in economic or industrial espionage and, among other things, a list of targeted technologies. Applying that approach to laboratories and universities engaged in advanced research would help oversight programs to be more cognizant of which foreign researchers get access to what government research projects. It would facilitate screening of foreign nationals working on government projects, and if the most critical technologies and processes for defense or national security application were prioritized, tell us where to be more discriminating in allowing foreign nationals access to research.

Finally, if there are new emerging technologies that require export controls to protect U.S. national security Congress should inquire as to what they are and oversee how such new controls are imposed.

¹ Micah Springut, Stephen Schlaiker, and David Chen, *China’s Program for Science and Technology Modernization: Implications for American Competitiveness*, A report prepared by Centra Technology Inc., Arlington, VA (Washington, DC: U.S.-China Economic and Security Review Commission, 2011), 6.

² Susan M. Walcott, “Chinese Industrial and Science Parks: Bridging the Gap,” *l. Professional Geographer* 54:349-364 (2002), http://libres.uncg.edu/ir/uncg/f/S_Walcott_Chinese_2002.pdf

³ Springut, Schlaiker and Chen, *China's Program for Science and Technology Modernization*, 18.

⁴ Federal Bureau of Investigation, *Counterintelligence*, "Higher Education and National Security: The Targeting of Sensitive, Proprietary, and Classified Information on Campuses of Higher Education," <http://www.fbi.gov/about-us/investigate/counterintelligence/higher-education-and-national-security>

⁵ U.S. China Economic and Security Review Commission, *Annual Report 2007* (Washington, DC: November 2007), 104-106.

⁶ U.S. China Economic and Security Review Commission, *Annual Report 2009* (Washington, DC: November 2007), 158-59.

⁷ <http://www.manufacturing.net/articles/2012/03/let-me-count-the-ways-china-is-stealing-our-secrets>

⁸ The White House, *National Security Decision Directive 198: The National Policy on the Transfer of Scientific, Technical and Engineering Information*, September 21, 1985.

⁹ The Undersecretary of Defense, Memorandum on Fundamental Research, The Pentagon, Washington, DC, May 24, 2010.

¹⁰ Subcommittee on Oceanography, Committee on Merchant Marine and Fisheries, House of Representatives, 98th Congress, Second Session, "U.S. Marine Scientific Research Capabilities Oversight," September 26, 1984, Serial 98-54.

¹¹ Office of the Under Secretary of Defense for Acquisition, technology and Logistics, *Report of the Defense Science Board Task Force on Basic Research* (Washington, DC: Department of Defense, January 2012).

¹² The Undersecretary of Defense, Fundamental Research, p. 2.

¹³ Daniel Golden, "American Universities Infected by Foreign Spies Detected by FBI," *Bloomberg*, April 8, 2012 <http://www.bloomberg.com/news/2012-04-08/american-universities-infected-by-foreign-spies-detected-by-fbi.html>

¹⁴ See Executive Order 13526 of December 29, 2009, "Classified National Security Information," *Federal Register*, 75:2, January 5, 2010, Part 1, Section 1.4 (e).

¹⁵ *Ibid*, Part 6, (cc).

Larry M. Wortzel, Ph.D.

Dr. Larry M. Wortzel has decades of experience in intelligence, international trade and economics, foreign policy, national security, and military strategy. He had a distinguished 32-year military career, retiring as an Army colonel in 1999. His last military position was as director of the Strategic Studies Institute of the U.S. Army War College. Dr. Wortzel spent four years an Army counterintelligence special agent and investigator assigned to the Office of the Secretary of Defense.

After his retirement from the Army, he was director of the Asian Studies Center of The Heritage Foundation and then vice president for foreign policy and defense studies at Heritage. Dr. Wortzel is a commissioner on the congressionally-appointed U.S.-China Economic and Security Review Commission.

Following three years in the Marine Corps and attending college, Wortzel enlisted in the U.S. Army in 1970. His first assignment with the Army Security Agency took him to Thailand, where he focused on Chinese military communications in Vietnam and Laos. Within three years he had graduated Infantry Officer Candidate School, as well as both the Airborne and Ranger schools.

After serving four years as an infantry officer, Wortzel shifted to military intelligence, assigned to the Intelligence Center Pacific, part of the U.S. Pacific Command, from 1978 to 1982. He then attended the National University of Singapore where he studied advanced Chinese and traveled in Asia. Wortzel was next assigned to the Office of the Secretary of Defense, developing counterintelligence programs to protect America from foreign espionage as well as investigating suspected espionage. He also managed programs to gather foreign intelligence for the Army Intelligence and Security Command.

From 1988–1990, Wortzel was Assistant Army Attaché at the U.S. Embassy in China, where he witnessed and reported on the Tiananmen Massacre. After assignments as an Army strategist and as an intelligence personnel manager, he returned to the American Embassy in China in 1995 as the Army Attaché.

In December 1997, Wortzel became a faculty member of the U.S. Army War College, serving as director of the Strategic Studies Institute. He retired from the Army as a colonel.

Dr. Wortzel's books include *Class in China: Stratification in a Classless Society* (Greenwood Press, 1987); *China's Military Modernization: International Implications* (Greenwood, 1988); *The Chinese Armed Forces in the 21st Century* (Carlisle, PA, 1999); and *Dictionary of Contemporary Chinese Military History* (Greenwood, 1999). He has edited six other books on China and contributed chapters to books on Chinese military history, war-fighting doctrine, and Asia-related strategy issues. His expert views on China and Asia have been sought by such publications as *The Wall Journal*, *The Washington Times*, *The New York Times*, *Tribune Newspapers*, *National Journal*, *Asahi Shimbun*, and *Sankei Shimbun*. Wortzel has appeared on *The PBS News Hour*, *The History Channel*, Fox News, CNN, MSNBC, BBC, and Al Jazeera. He is a member of the Council on Foreign Relations and the International Institute of Strategic Studies.

Wortzel's newest book, *The Dragon Extends its Reach: Chinese Military Power Goes Global* will be published by Potomac Books, Inc. next month (www.potomacbooksinc.com).

A graduate of the U.S. Army War College, Wortzel earned his B.A. from Columbus College, Georgia, and his M.A. and Ph.D. in political science from the University of Hawaii. He resides in Williamsburg, VA.

Chairman BROUN. Thank you, Dr. Wortzel.
Now, Ms. Van Cleave, you are recognized for five minutes.

**TESTIMONY OF HON. MICHELLE VAN CLEAVE,
SENIOR FELLOW, HOMELAND SECURITY POLICY INSTITUTE,
GEORGE WASHINGTON UNIVERSITY**

Ms. VAN CLEAVE. Thank you, Mr. Chairman and Members of the Committee. It is, as you say, a pleasure for me to be here because it is like old home week being back in the old Committee hearing room for me.

Chairman BROUN. Do you feel like you need to sit back up here somewhere?

Ms. VAN CLEAVE. Yes, sir. That is fine.

Chairman BROUN. Go ahead. Sorry.

Ms. VAN CLEAVE. But what I would like to do is just to take a second to tell you about another job that I had, which was in the last Administration as the National Counterintelligence Executive of the United States. I have to say it is the most fascinating job that no one has ever heard of and very relevant to the subject of today's hearing.

There were two major currents that led to its creation. One was in the wake of the Rick Ames espionage case. Ames had been spying for then the Soviet Union and later Russia for nine years deep within CIA and it was quite a shock to U.S. intelligence to discover that there had been such a damaging and horrible penetration into U.S. intelligence. So there were studies in the wake of that asking what had we missed? Why did we miss it? What were the seams that needed to be plugged?

And out of those studies came a recommendation from President Clinton that there should be created a National Counterintelligence Executive to head up all of U.S. counterintelligence. We had not in decades past since the inception of our current intelligence infrastructure ever had any individual position where all parts of U.S. counterintelligence would come together. So President Clinton, in an Executive Order, created this position, which was later put into law in 2002 by the Counterintelligence Enhancement Act passed by this body.

Second, in the wake of the end of the Cold War, there were a lot of other actors involved in intelligence activities against the United States. That included not only the more traditional targets of espionage of our national security secrets, but broader interests in the U.S. science and technology, our economic base, the riches of this country as well; and we didn't have a way within the U.S. Government to bring together policy and strategy to deal with this kind of threat broadly to the U.S. economy and society. So that was another current that led to the creation of the position of the NCIX, as the job is called.

And thirdly, I would observe—and this is from my experience with the job—that intelligence is an asset, a technique, resources, a set of tools that foreign powers use to advance their interests and disadvantage ours. And there is a question about how we think about those kinds of threats to the United States from the perspective of how we develop national strategy and policy. And that be-

came yet another responsibility of the office of the NCIX: to provide these kinds of policy options to the President and his national security team.

With that lengthy explanation, it brings me to why I think today's hearing is so important and the fact that the Oversight Subcommittee is taking on this subject.

The United States invests more in R&D on an annual basis than all of the G-8 combined. We are everybody in the world's number one target for collection because of that. This is where everything is. All the goodies of our R&D capabilities are resident here in the United States in the things that we do, and so we are everyone's number one target with the possible exception of some of our closest allies, and in that case, even some of those would find us their number one target.

And they are interested in virtually everything in our economy, in our economic activity, including, of course, our science and technology. This is not a new threat, but the point I want to convey to you is that these numbers are growing in terms of actors and reach and costs. It is true that during the Cold War we had a core unitary threat, and the fact that we had a unitary threat made it easier to deal with that. Today, the multiplicity of threat, multiplicity of actors makes it vastly more difficult to deal with. And these numbers have frankly overwhelmed our ability to deal with those kinds of threats given the current apparatus that we have.

Mr. Chairman, the report that you mentioned that the Pentagon released on Chinese military activities is significant for many reasons, but one of those reasons is that it is the first official acknowledgement that the Chinese have a dedicated program to acquire U.S. technology that is sophisticated, highly resourced, tasked, and very, very active and successful against us and they are not the only ones.

So how do we understand the costs of this? Well, the FBI estimated in the last Fiscal Year that economic espionage costs us about \$13 billion a year, but I would say that figure substantially underestimates the potential cost, first, because there is under-reporting. You don't see firms coming forward and saying we have been hit, so it is difficult to estimate all of that. Second, there is a dynamic cost in estimating—dynamic scoring if you will in understanding real economic costs. You know, what is the cost when we lose competitive ideas in our R&D base. And then thirdly, the whole cyber dimension, which is a hearing unto itself—“the largest transfer of wealth in history” as the Director of NSA has called cyber attacks against us.

So when you put all of those things together, we have a serious problem and it is growing worse every year, and reports out of government are worse every year. And so we talk every year about the need to balance. So the question back to this Committee is if things continue to grow worse at what point is it genuinely a terribly serious problem for the United States that there is this hemorrhaging of our technology?

I welcome your questions.

[The prepared statement of Ms. Van Cleave follows:]

Michelle Van Cleave
Senior Fellow, Homeland Security Policy Institute
George Washington University
Statement before the

House Committee on Science, Space, and Technology
Subcommittee on Oversight
May 16, 2013

***Espionage Threats at Federal Laboratories:
Balancing Scientific Cooperation while Protecting Critical Information***

Mr. Chairman,

Thank you for the opportunity to appear today to discuss the foreign intelligence threats to America's science and technology enterprise. Having served as head of U.S. counterintelligence under President George W. Bush, I can tell you that foreign intelligence services are far more active against us ... and far more successful ... than most Americans would ever imagine possible.

The most intense and dangerous foreign espionage efforts are directed against what we might call traditional targets, e.g., the secrets of our weapons laboratories, or the operational specifications of our intelligence satellites, or our military plans and capabilities, or the sensitive decision making apparatus of our government. But it doesn't stop there.

In fact, foreign collectors are interested in virtually all aspects of U.S. economic activity and technology, and their numbers are growing. According to Battelle's Congressional R&D Caucus brief, America invests some \$420 billion annually in R&D, more than all of the G-8 combined. So it is little wonder that we are the world's candy store for other powers looking to gain advantage on the cheap: by stealing it.

While some of this illicit activity may be opportunistic, the larger threats are purposeful and strategically directed and coordinated. As I will explain, this is hardly a new phenomenon but it is growing in significance and scope. Some of the very factors that historically have contributed to U.S. economic growth and technological progress have at the same time facilitated foreign entities' technology acquisition efforts against us. Human collection is integrated with cyber operations in ways that magnify the reach of both. And it is far from clear that our intelligence insights are deep enough, or our policies effective enough, to address the strategic implications of these threats.

This is a reality that is sharply at odds with the free and open values that underpin the world of science and research and the expansion of knowledge. As the National Research Council wrote in its 2007 study on science and security,

The task of achieving the appropriate balance between the need for rapid, open communication among scholars and the safeguarding of information that could be used to do us harm is a challenging one, and it is one that requires the continual and sustained attention of the scientific community. The... nation can and must strike this balance so that our extraordinary creativity and productivity can continue to flourish and propel us into a prosperous future.¹

The question is, is the current balance “appropriate”? And how would we know if it was not?

Russia

Let me begin by telling you a success story out of the Cold War. At their very first meeting, newly elected French President Francois Mitterrand brought President Reagan a very special gift. Mitterrand confided that French intelligence had a source, deep inside the KGB, who was providing unparalleled information about Soviet technology acquisition from the West. Thanks to this source, codenamed “Farewell,” western intelligence gained invaluable insights into Soviet intelligence tasking and collection operations directed against our R&D and technology base.

“Farewell” revealed that the Soviet Union had built an intricate network of state organizations to carry out focused and wide-ranging technology acquisition activities to support its military buildup. In addition to the KGB and the GRU (military intelligence), these included the State Committee for Science and Technology, the Ministry of Foreign Trade, and the State Committee for Foreign Economic Relations. The Soviet Academy of Sciences also played a role in obtaining documents and facilitating contacts.

Among other things, “Farewell” was able to provide the central Soviet “shopping list” for U.S. technologies. We learned that Soviet weapons production planning included express requirements for the acquisition of Western technologies or parts, as an integral feature in their weapons development work. So in effect, the U.S. was subsidizing the Soviet economy and in particular its military buildup.

The insights provided by “Farewell” – whose real name was Vladimir Vetrov -- played a significant role in our winning the Cold War. The Soviet economy was stretched thin and they depended on access to western technologies to support their military aims. With their “shopping list” in hand, the U.S. was able to join with NATO and other allies to control the export and sale of dual use technologies, as well as to undercut KGB “Line X” collection efforts through other creative means. For his part, after landing in jail for other reasons, Vetrov later was convicted of espionage by the Soviet authorities and executed.

¹ National Research Council of the National Academies of Sciences Committee on a New Government-University Partnership for Science and Security, Committee on Science, Technology, and Law Policy and Global Affairs, *Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security Communities* (Washington DC: The National Academies Press) 2007, p5.

Why dwell on this story from the Cold War Past? Well, (as that former U.S. President might have begun), because today, everything old is new again ... but with a better public relations campaign. Mikhail Fradkov, the current head of the SVR (the successor to the KGB) helpfully explains, "Intelligence aims at supporting the process of modernization of our country and creating the optimal conditions for the development of its science and technology."

Translation: "Farewell" may be out of business, but the old KGB Line X (technology acquisition) practices are not.

In fact, the numbers of Russian intelligence officers and operations in the United States today are easily at Cold War levels. The time and effort and treasure Russia devotes to these activities provide some indication of the rate of return Moscow gets from that investment. And with long practice, they know what they are doing – with the added advantage that, in the aftermath of the Cold War and with so many other demands on U.S. national security, we are perhaps not watching as closely as we once did.

China

Still, when it comes to stealing western technology, China is giving Russia a run for its money. China's intelligence services employ a full range of collection methodologies, from the recruitment of well-placed foreign government officials, senior scientists, and businessmen to the exploitation of academic activities, students populations, and private businesses. These Chinese intelligence efforts take advantage of our open economic system to advance China's technical modernization, reduce the US military advantage, and undermine our economic competitiveness.

According to the Defense Department's 2013 report on PRC military activities,

The Chinese utilize a large, well-organized network to facilitate collection of sensitive information and export-controlled technology from U.S. defense sources. Many of the organizations composing China's military-industrial complex have both military and civilian research and development functions. This network of government-affiliated companies and research institutes often enables the PLA to access sensitive and dual-use technologies or knowledgeable experts under the guise of civilian research and development. The enterprises and institutes accomplish this through technology conferences and symposia, legitimate contracts and joint commercial ventures, partnerships with foreign firms, and joint development of specific technologies. In the case of key national security technologies, controlled equipment, and other materials not readily obtainable through commercial means or academia, China has utilized its

intelligence services and employed other illicit approaches that involve violations of U.S. laws and export controls.²

So in a manner reminiscent of the old Soviet practices, China has an extensive government apparatus and highly coordinated tasking and collection activities targeting U.S. technologies. Consider also that these same tasking and collection operations can be and are put to use in acquiring intellectual property and other proprietary information of commercial value. And business is booming, thanks in part to growing employment of Chinese nationals in U.S. facilities as well as the off-shoring of U.S. production and R&D to facilities in China.

During the Cold War, we understood Soviet objectives to be adversarial to our own; and there was a western alliance of free nations working closely together to protect and preserve our collective security and advance our common prosperity. The United States had a carefully developed strategy concerning the Soviet Union, articulated in such seminal Presidential directives as Truman's NSC-68 and Reagan's NSDD-75. This strategic guidance also ordered our response to identifying and disrupting illicit technology acquisition activities by the USSR.

No such clarity of purpose exists with respect to U.S. interactions with China. In my view, some of the deficiencies in U.S. policy toward Chinese economic espionage and other illicit activities targeting U.S. R&D derive in no small measure from the absence of a larger strategic framework guiding U.S./Chinese relations.

Disturbing Trends

By far the vast majority of foreign acquisition of U.S. technology is open and lawful, as are the transactions of individuals and businesses involved in international commerce, as well as the free exchange of ideas in scientific and academic forums. But let me turn to the cases that fall outside the bounds of what is open and lawful – a category that is growing in scope and import.

The last year I was in office, we tracked efforts by foreign businessmen, scientists, academics, students and government entities from almost 100 countries to acquire sensitive U.S. technologies protected by export control laws or other means. Of those, the top 10 countries accounted for about 60% of the suspicious foreign collection efforts against cleared defense contractors. The two countries that always rank at the top of the list are of course Russia and China, which have particularized interests especially in dual use technologies with military application. But the top ten also included certain of our allies, who sometimes exploit their easy access to push the envelope into areas where they have not been invited.

In recent years, U.S. counterintelligence has observed more interaction among collectors from different countries and different regions. As the Pentagon's Defense Security

² Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013*, pp 11-12.

Service (DSS) explained last year, “Whether working with each other, working through each other, buying from each other, or attempting to throw suspicion on each other, these convoluted pathways make it more difficult to ascribe collection attempts to a particular country, region, or collector affiliation.”³

In other words, it’s a crowded field. And the prognosis is not good. According to the same DSS report, the total number of incident reports from industry in 2012 went up 75% over the past two years, continuing a relentless upward trend at roughly the same pace for the past decade.

In fact, each year the reports out of U.S. counterintelligence and security reflect figures that are worse than the year before. Losses are growing. Numbers of collectors are growing. Vulnerabilities are growing. And the erosion of U.S. security and economic strength is also growing. It reminds me a little of Senator Dirksen’s famous remark, “A billion here and a billion there and soon you’re talking about real money.”

Mr. Chairman, we’re talking about real money. For fiscal year 2012, the FBI estimated that losses to the United States from economic espionage totaled more than \$13 billion. Other analyses suggest that figure may significantly understate the true costs:

- **Underreporting.** As difficult as it is to track foreign efforts to acquire military and dual-use technologies—where defense contractors are required to report suspicious targeting incidents—it is far more challenging for the CI Community to monitor foreign targeting of purely commercial technologies. The FBI has outreach programs that are geared to encouraging US firms to report suspicious targeting incidents but, even so, such reporting is uneven at best. US firms have sometimes been reluctant to raise alarms about possible technology theft out of concern for the potential impact on investor and consumer confidence and stock prices.
- **Dynamic costs.** The National Science Foundation calculates that the U.S. invests about 2.8% of our GDP annually in R&D ... or some \$436 billion in 2012. R&D is the engine for new ideas and concepts and products and wealth. How much of that national treasure is targeted by foreign collectors to fuel their business and industry (and government programs)? What are the dynamic costs to the U.S. economy (in lost competitiveness, jobs, market share, etc.) as a result?

When one adds in cyber collection, the estimates of real losses skyrocket. The Director of the National Security Agency, General Keith Alexander, has called cyber espionage “the greatest transfer of wealth in history.” I would say that cyber exfiltration is of a piece with a global rats nest of technology and intellectual property theft.

³ Defense Security Service, *Targeting U.S. Technologies 2012: A Trend Analysis of Reporting From Defense Industries*, p6

Why are things getting worse?

Globalization has been wonderful for business and commerce and the free flow of ideas and information, bringing greater opportunities for trade, investment, growth, cultural and personal exchange and the expansion of knowledge.⁴ It has also been wonderful for spies.

Our general culture of openness has provided foreign entities easy access to sophisticated technologies. Each year, recognizing the mutual benefits of an unhindered exchange of information, we allow tens of thousands of official foreign visitors into US Government-related facilities such as military bases, test centers, and research laboratories. For example, NSF statistics show that 60% of postdocs employed at Federally Funded R&D Centers are foreign born nationals on temporary work visas. And each year, the counterintelligence community receives incident reports about foreign experts wandering into restricted areas, peppering U.S. researchers or scientists with questions well outside the range of issues they are supposed to discuss, and taking photographs of sensitive equipment that the foreign experts are not supposed to see.

The losses that result from such visits can be significant. Such foreign visitors are often among their nations' leading experts and, as such, may be much more effective at extracting sensitive information than would be traditional foreign intelligence officers. Specialists know their countries' or companies' specific technological gaps and can focus their collection efforts directly on the critical missing information. Finally, such experts are also in a position to recognize and exploit information that may be inadvertently exposed during visits.

And the technology losses to long-term foreign visitors can be even more significant than those to foreign experts making shorter visits. For one thing, overseas specialists who stay on site for extended periods of time become familiar with security procedures meant to limit their access to sensitive technologies. The insights thus gained may enable them to circumvent those security practices. This is particularly true of cyber security procedures. A long-term presence may allow visitors time to acquire passwords and to learn where on hard drives sensitive information is stored. Whereas short-term visitors are viewed as strangers on sensitive sites, long-term visitors become part of the landscape. Their activities naturally receive less notice, which enables them to wander into sensitive areas without attracting undue attention.

⁴ According to the U.S. Travel Association, there were over 62 million international arrivals into the United States in 2011. Between 2004 and 2011 (the most recent Commerce Department statistics) the number of Russian visitors to the U.S. more than doubled, with most of the increase in business and professional travel. The number of Chinese visitors over the same period more than quadrupled.

http://tinet.ita.doc.gov/outreachpages/download_data_table/2011_Russia_Market_Profile.pdf

By 2016, DoC forecasts that Russian visitors will be up another third, while the number of Chinese visitors will nearly triple again.

http://www.ustravel.org/sites/default/files/page/2009/09/US_Travel_Answer_Sheet_Jan2013.pdf

Similarly, American colleges and universities, centers for high-tech development, employ large numbers of foreign born faculty and train large numbers of foreign students, many of whom will return to their home countries. The vast majority of these are legitimately studying and advancing academic pursuits. But some are not.

Globalization has also mixed foreign and U.S. companies in ways that have made it difficult to protect the technologies these firms develop or acquire, particularly when that technology is required for operations overseas. Foreign direct investment in the United States currently stands at \$3.1 trillion – the highest on record, according to the Commerce Department. The Committee on Foreign Investment in the United States (CFIUS), which advises the President on the national security implications of proposed foreign investments and acquisitions, has seen its workload grow 75% in the last few years.⁵ Having had responsibility for providing intelligence assessments to the CFIUS when I served as the National Counterintelligence Executive (NCIX), I am concerned that our insights into the nexus of foreign business, industry and government programs fall short of satisfying those requirements.

And then there is the Internet. The information revolution is enabling once unimagined processing, transmission and storage of data, empowering the individual and opening our world to extraordinary new horizons. It has also altered the face and prospects for espionage, in scope and scale. The “Wikileaks” postings are but the tip of the iceberg of the challenge facing the government in protecting U.S. national security secrets, or industry protecting its proprietary information, or individuals protecting their privacy.

As this Committee is keenly aware, sophisticated information systems that create, store, process, and transmit sensitive information have become increasingly vulnerable to cyber exploitation. Many nations have formal programs for gathering our networked information, and foreign competitors are developing and employing the capability to exploit those vulnerabilities, interjecting a whole new dimension of national security threat and risk. The jury is out whether proposed legislative or other remedies will help better protect our nation’s information systems or deter or defeat cyber exploitation or attack.

What are they interested in?

Our national laboratories are the guardians of some of our nation’s most closely held and vital secrets. As such, they are targets of extreme interest by foreign powers seeking to acquire those secrets. The first time our nuclear weapons secrets were stolen, it led to a 50-year Cold War with the Soviet Union. In the late 1990s, the Cox Commission revealed that China acquired through espionage design information on all nuclear weapons currently in the U.S. inventory...and we still don’t know how they did it.

Other sensitive areas of federally funded R&D are clearly of great interest to our adversaries as well – as are the propriety secrets and intellectual property of American business and industry. The latest NCIX report on economic espionage assesses that the

⁵ Committee on Foreign Investment in the United States, *Annual Report to Congress 2012*, p3.

greatest foreign interest is in information technologies, military technologies, and civilian/dual use technologies in sectors likely to experience fast growth such as clean energy, health care, and pharmaceuticals.

In 2012, DSS found that the top four most targeted technology categories were unchanged from the year before: information systems, lasers, optics and sensors; aeronautics systems; and electronics. Armaments and energetic materials came in fifth, with a growing interest in technologies for processing and manufacturing, directed energy, and space systems.

I would invite the Committee's attention to the prominent position of aeronautics and space systems on the list of foreign interest. The launch of Sputnik some 56 years ago, which led to the creation of this Committee, was a technology challenge and a national security shock that profoundly changed the way the U.S. government approached science and technology. From that point forward, it did not require much of a visionary to understand that space would be critical to national defense – or that its enabling technologies would be coveted by adversaries and competitors.

The Chinese, in particular, are keenly interested in space technology, in which America is still the world's unquestioned leader. Just ask 30-year spy Dongfan Chung (Orange County, Calif.) or Shu Quan-Sheng (Newport News, Va.) or Lian Yang (Seattle), now serving time for passing inter alia space-shuttle communication technologies, space-launch cryogenic fuels data and satellite semiconductor devices, respectively. And that's just the tip of the iceberg.

Collection activities

There are significant intelligence gaps in understanding how foreign nations collect against U.S. technology. However, we do know that a number of the major foreign intelligence agencies have:

- Dedicated programs whose primary task is technology acquisition. These programs often involve the use of front companies, which operate surreptitiously.
- Laundry lists of targeted technologies and specific strategies for acquisition. Where an entire system cannot be acquired, foreign intelligence services may attempt to steal component parts.
- Arrangements to share technology that has been both legally and illegally acquired with other countries' intelligence and security services, even when the sharing of that technology is itself illegal.
- Programs that provide funding for students and businessmen who assist in collecting intelligence information.

In other words, foreign targeting of the U.S. science and technology base is driven by purposeful collection, tasking and exploitation by foreign nations who employ the full reach of their intelligence capabilities to that end. Moreover, the techniques used to acquire sensitive US technologies go beyond those traditionally associated with espionage. The rich network of human interaction, business and commerce that is innocent and open and above-board provides excellent cover for the sliver of activity that is none of that. Let me review some of these techniques.

In a majority of cases, foreign collectors simply ask, via e-mail, phone call, FAX, letter or in person – for the information or technology of interest. When a foreign request for U.S. technology is either refused by a US company or the US firm asks the foreign firm to apply for an export license, the foreign company often simply breaks off communication and looks for another possible US seller. With search costs extremely low, the foreign firm can afford to continue looking until it locates a US company that either does not understand the export licensing requirements or is willing to ignore them in order to make the sale.

U.S. businessmen, scientists and academics traveling abroad provide another valuable source of information for foreign countries. Foreign governments and businesses also acquire sensitive US proprietary information from all types of electronic storage devices, including laptop computers, personal digital assistants (PDAs) and cell phones carried by US businessmen traveling abroad. Foreign businesses and security services gain access to such information by using clandestine entry to hotels and business establishments or by electronically downloading information during routine security inspections at airports or other ports of entry. In addition, technology weaknesses in some PDAs make it easy for foreign entities to extract information without directly accessing the storage devices.

In some cases, foreign entities seeking to acquire sensitive US technologies find that the easiest route to acquisition is to either purchase outright or form a joint venture with a US firm that has access to that technology. Even joint venture negotiations where no agreement is reached can yield proprietary information valuable to foreign entities. The negotiation process often includes plant tours and inspections of manufacturing processes, and the US firms may provide proprietary information on customers and marketing plans in an effort to secure the deal.

One indirect method used to acquire U.S. technology is for foreign firms to offer their services or technology – particularly IT-related support – to U.S. firms that have access to sensitive items. Marketing pitches can elicit useful information. Sales can get foreign firms (and foreign collectors) inside the U.S. concern ... which may be all they need to walk off with sensitive proprietary information ... or to facilitate remote access to computer systems for future exploitation. Such deals, at a minimum, have provided foreign visitors access to facilities where trade secrets or proprietary information are stored. In their most dangerous forms, however, these deals can result in foreign companies subverting U.S. firms' supply chains by selling tainted products. These subversions could give foreign companies long-term, remote access to significant proprietary information and trade secrets. Well-executed supply chain subversions are almost impossible to detect, even years after implantation.

Foreign collectors may exploit joint research undertakings or visits to U.S. businesses, military bases, national laboratories, and private defense suppliers, to extract protected information. In particular, DSS noted that “[p]lacing academics at U.S. research institutions under the guise of legitimate research offers access to developing U.S. technologies and cutting-edge research” in such areas as information systems, lasers, aeronautics and underwater robots.

Foreign students, scientists, and other experts who come to the United States to work or attend conferences also serve as a funnel for sensitive U.S. technologies. For example, a student may seek a postdoctoral position or other job with a cleared contractor, thereby gaining access to sensitive or classified technologies to support parallel R&D efforts in their home countries. China, in particular, seems to be benefiting from the access its experts have here. The Chinese press explicitly recognizes the role of the overseas community in increasing China's technological prowess. Moreover, Beijing has established a number of outreach organizations in China to help maintain contact with its overseas community and facilitate technology transfer, groups such as the Overseas Chinese Affairs Office, the Chinese Overseas Exchange Association, the State Administration of Foreign Expert Affairs, etc. China also supports a number of US-based advocacy groups that facilitate its interaction with its experts here, including the Association of Chinese Scientists and Engineers, the China Association for Science and Technology, and the Chinese Institute of Engineers.

According to the FBI, ***foreign intelligence targeting of U.S. colleges and universities in on the increase.*** For example, in 2009 Michigan State University was approached by a Dubai based concern offering to fund their extension campus in Dubai – which (as reported in the press) later turned out to be a front for Iran; MSU said “no thanks.”. Attempts by countries in East Asia, including China, to obtain classified or proprietary information by “*academic solicitation*,” such as requests to review academic papers or study with professors, jumped eightfold in 2010 from a year earlier (as reported by DSS); such approaches from the Middle East doubled.

The late Sergei Tretyakov, the highest ranking Russian intelligence officer ever to defect while stationed in the United States, managed Russian intelligence operations out of New York from 1995 through 2000. In his words, “We often targeted academics because their job was to share knowledge and information by teaching it to others, and this made them less guarded than, say, UN diplomats.”⁶ This included satisfying collection taskings from Moscow such as “a study of genetically engineered food being done at New York University.”⁷

Increasingly, foreign entities need not even come to the United States to acquire sensitive technology but, instead, can work within their own borders. There, US firms

⁶ Former Deputy Resident Sergei Tretyakov quoted in Pete Earley, *Comrade J: The Untold Secrets of Russia's Master Spy in America After the End of the Cold War* (New York: G.P. Putnam's Sons, 2007) 196.

⁷ *Ibid* at 194.

have difficulty securing their secrets and have few legal protections once proprietary information has been lost. Globalization is forcing US companies toward a more diversified business model that includes foreign outsourcing and external partnerships. These arrangements, while making US firms more competitive by providing a source of inexpensive inputs, at the same time make sensitive US technologies more vulnerable.

Conducting due diligence on foreign partners is difficult, but the problem becomes far more complicated when the foreign partners themselves increasingly outsource to other firms. These trends not only leave U.S. firms more exposed to a direct outflow of technology but also make it difficult to guarantee that the foreign-provided inputs—particularly IT hardware and software—are free from Trojan horses or back doors that could be used later to extract sensitive technology.

It is difficult to determine how much of the theft of U.S. sensitive technology and intellectual property is being directed by foreign governments, rather than self-initiated by companies or academics or unscrupulous entrepreneurs. But the more we learn about illicit technology collection, the more we see patterns that reveal the hand of foreign government involvement. So for example the 2012 DSS report attributed a large number of cases to government entities which would likely have been designated “unknown affiliation” in the past.

Even where there may not be central government direction and control, most foreign governments that are involved do not discourage such theft and themselves benefit from the transfers. For example, Chinese universities and research institutes in particular have associations with their nation’s militaries, which means that students and academics are likely to contribute to military R&D following completion of their studies or research fellowships. Think of it as part of the study abroad experience to bring back something useful when you come home.

U.S. National Strategy and Policy

The history of technology security policy debates is long and contentious, and marked by a lack of clear authority or uniform practices, despite volumes of outside commissions, recommendations for improvement, and internal substantive reviews. Yet technology protection regimes are only as strong as their weakest link. Inconsistent practices among government agencies and especially the divide between national security departments and agencies on the one hand, and at-risk agencies not within the national security community on the other, are a persistent problem.

In my view, government policy is most effective when we coordinate the full range of public policy instruments so they are applied to strategic effect. Stopping the illicit foreign acquisition of sensitive U.S. technologies requires a combination of national security tools, including export control laws, diplomatic measures, industrial security arrangements, limits on foreign investment in strategic U.S. industries, and counterintelligence. Each of these merits scrutiny, to ask whether they are properly

conceived, resourced and implemented in light of the growing threats to the U.S. science and technology base and the fundamental values they are meant to protect.

It is also worth exploring what gaps may exist in national policy and strategy. For example, there are no post-employment restrictions on federal employees from going to work for foreign firms, even firms with close ties to the military. Accordingly, Huawei has been hiring key U.S. talent... including (according to press reports last year) the former head of the cybersecurity division of the Homeland Security Department. Former U.S. government employees are barred by law from disclosing classified information, to be sure; but they walk off the job with specialized knowledge and understanding informed by their intimate familiarity with sensitive programs and operations. When I stop to think what we could learn if the roles were reversed – if senior Chinese government employees were to be hired away by US companies secretly employed by the USG to penetrate Chinese markets or critical infrastructure – I find myself wondering if we shouldn't take a closer look at this particular revolving door.

Among other things, Congress has a vital role to play in advancing awareness of foreign intelligence activities directed against our R&D base, including such activities as today's hearing. Awareness begins with educating the S&T community and the public – as well as our national leadership -- about the threat. In that regard, the National Research Council Report, which I cited earlier, was occasioned in part at the urging of this Committee. The time may be ripe for the National Academies to commission a fresh look. Certainly in the six years since their last report was issued, foreign targeting and exfiltration of sensitive U.S. R&D and technology have risen sharply. Perhaps there is more that the S&T community could be doing to help.

The larger solutions fall to national policy leadership and the security disciplines. How do we weigh the risks of foreign visitors and researchers at our federal R&D establishments against the benefits of scientific exchange and the value of collaboration? Are existing vetting and security procedures well designed and enforced? How do we protect information of value in all its forms, from paper to digital to conversations in person or at a distance? Do security and awareness training enable personnel to understand why they are being asked to take safeguards, or are they just handed a set of rules?

And most significantly, do we have a national capability to counter foreign intelligence operations that threaten our economic prosperity and national security? The scorecard of America's counterintelligence enterprise falls short of the growing strategic foreign intelligence threats directed against us, to include the extraordinary creativity of our S&T enterprise. We need better insights into what foreign intelligence services are doing and how they are doing it, and a genuine national strategic counterintelligence program, so that we might stand a better chance of stopping them.

Conclusion

This is likely not the first time the members of this Committee will have heard that we are facing growing foreign intelligence threats targeting U.S. science and technology; indeed, I am sensitive to the fact that such warnings may sound like a broken record which, in time, loses its appeal. But I have endeavored today to provide some of the reasons why I believe you should take that warning to heart.

In closing, I want to say that it is a special honor for me to be here, having served as minority counsel to this Committee in 1989. Accordingly, I am familiar with the unique jurisdictional responsibilities of HSS&T, and I commend the Oversight subcommittee for taking on the difficult questions raised by today's hearing. I hope it will give you a starting point for more detailed inquiry into the security practices of our federal laboratories and related national policies affecting America's science and technology enterprise. Thank you and I look forward to your questions.

Michelle Van Cleave served as the National Counterintelligence Executive under President George W. Bush. As the head of U.S. counterintelligence, she was responsible for providing strategic direction to and ensuring the integration of counterintelligence activities across the federal government. She has also held senior staff positions in the Congress (including staff director, Senate Judiciary Subcommittee on Technology, Terrorism and Government Information; Minority Counsel, House Science, Space and Technology Committee; and professional staff member, House Appropriations Subcommittee on Foreign Operations), at the Pentagon working homeland defense policy in the aftermath of 9/11, and in the White House Science Office, where she served as Assistant Director and General Counsel under Presidents Ronald Reagan and George H.W. Bush. A lawyer and consultant in private life, she is also a Senior Fellow at George Washington University and a principal with the *Jack Kemp Foundation*, helping to establish and manage programs to develop, engage and recognize exceptional leaders.

Chairman BROUN. Thank you, Ms. Van Cleave. And that point is well-taken. And we would very much like to hear some prescription from all of you about how we should go forth legislatively to try to make sure that the tension between openness and security is met. As a physician, as a medical doctor, and as a scientist, I understand the importance of openness of research and development, but this is a tremendous tension. And thank you, Ms. Van Cleave. And if you all do have some ideas, we would like for you to present them to us later on, maybe answers to questions for the record.

Now, you look like an FBI agent. Mr. Major, you are recognized for five minutes.

Please turn on your microphone.

**TESTIMONY OF MR. DAVID G. MAJOR,
FOUNDER AND PRESIDENT,
THE CENTRE FOR COUNTERINTELLIGENCE
AND SECURITY STUDIES**

Mr. MAJOR. Yes. I have been studying espionage for 43 years, which makes me one of the oldest people in this room looking at this particular problem. Michelle and I were at the White House together in the Reagan Administration trying to put counterintelligence at the policy table, and since that time I have formed this company called CI Centre. It is a little red schoolhouse that tries to train people on the significance of counterintelligence, and we have trained over 100,000 people in the intelligence community on espionage and counterespionage.

And we take our information, we put it on an empirical basis, because what we have created is a thing called SPYPEDIA, and SPYPEDIA is a way we track espionage around the world every day and make it available to members who are a member of our—what is a membership webpage.

And if I would look at the United States, espionage is a big issue. In the United States from 1945, the end of Cold War to today, I can put some numbers on that and explain exactly the size of espionage as we see it today. Don't forget that during the Cold War, the Russians had 531 Americans who were their clandestine agents operating for them during the Cold War.

And since that time, how many cases have we had? Well, what we do is we track these cases based on these laws, economic espionage, and national security laws, classified information, and the private sector, and we use this—these criteria to track it, and where right now the big talk is about the insider threat, and that is what this hearing is about. The fact of the matter is the insider threat has always been with us and will be with us.

We say how many espionage cases have we had which has been legal action taken against the people who have acquired the information in the last 68 years? The answer is 564 people. Now, we look at espionage cases, technology transfer where they take the material itself, and technology acquired through—in the private sector. And if you notice, last year, we had 64 cases, the largest we have had. Notice the last ten years since 2000 there is an expansion, a growth, exactly as Michelle was talking about. The reality

of what we have on this issue, 564 cases, an average of 8.1 over that time period but not in the last 10 years.

Where are they coming from? Now, they are coming from the private sector. Over 260 people have been charged from the private sector and the government section also we see it. How are we doing catching spies? Well, one good news is one of these cases where a case related to national security information in which they were trying to acquire classified information were interdicted by the FBI before the person ever actually passed it. That is the good news. These two were at the National Laboratories and they were trying to acquire information for Venezuela. We have—and also three cases of Foreign Agent Registration Act. That is the good news.

Here is another bad news message. If we look at every case someone was an agent of a foreign power operating in the United States but hadn't been caught yet, we said how many agents are out there each year? Well, our average turns about to at least 25 who eventually get caught. And for 33 years the average has been above 25. The biggest we had is 53. Compare that to how many we caught and we are using catch to get the best of the years, 25 percent. So it is—continues to be a problem. It continues something we have to invest in.

Now, the average spy will last about 1 to five years, but they can do significant damage during that period. We say what countries are conducting espionage against the United States, and it turns out that obviously Russia, the Soviet Union is the largest, but China is coming up really quickly. Between 1949 and 2000 there were only five Chinese cases. Now, there are 100 cases. There have been 95 new cases in the last 13 years and they are the largest growth area has in Chinese cases that have led to legal action against the individuals. You can see the other countries.

But what is interesting here, we have tracked the countries. The dark blue represents national security cases, in other words, classified material; and the light blue represents private sector or corporate espionage, and you notice that China is a very large profile in the private sector espionage cases even though they have attacked classified information. Notice that Iran has never—has—they are only using diversion—or there is no national security Iran cases but they are the largest diverter of material. And if we look at Chinese cases, the 100, you notice what the trend line has been since the year 2000. If we also look at that compared to Russia, you can see how many cases that we have seen here in the United States.

We talk about foreign entities and declassified information. This shows you that it has been the Soviet Union and Cuba and China and Iraq and so forth. On economic espionage cases, what the target is, we have talked about—this is a great thing; it comes from scientific America and it shows you between research papers, patents, issues, expenditures, and higher education, the United States is number one. But if you go down to China, number three, and you go way over to the right-hand side, they are not even on the higher education side because they get here to get their education. And some of them stay and then steal information and pass it on to China.

If you look at cases of economic espionage, you can see the trend line. The red line is the number of cases. The blue line is the number of people. Because of economic espionage cases, you are normally looking at 1 to 1.8 per case. It is more of a conspiracy than it is an individual by themselves. But the company benefitting from economic espionage cases have been China, Taiwan, South Korea, India, Japan. Eighty-five percent of all these cases come from Asia. That is where the majority of these kinds of cases are coming from.

If you look at domestic and foreign cases, you can see China, Iran, Russia. These are the actors in this side of the issue. Why—what are they targeting? I think very revealing that the number one target is information systems. They are targeting our information systems to get the technology to do external targeting of our information. So they do cyber warfare by using our information to then attack us externally. So they internally acquire it and then use that to externally target us. And it is across the board the kinds of information they are targeting.

Why target the United States? As I said, information technology, industrial information, military information, and business, it is across the board on what United States manufacturers. That is who is targeting us during this period.

On illegal exports, the exports are obviously increasing, primarily coming from Iran. And if we look at these cases benefitting China, Iran, Russia, Taiwan for illegal export cases.

So that is what we are finding in SPYPEDIA as we track this, and excuse me for going a minute over on that. I will answer any questions you have on this material.

[The prepared statement of Mr. Major follows:]

**“Espionage Threats at Federal Laboratories:
Balancing Scientific Cooperation while Protecting Critical Information”**

**Subcommittee on Oversight
Committee on Science, Space & Technology**

Thursday, May 16 2013 – 2 to 4 pm
2318 Rayburn House Office Building

Opening Statement of David Major
President and Founder of the CI Centre and SPYPEDIA®

My name is David G. Major and I am a retired FBI Supervisory Special Agent. During my career in the bureau from 1970 to 1994 I specialized in counterintelligence and counterterrorism. I was the first FBI agent to be appointed to the National Security Council, advising the President of the United States on counterintelligence policy and issues. Prior to joining the FBI I spent 5 years in the US Army as an officer in the Armor Branch. As a result of my experience at the White House, I recognize the need to establish a center of excellence to train personnel on the strategic importance of the counterintelligence discipline. From 1994 to 1997 I was a subject matter expert to the USIC on counterintelligence. In 1997 I established The Centre for Counterintelligence and Security Studies® (CI CENTRE) as a veteran-owned small business with its facility in Falls Church, VA. We provide over 55 commercial, off-the-shelf unclassified training courses and briefings for the US Intelligence Community and corporate clients on:

- Counterintelligence Strategy, Tactics & Skills
- Security Awareness Training & Briefings
- Interviewing & Investigations
- Counterterrorism Strategy, Tactics & Skills
- Area/Country Studies; Foreign Intelligence Services

Our training is designed to enhance an organization’s mission and to protect their information, facilities and personnel from foreign intelligence collectors, global terrorists and competitor threats. We have trained over 100,000 Intelligence Community, Military, Law Enforcement, Homeland Security, Government and Corporate employees over the past 15 years.

To ensure we remain current and relevant for our classes, the CI Centre has maintained a highly robust research and analyst capability of worldwide espionage, economic espionage, cyber security, and terrorist events and cases. In 2011 we began to make our database available via a membership site, SPYPEDIA®. This is a one of kind open source database that provides it members a rich source of counterintelligence, counterterrorism, and security-related information that is updated daily. We collect worldwide government documents, reports, analysis, case studies, in a deep digital library. The SPYPEDIA® staff reviews this material daily to produce original analysis that highlights trends, issues, lessons learned and key information essential to assist our customers to enhance their security posture.

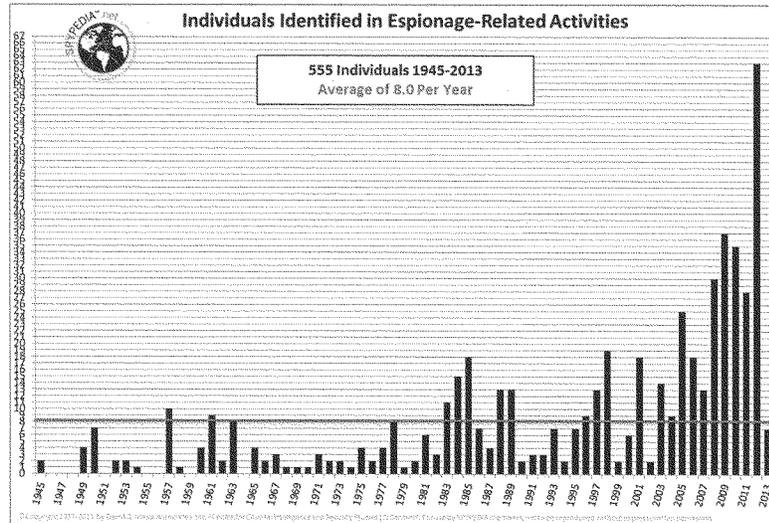
US Government agencies and personnel, corporations, universities and private citizens are members of SPYPEDIA® to meet a variety of their individual diverse needs and interests.

We have studied espionage extensively and have come to some empirical conclusions that provide both a big picture and micro study of espionage. In our study of the Espionage threat to our nation and more specifically the Federal Laboratories we have made some observations that I would like to highlight for the committee.

We collect espionage data for the period of 1945 to the present looking at the following individual charges to draw our conclusions.

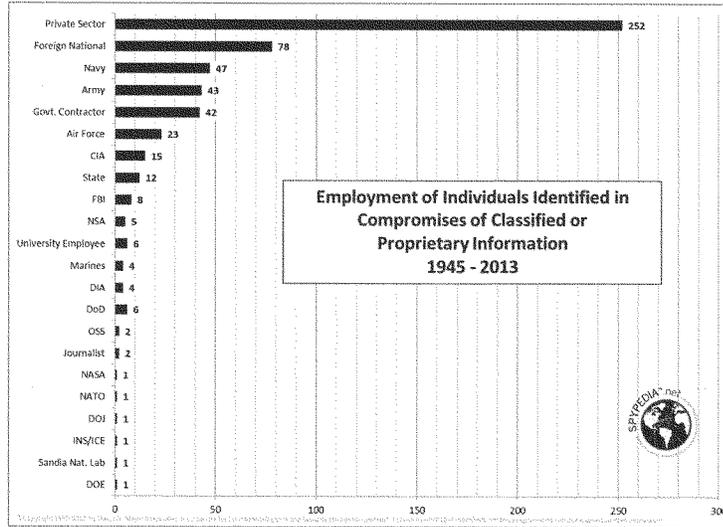
- Foreign Nationals charged
- “Espionage” related arrests for violation of
 - US Code Title 18, Section 793 and Section 794
 - FARA US Code 18, Section 951
 - Economic Espionage, US Code 18, Section 1831 and Section 1832
 - Violation of US Code Title 18 Section 1001
- Individuals who defected pending arrest
- Individuals who committed suicide pending arrest
- Individuals who diverted technology for foreign governments in violation of International Traffic in Arms Regulations (ITAR)

We have identified at least 555 individuals that meet these criteria.

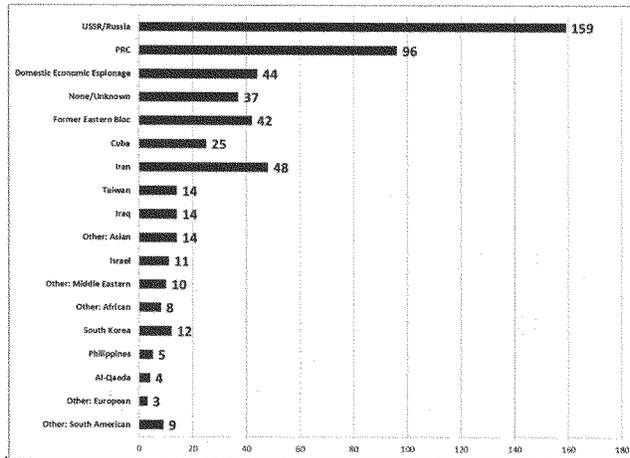


© Copyright by DGMA, Inc. 1992-2013 all rights reserved; reproduction in any form is expressly prohibited without prior written permission.

The vast majority these individuals are from the private sector with 252 cases and 78 foreign nationals.

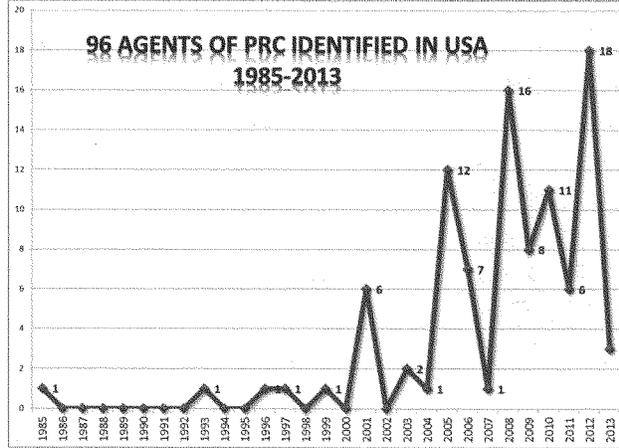


There are 31 countries identified in the public record as responsible for conducting the “espionage related cases” with the USSR/Russian and the People’s Republic of China (PRC) having the largest number of cases.

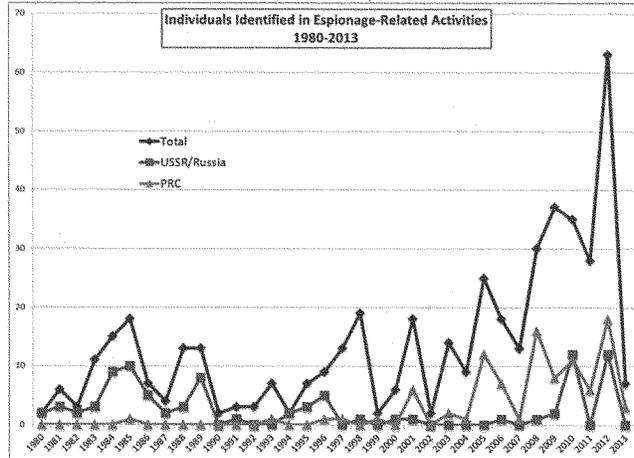


Copyright by DGMA, Inc. 1992-2013 all rights reserved; reproduction in any form is expressly prohibited without prior written permission.

The largest increase by country has been the PRC which has been associated with a total of 96 cases with only 5 cases between 1949 to 1999 (50 years) and 91 cases from 2000 to 2013. There have been more PRC cases than Russian cases in 9 out of the past 13 years and an equal number the other 4 years.



There have been 70 Economic/Trade Secret theft cases involving 113 people since 1996. Thirty (30) of the 70 cases were domestic US cases, while in the remaining 40 cases the beneficiary of the theft was a foreign country. The PRC was the beneficiary of 67.5% of these 40 cases.



© Copyright by DQMA, Inc. 1992-2013 all rights reserved; reproduction in any form is expressly prohibited without prior written permission.

Is it the insider or outsider, US citizen or Foreign national who are stealing economic/trade secret information? The average industrial/economic spy is in their mid-40s. There are very few cases of the impulsive 20 year old we see in traditional espionage cases. Instead they are often relatively accomplished professionals who make calculated, deliberate efforts. They are majority male.

If a person is an insider, they use their natural access to proprietary material. There are cases where insiders provided information for reasons of nationalistic loyalty or ideological reasons, a significant number are looking for personal economic benefit: to either sell the information directly, to bring that information to a firm with the promise of a better position, or to help start their own business in competition with their previous employer.

There were 46 people who worked alone and 66 who worked with conspirators who were eventually indicted. Forth-six (46) cases were perpetrated by individuals working alone and 24 multi-person cases. The number of domestic espionage cases and foreign economic espionage cases are roughly equal. There are slightly more individuals involved in the foreign cases. The domestic cases are perpetrated largely by US citizens, whereas the foreign cases involved Naturalized US legal residents and foreign nationals. People who provide information to foreign firms and governments are likely to have foreign attachments. Individuals with foreign attachments also make up a disproportionately large size of the workforce in the most heavily targeted industries. Portions of the world's scientific, math, and engineering talent is being produced in other parts of the world, so US tech firms naturally draw talent from overseas.

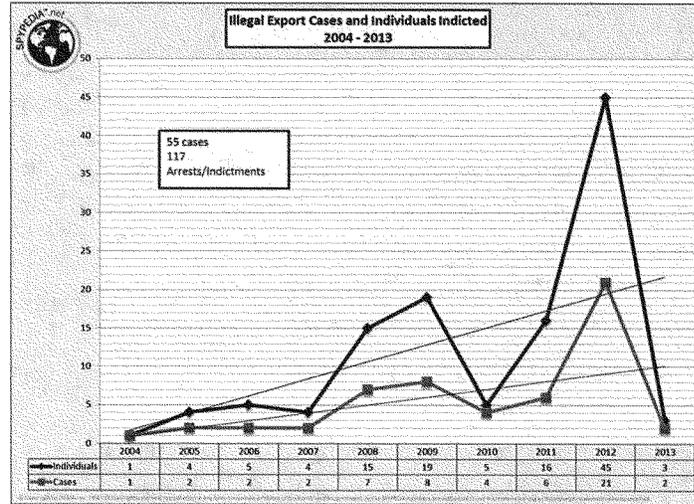
As for how this information is stolen, the majority of the subjects' simply downloaded protected files onto an external hard drive and other personal devices, or forwarded it via email. There are a few interesting cases where individuals traveled to foreign locations and gave lectures at universities/business conferences, and in doing so verbally disclosed protected information. There is only one case where a computer genius actually built "a computer within a computer" to have two separate -functioning hard drives within his work computer, and then used one of the hard drives to steal.

Some things to look out for from insiders: if the person is downloading an unusually large amount of information; if the person is accessing data that does not directly relate to their job requirements; if the person is undertaking a lot of travel to foreign countries, particularly if they are not reporting it. This is a problem since many of the naturalized US/foreign nationals have legitimate reason to travel and visit family; if the person is accessing data after work hours.

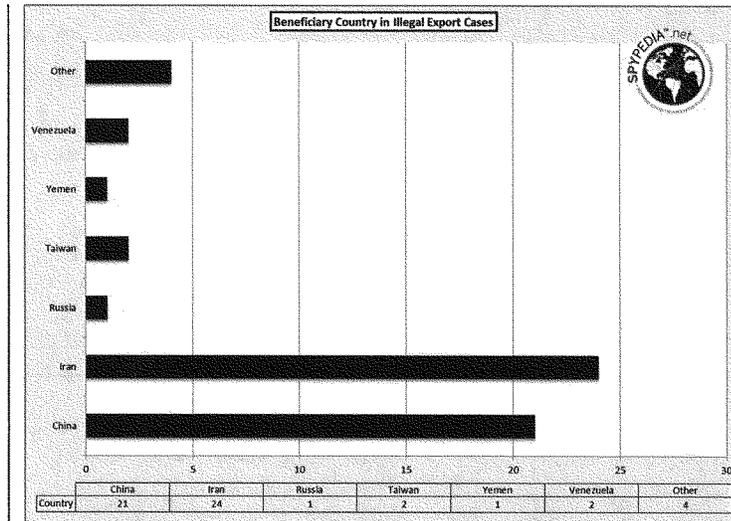
Some basic security procedure should be implemented and enforced in the Federal Laboratories:

- Foreign nationals in labs -- they need extremely robust real-time 100% computer monitoring
- Foreign nationals need to be sealed off from physical access to sensitive areas.
- The labs need vigorous and realistic training of cleared personnel regarding loose chatter to un-cleared personnel.

There have been 55 technology diversion cases involving 117 individuals



The PRC and Iran has been the biggest beneficiary of these diversion cases with 21 of the cases being PRC (38%) and 24 being IRAN cases (44%)



David Major Narrative Biography

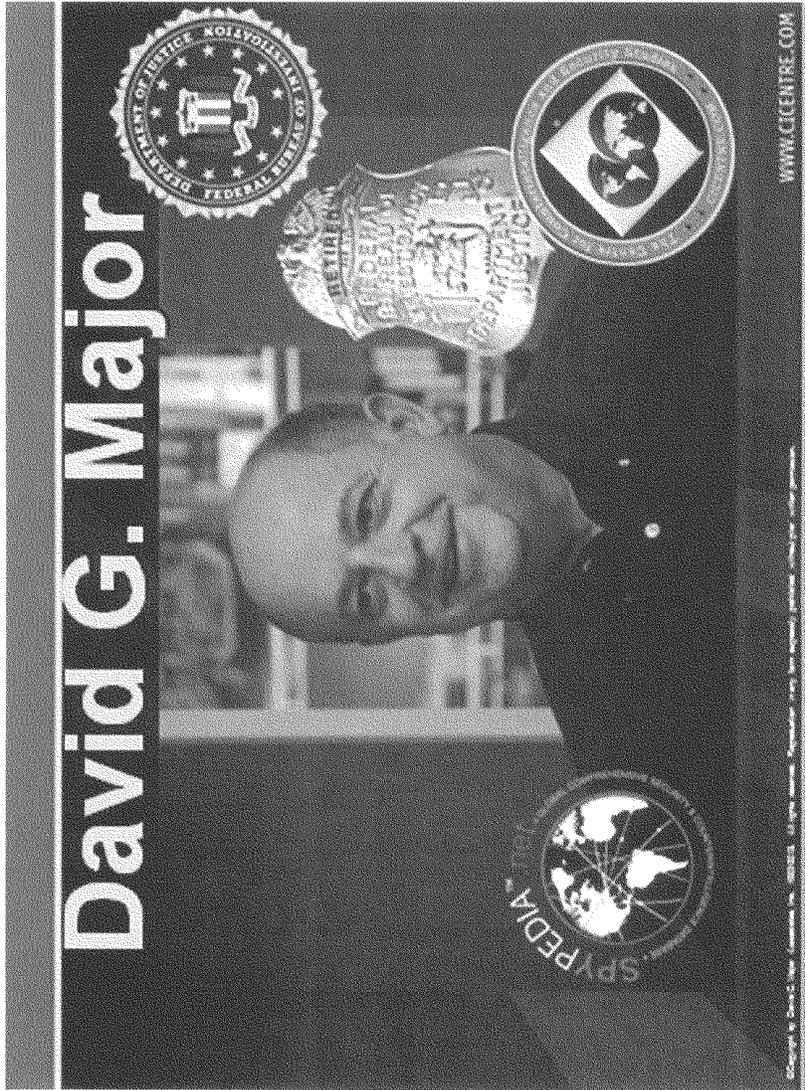
David Major, a retired FBI Supervisory Special Agents (1970-1994) has made a life-long commitment to the practice and study of counterintelligence and its subsets, counterterrorism, security making him one of the nation's top experts on the subject. His views and advice are sought after by the government, private companies and national and international media. A 1965 graduate of Syracuse University with a degree in the life sciences, after graduation Mr. Major served in the US Army as a Captain in Armor Branch for 5 years before being appointed an FBI Special Agent. He served in Sarasota Florida, Newark New Jersey, Washington DC, and Baltimore FBI as Field Offices as well as two assignments at FBI Headquarters in the Security Office, the Counterintelligence Division and the Inspection office.

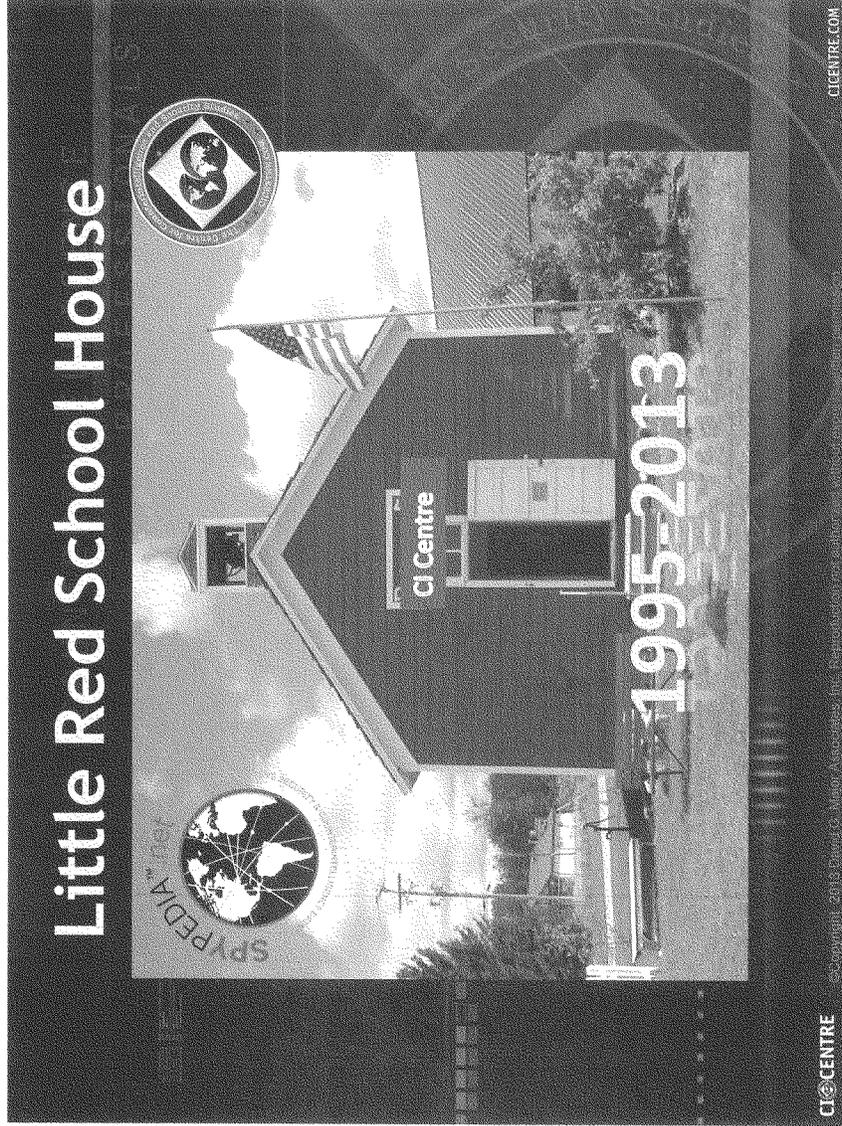
Major's skills and abilities propelled him to being named by the FBI to being the first FBI official to be assigned to the National Security Council as a staff officer. He served as the Director, Intelligence and Counterintelligence Programs in 1985 and 1986, and briefed and advised President Reagan on counterintelligence matters and security policy and programs.

Upon retiring from the FBI, Major founded the Centre for Counterintelligence and Security Studies to provide high-quality counterintelligence, counterterrorism, investigative skills, area studies and security training for the government, academic and corporate sectors of our society. The Centre has trained nearly 100,000 people in these topics since 1995 and has developed over 55 COTS seminars and courses.

SPYPEDIA®, the CI Centre's, robust counterintelligence, counterterrorism, cyber-attack and security database, is an excellent resource of cases, latest news, podcasts, videos, CI calendar events, quotes, reports, and more. SPYPEDIA® was in research and preparation for 15 years. It is continually updated, rich, open source database provides exclusive access for professionals in the counterintelligence, security, and counterterrorism disciplines; educators; authors; researchers; academia; students; and all who hold an interest in CI and CT.

SLIDES SHOWN DURING MR. MAJOR'S TESTIMONY

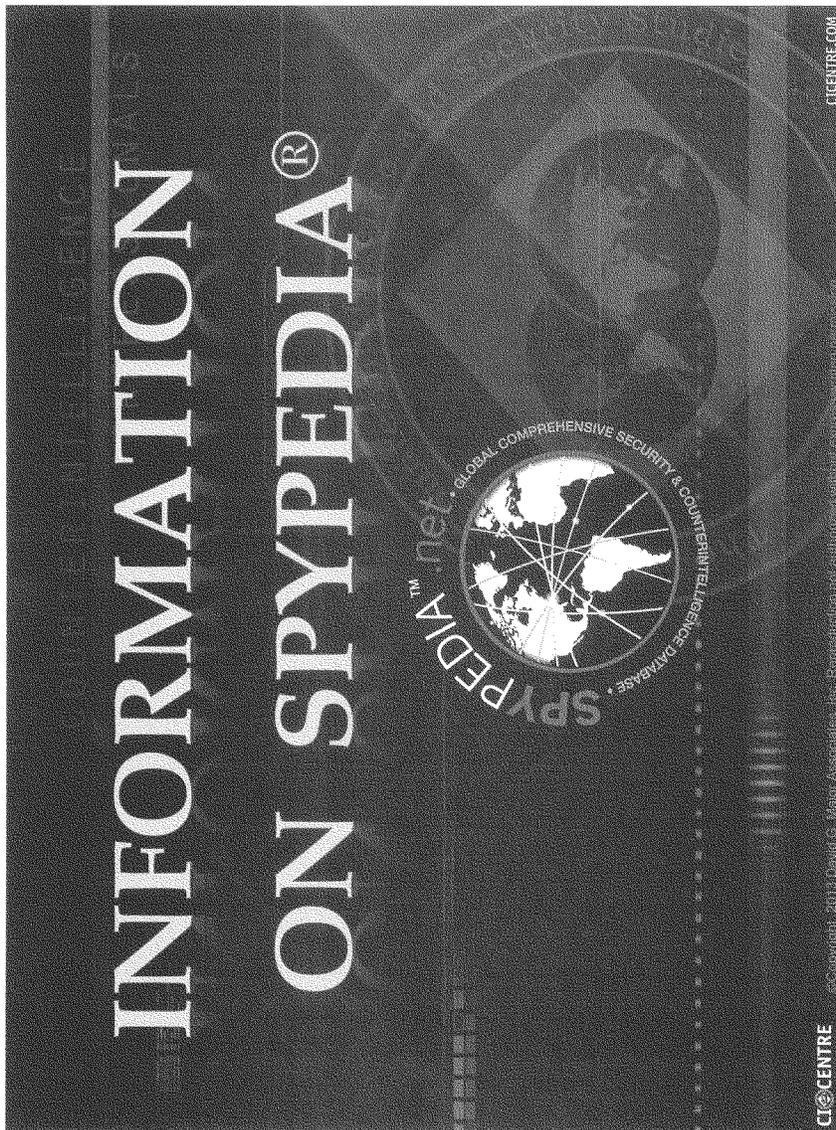


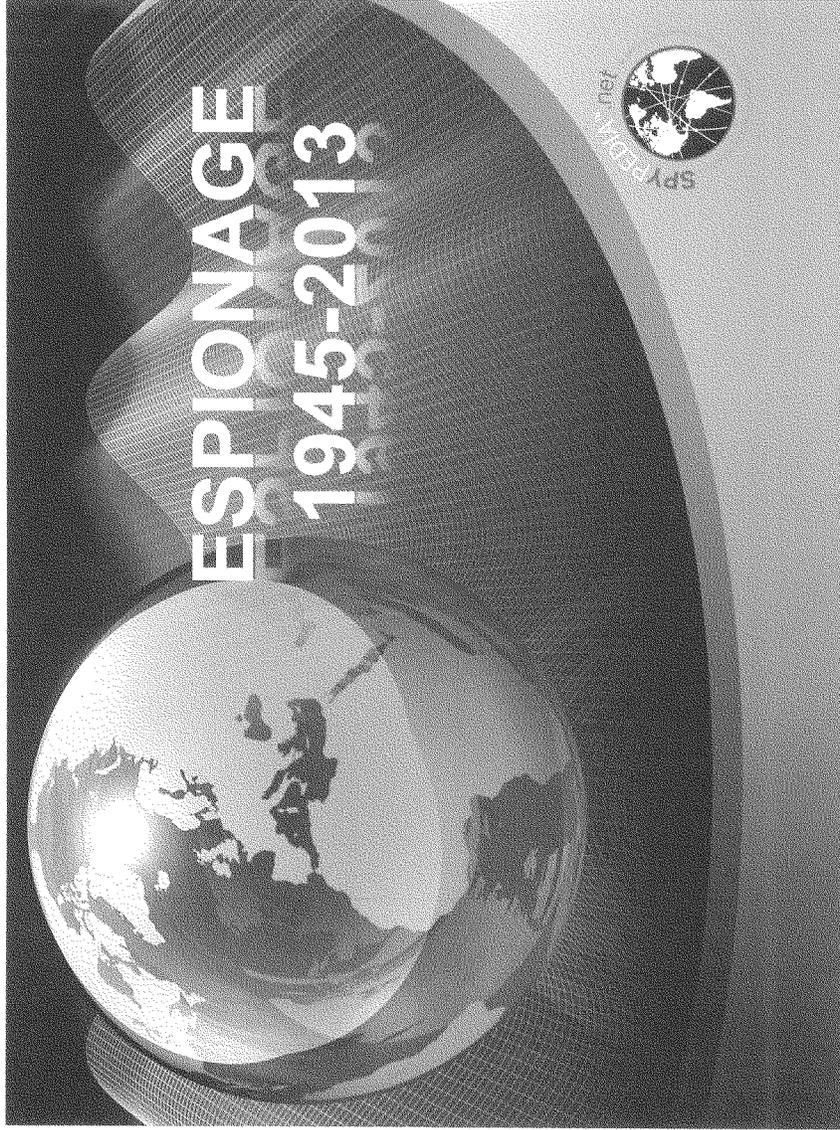


CI CENTRE

©Copyright 2013 Dyer Co. Nigam Associates (Pvt.) International Private Sector

CI CENTRE.COM





1945-2013

- Based on date of arrest
- Includes Foreign Nationals (collectors)
- Includes Betrayers and Co-Conspirators
- Includes “Espionage” related arrests
 - Title 18, 793 and 794
 - FARA
 - Economic Espionage,
- Violation of Title 18 Section 1001
- Individuals who defected pending arrest
- Individuals who committed suicide pending arrest
- Individuals in diverting technology ITAR for foreign government

THE INSIDER THREAT

Insider Threats are seldom this obvious

Insider Threat

Insider Threat

GovCon
The Insider Threat

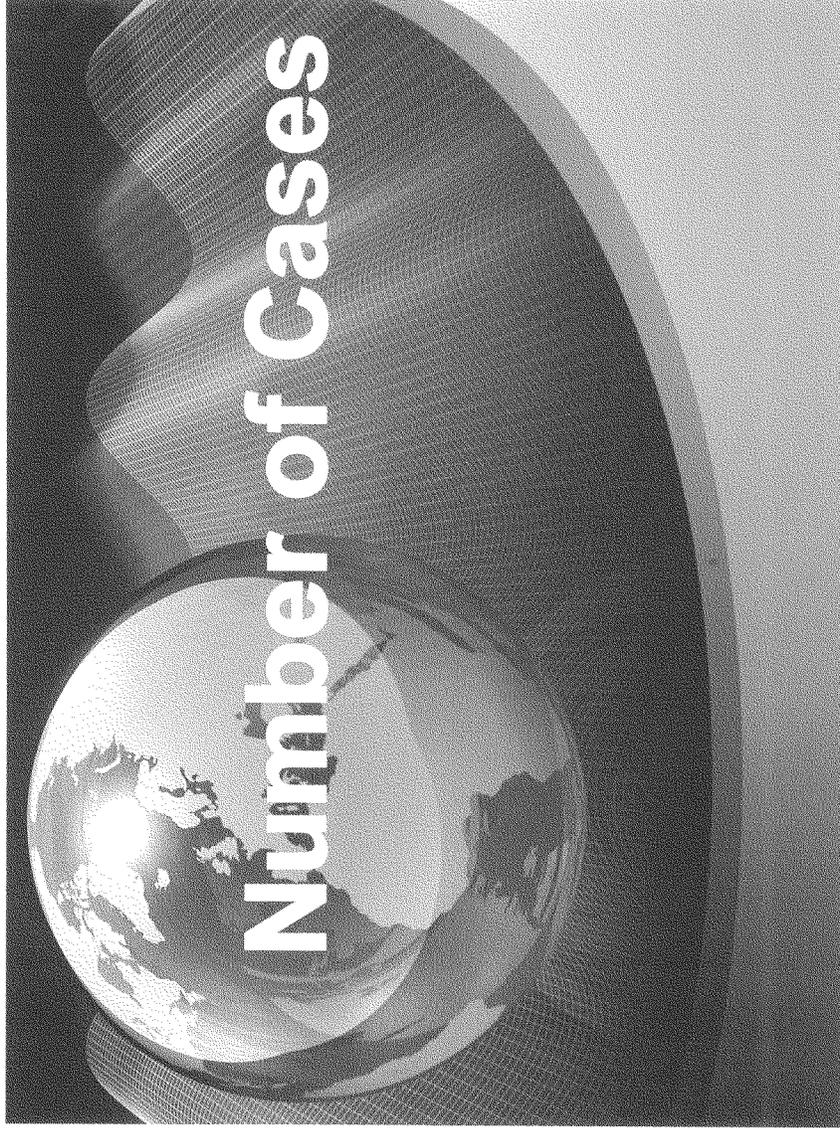
Enemy At the Water Cooler

SECURITY QUIZ
How well do you know the insider threat?
Measure your knowledge of data breaches, stolen secrets and network sabotage.

CI CENTRE

CI CENTRE.COM

© Copyright 1997-2013 by David G. Major Associates, Inc. All rights reserved. Reproduction in any form expressly prohibited without prior written permission.

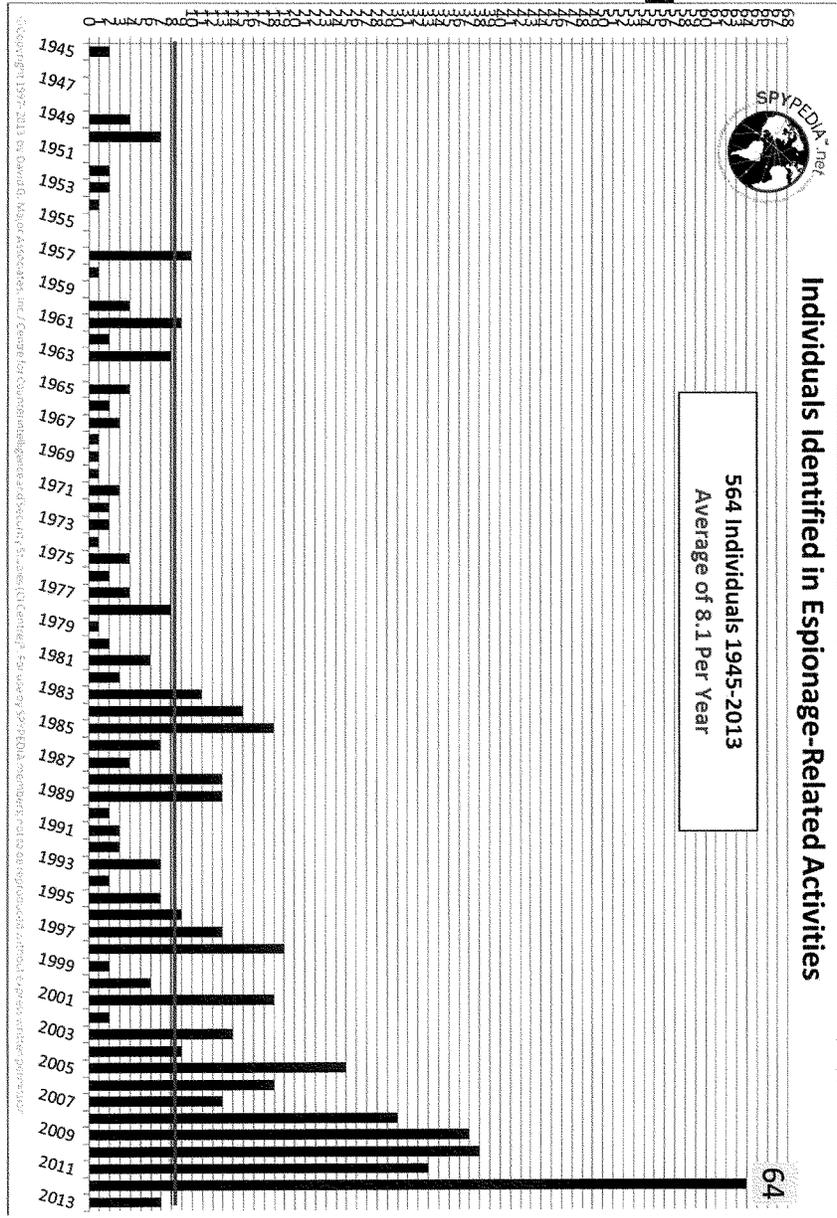


WHAT ABOUT SPIES?

1945-2013

Past 68 Years

CICENTRE.COM



1945-2013

564



1945-2013

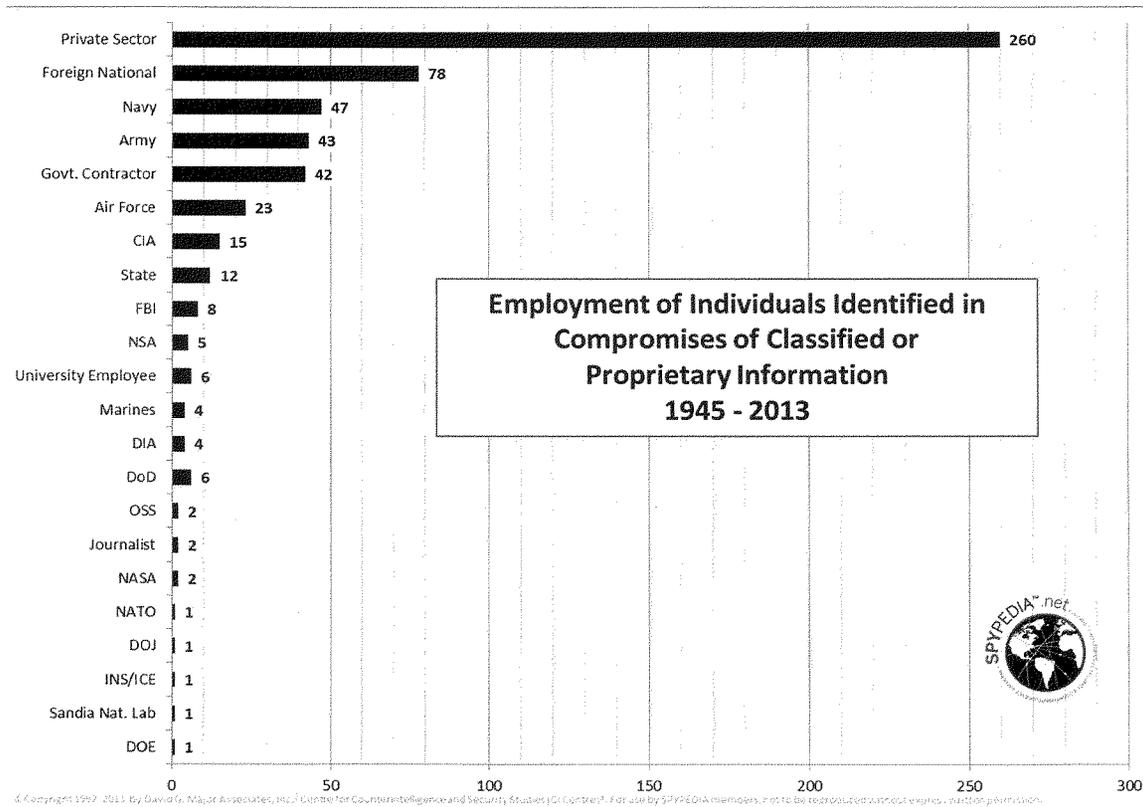
Average of 8.1 per year



CI@CENTRE

Copyright © 2013 by Data & Maps Associates, Inc. All rights reserved. Reproduction in any form is expressly prohibited without prior written permission.

CIESIN.COLUMBIA.EDU

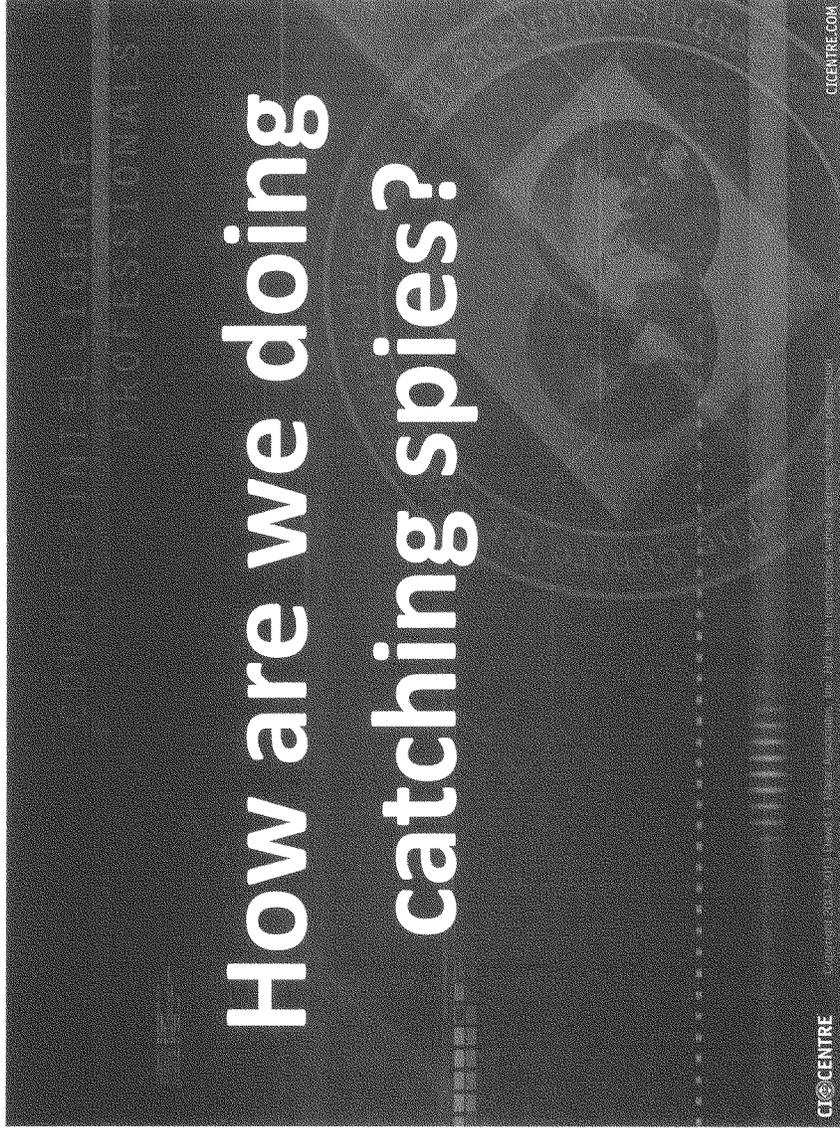


**Employment of Individuals Identified in
Compromises of Classified or
Proprietary Information
1945 - 2013**

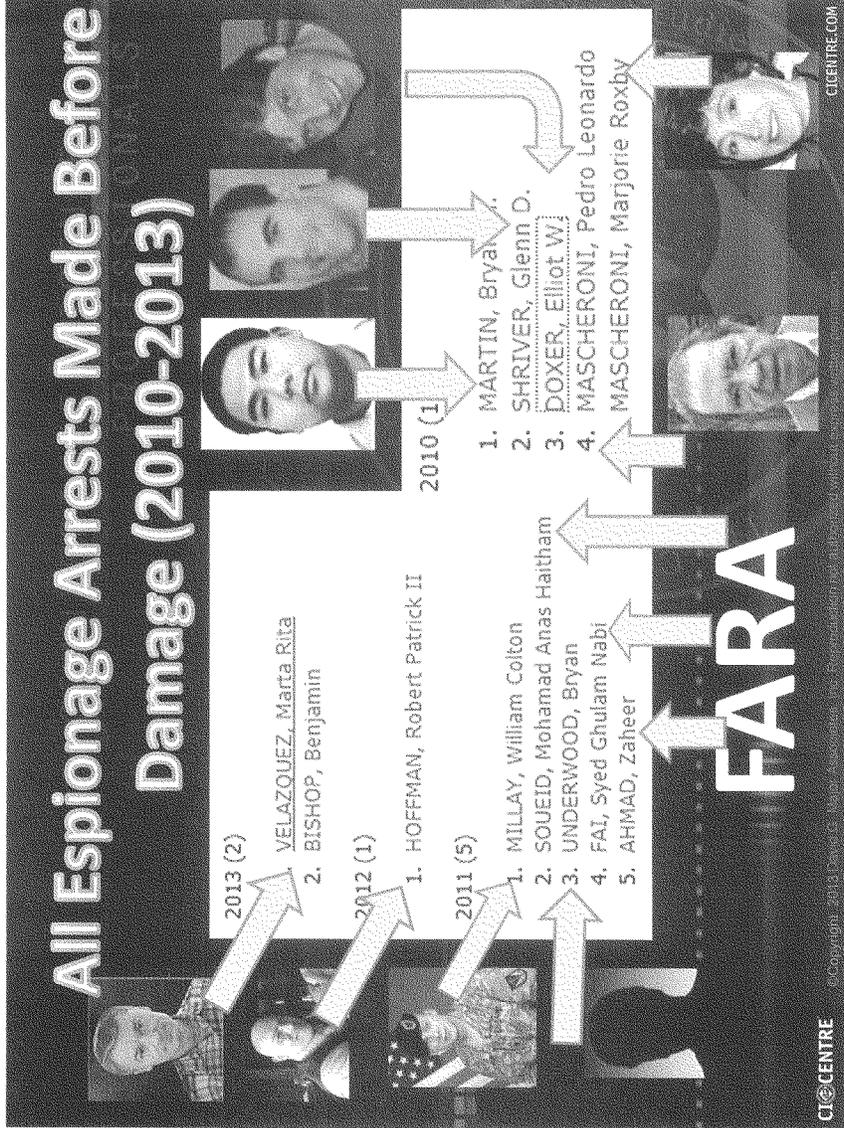


© Copyright 1992-2013 by David G. Major Associates, Inc. (Data for Counterintelligence and Security Studies (CISS) Centre). For use by SPYEDIA members. Not to be reproduced without explicit permission.

© Copyright by David G. Major Associates, Inc., 1992-2013 All rights reserved. Reproduction in any form expressly prohibited without prior written permission.

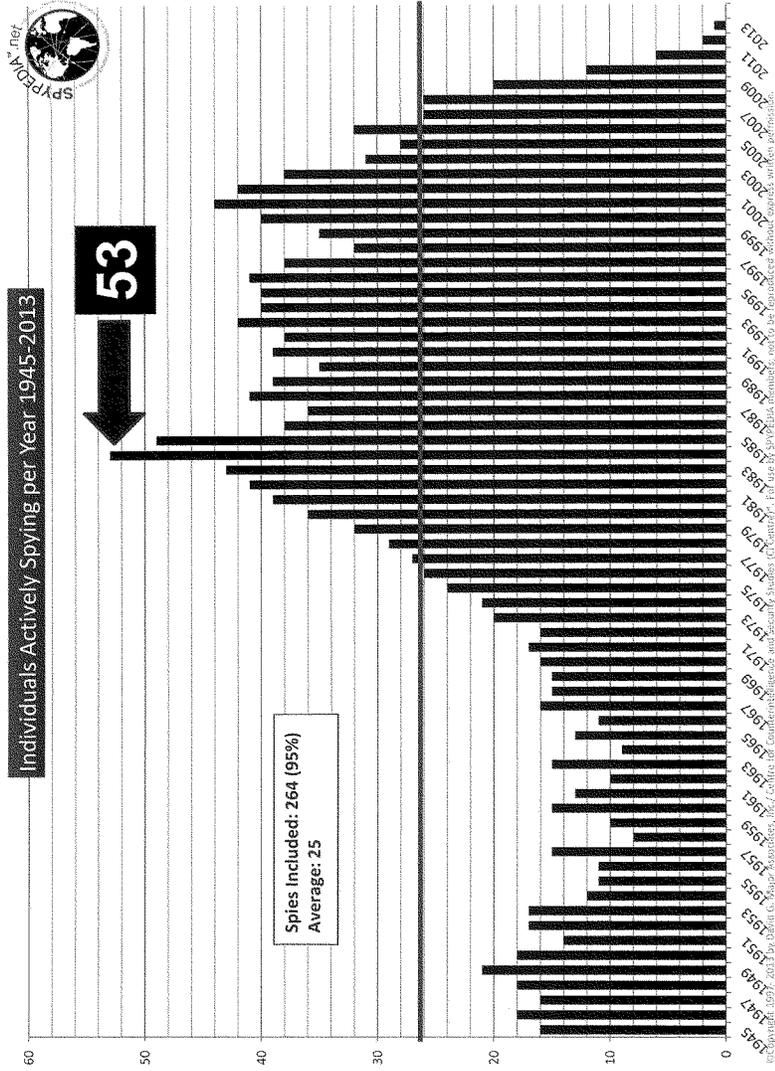


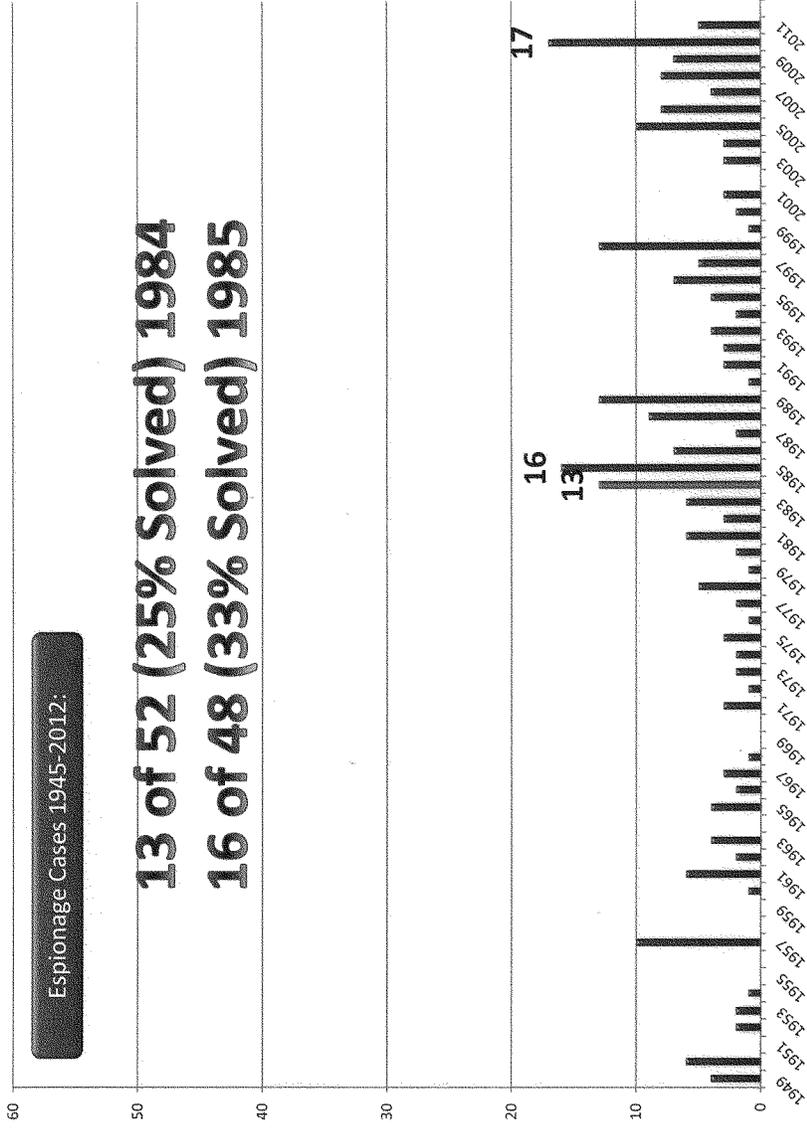
All Espionage Arrests Made Before Damage (2010-2013)



CL@CENTRE

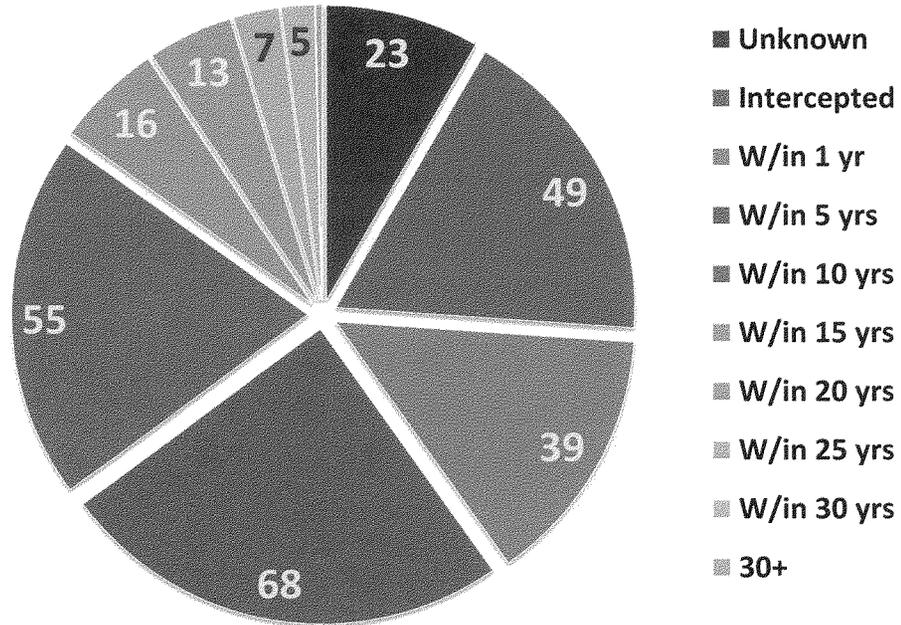
© Copyright 2013

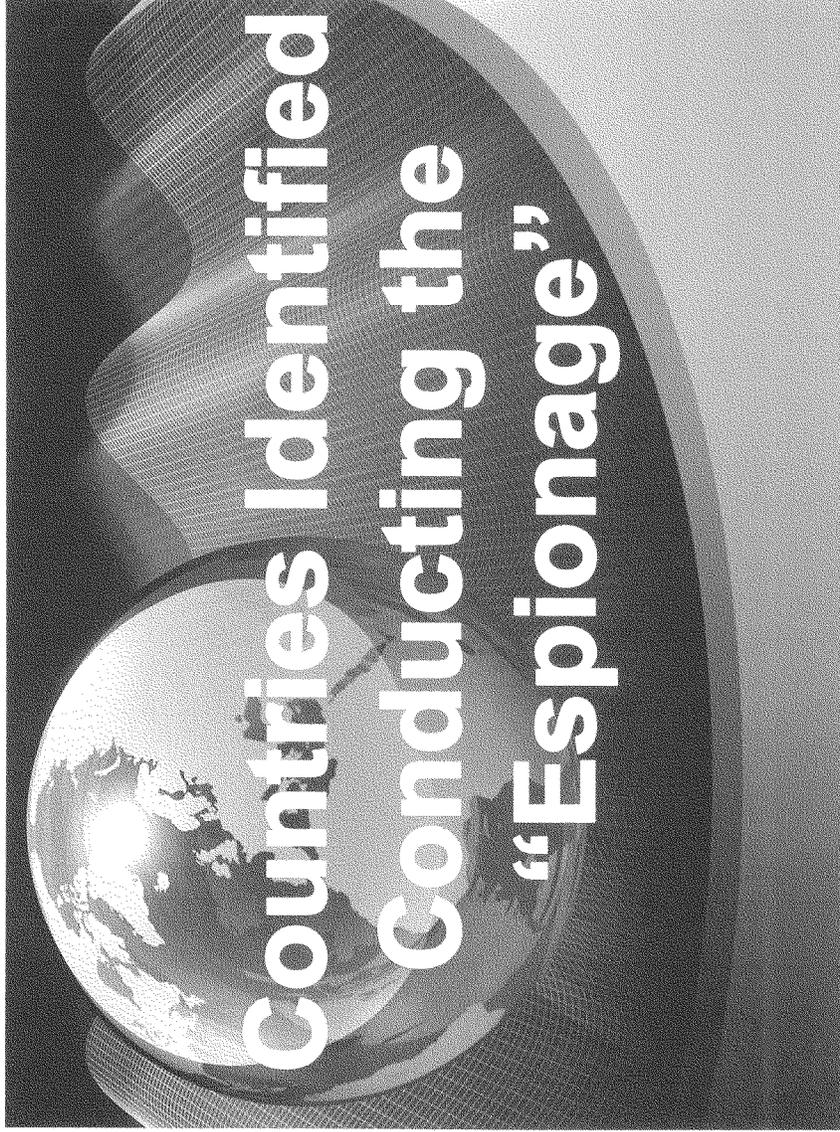


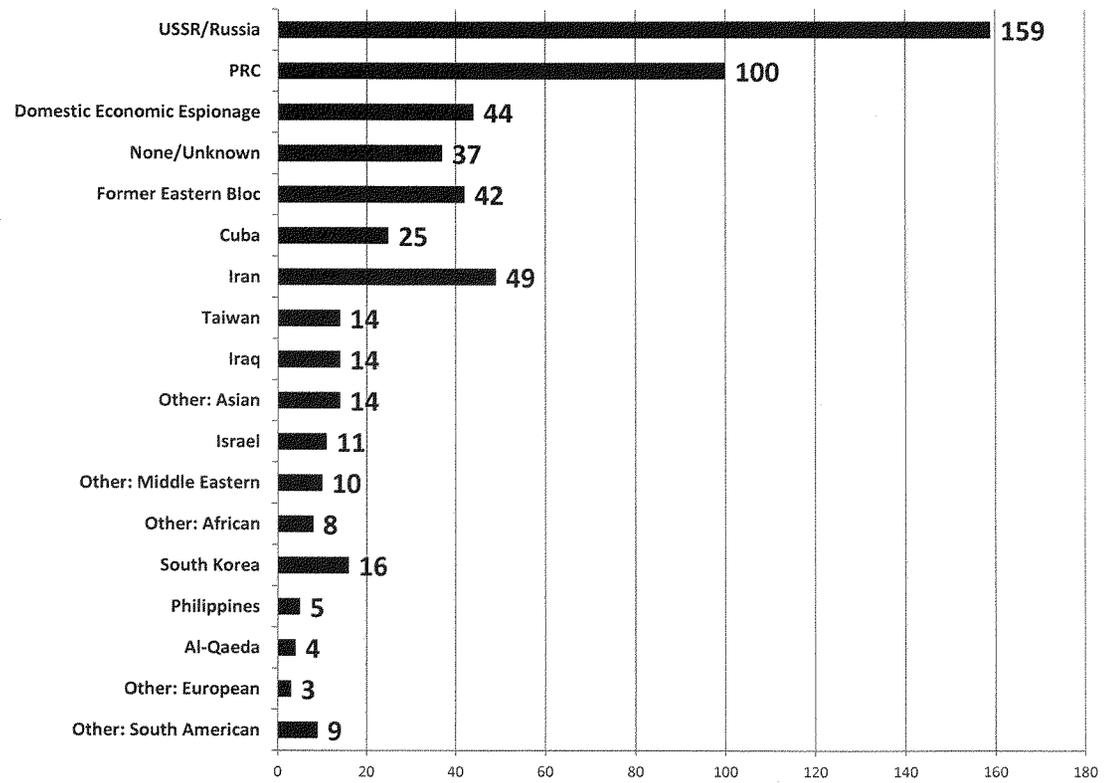


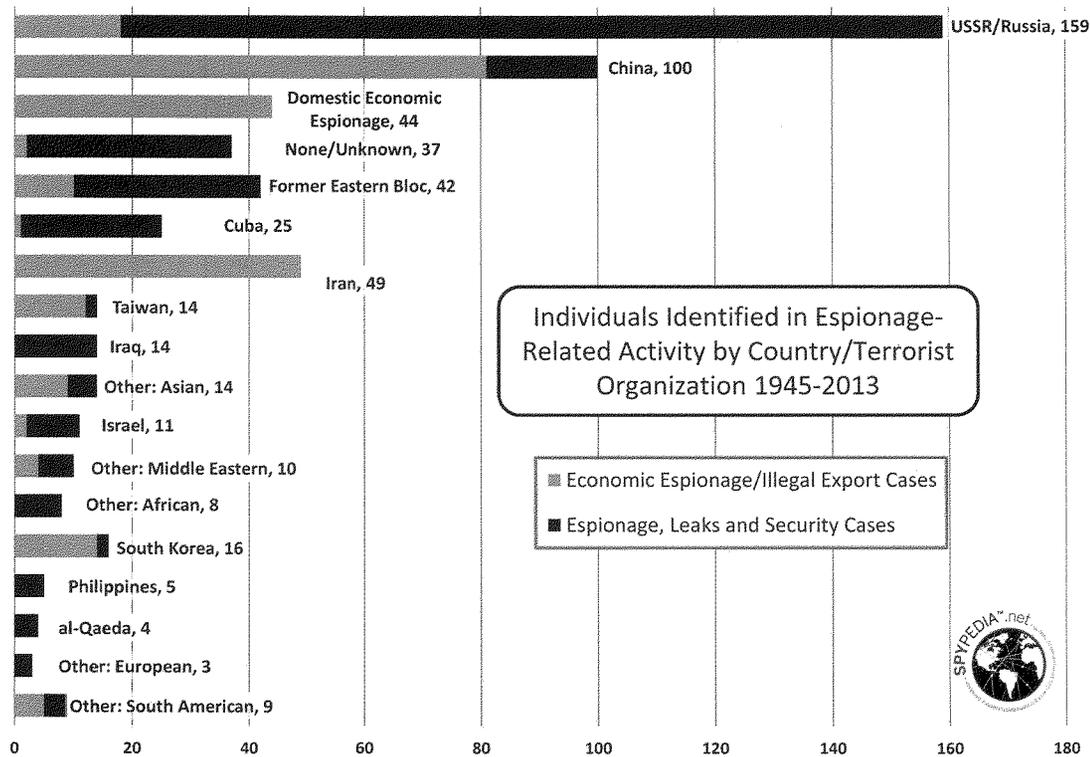
© Copyright by David G. Major Associates, Inc., 1992-2013 All rights reserved. Reproduction in any form expressly prohibited without prior written permission.

Time Before Spy Identified or Stopped: (1)





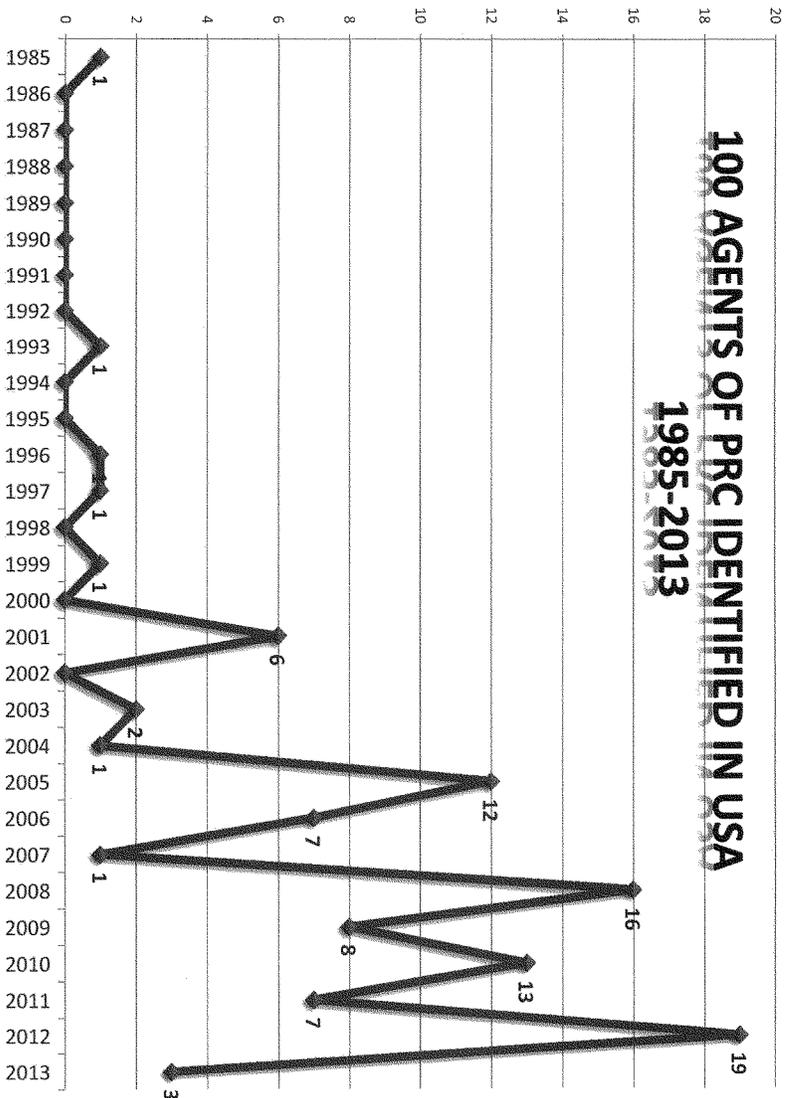


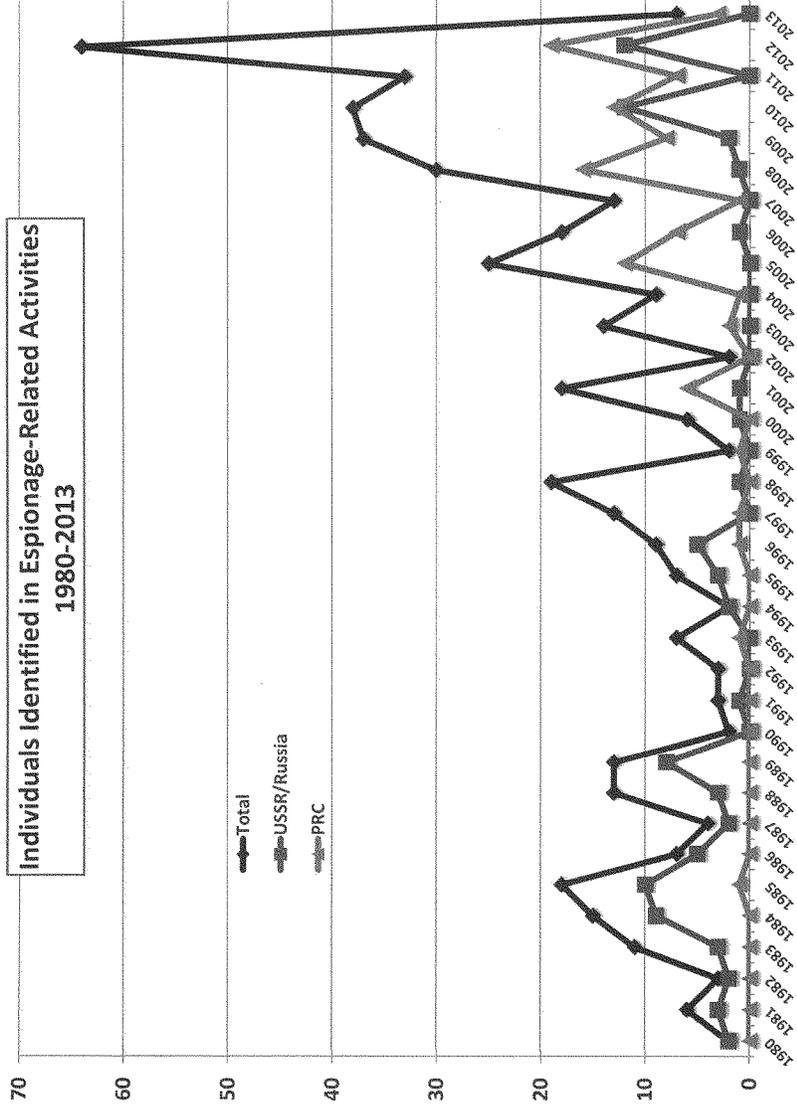


©Copyright 1997-2013 by David G. Major Associates, Inc./ Centre for Counterintelligence and Security Studies (CI Centre)* For use by SPYPEDIA members; not to be reproduced without express written permission.



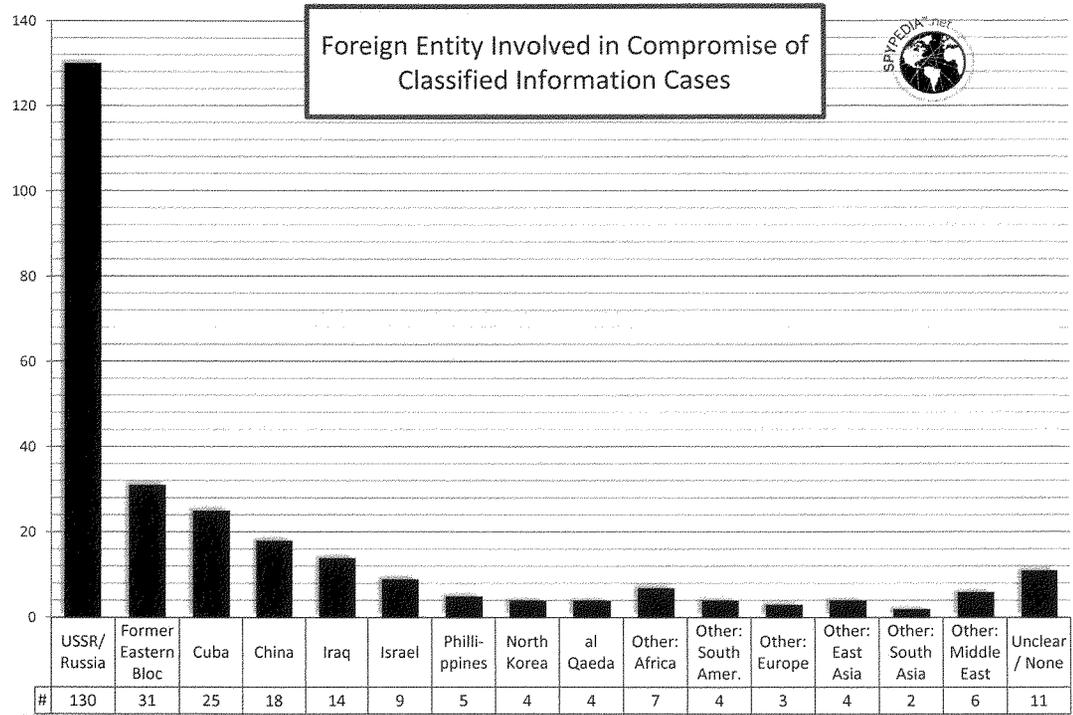
100 AGENTS OF PRC IDENTIFIED IN USA 1985-2013



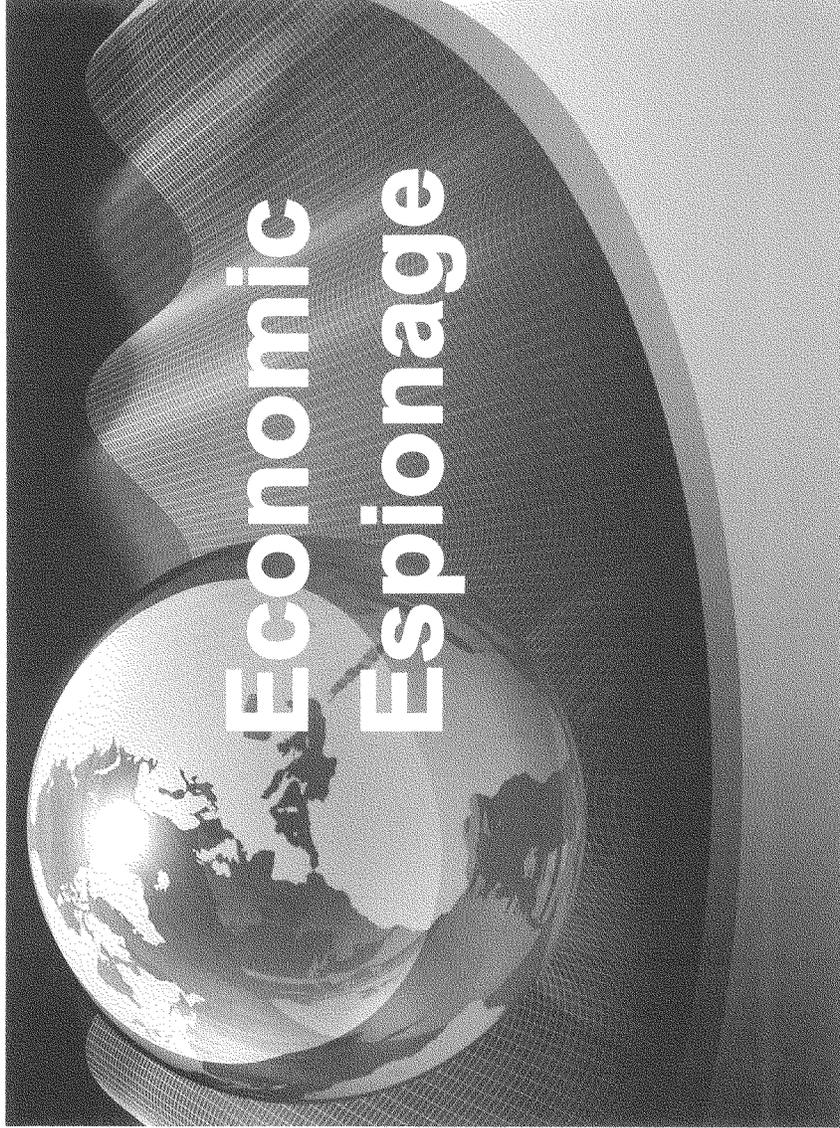


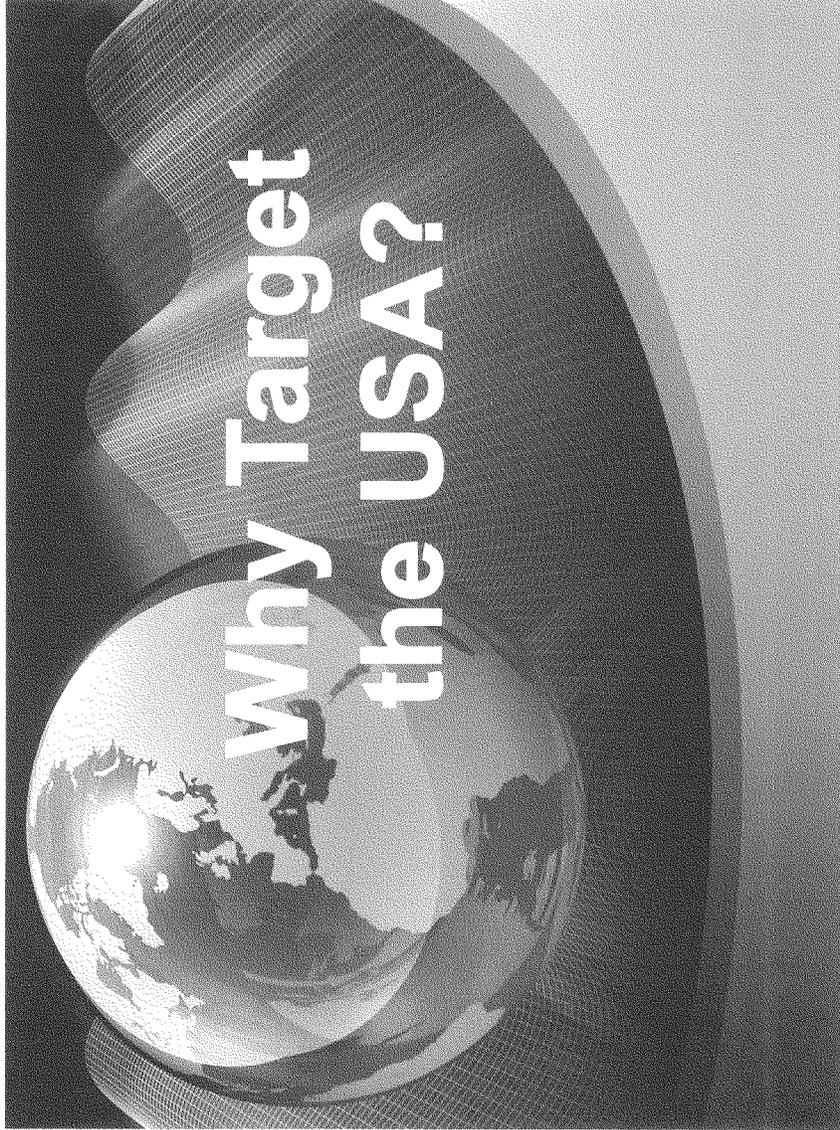
© Copyright by David G. Major Associates, Inc., 1992-2013 All rights reserved. Reproduction in any form expressly prohibited without prior written permission.

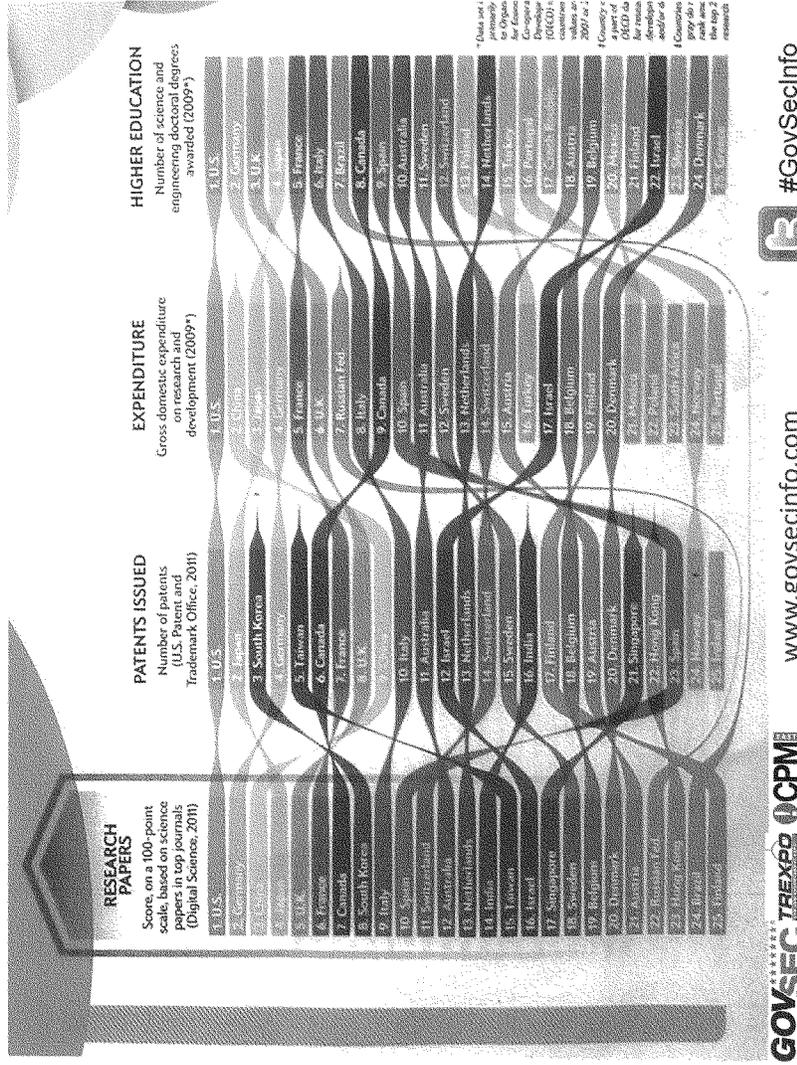




© Copyright 1997-2013 by David G. Major Associates, Inc./ Centre for Counterintelligence and Security Studies (C1 Centre). For use by SPIYPEDIA members; not to be reproduced without express written permission.





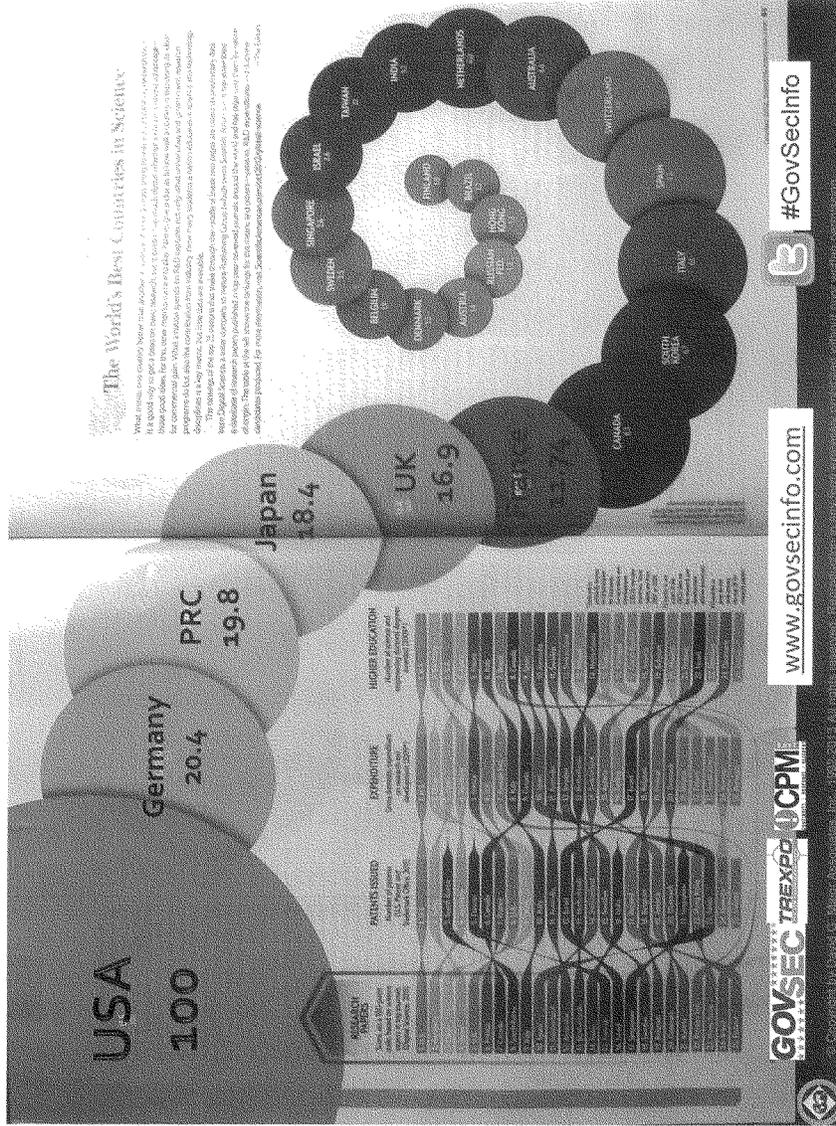


#GovSecInfo

www.govsecinfo.com

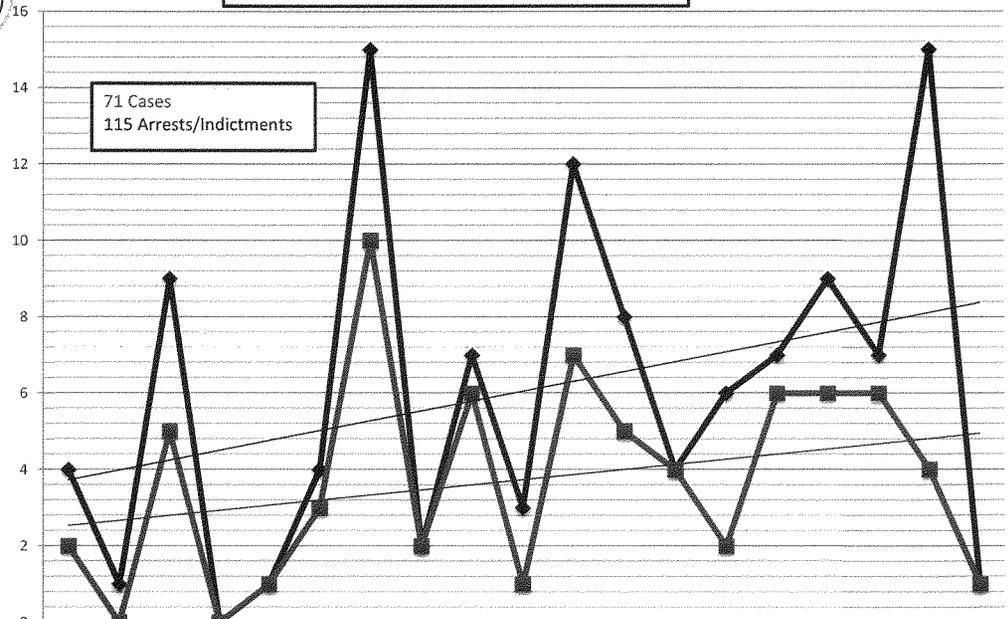


© Copyright by David G. Major Associates, Inc., 1992-2013. All rights reserved. Reproduction in any form expressly prohibited without prior written permission.





**Cases of Economic Theft and Individuals Indicted
1995 - 2013**

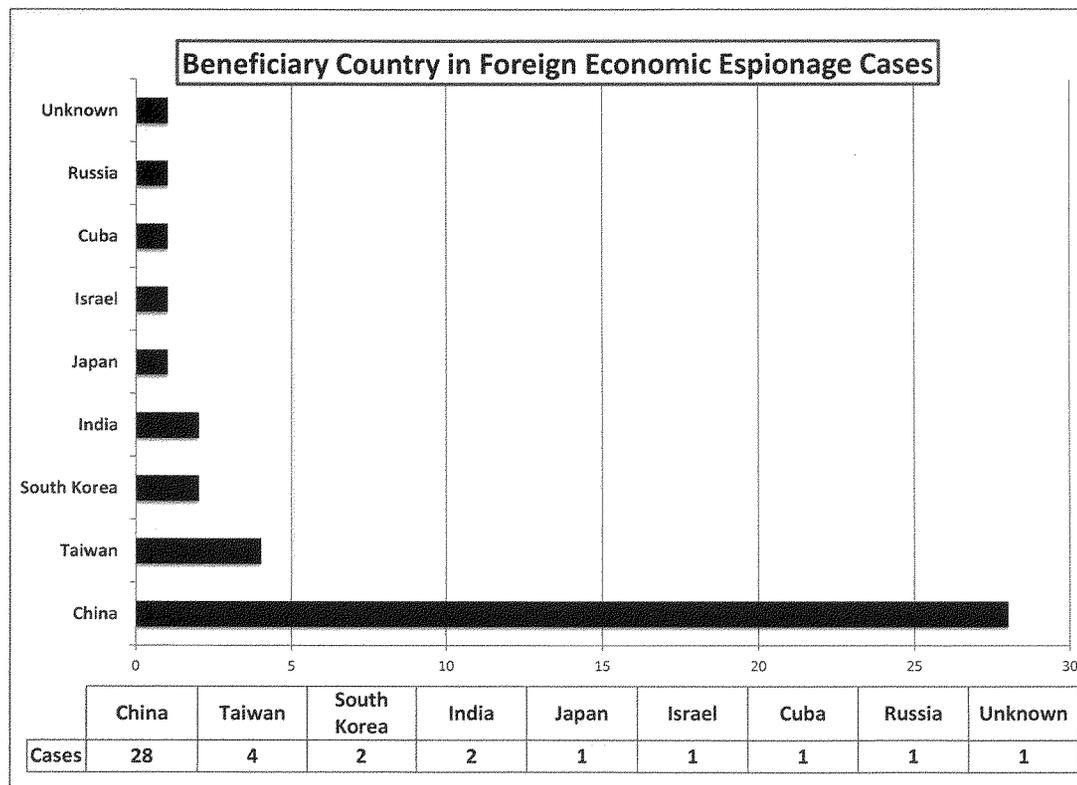


	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Individuals	4	1	9	0	1	4	15	2	7	3	12	8	4	6	7	9	7	15	1
Cases	2	0	5	0	1	3	10	2	6	1	7	5	4	2	6	6	6	4	1

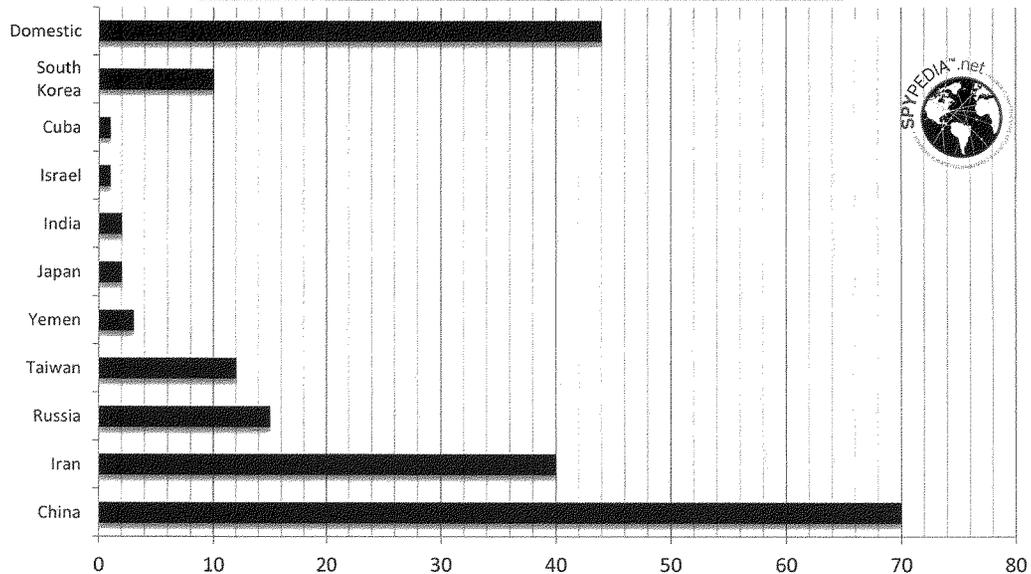
© Copyright by D&MA, Inc. 1992-2013 All rights reserved. reproduction in any form is expressly prohibited without prior written permission. Active SPYEDIA members are authorized to use this material as long as the copyright statement remains attached.



© Copyright by David G. Major Associates, Inc., 1992-2013 All rights reserved. Reproduction in any form expressly prohibited without prior written permission.



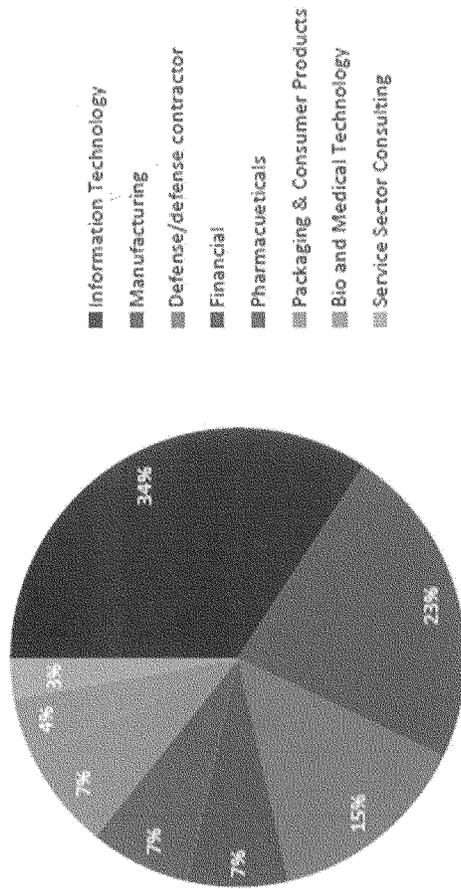
Foreign and Domestic Economic Espionage Agents 1995-2012



	China	Iran	Russia	Taiwan	Yemen	Japan	India	Israel	Cuba	South Korea	Domestic
Individuals	70	40	15	12	3	2	2	1	1	10	44

What is Targeted?

Industry Targeted by Case



What is Targeted?

- Information Technology High Tech (*software source codes, technical research and development*): 26 (38%)
- Industrial (*chemical formulas and manufacturing processes*): 19 (28%)
- Military (*weapons systems designs*): 10 (14%)
- Business (*customer/marketing files and business negotiations*): 9 (13%)
- Biological (*organic samples, medications and research*): 5 (7%)



www.govsecinfo.com

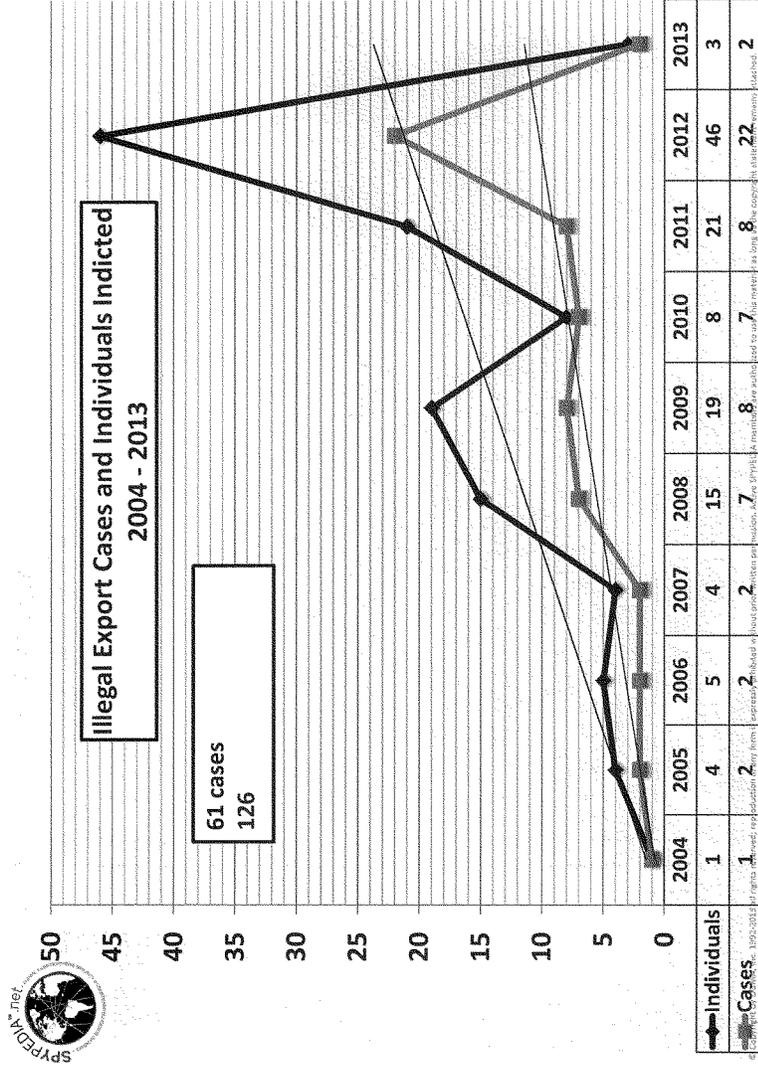


#GovSecInfo

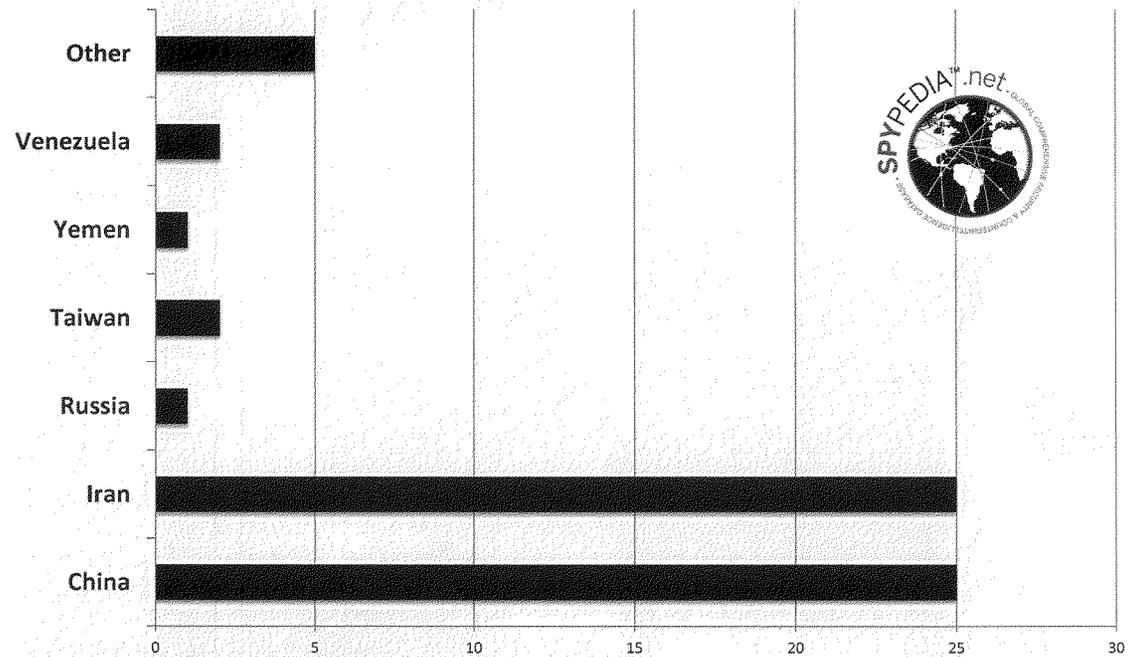
CI@CENTRE

CICENTRE.COM

Copyright © 2015, Center for Strategic Studies, Inc. (CIS) All rights reserved. Reproduction in any form, express or implied, without prior written permission.



Beneficiary Country in Illegal Export Cases



Country	China	Iran	Russia	Taiwan	Yemen	Venezuela	Other
	25	25	1	2	1	2	5

GOVSEC TRENDS OCPM

www.govsecinfo.com

#GovSecInfo

© Copyright by David G. Major Associates, Inc., 1992-2013 All rights reserved. Reproduction in any form expressly prohibited without prior written permission.

Chairman BROUN. You could go on with that longer. You didn't have to talk that fast. That was a lot of information. I appreciate it, Mr. Major. It is excellent. I thank you all for your testimony.

Now, reminding Members that the Committee rules limit questions to five minutes. The Chair at this point will open the first round of questions, and I recognize myself for five minutes.

Now, Dr. Vest, in your testimony you used the analogy of a leaky bucket and suggested that it would be better to keep filling the bucket rather than to obsess over plugging the holes, but reports from the U.S. intelligence community, the Pentagon, and testimony that we have heard today seem to suggest that at least one of those holes are pretty big and continues to grow. If we don't do something about China, we may not have much water left in our bucket. Would it be possible and acceptable within the academic and scientific communities to implement a targeted approach to address the growing threat from Chinese espionage while still generally adhering to the principle of keeping basic, fundamental research open and unrestricted?

Dr. VEST. It is obviously a complicated question, and I go back to something that Ms. Van Cleave said, which is they are interested in virtually everything. And I do not think that we can keep virtually everything secret from the Chinese or anyone else, so I would still contend that we should focus on two things: one is really protecting those things that the national security community believes to be the most important—weapons systems, et cetera—and secondly, I very much agree with what has been said by you, Mr. Chairman, and others that we really have to do something about making ourselves more secure against cyber intrusion. Stealing is different than openness of the academic community.

Precisely where that line is I don't know, but given the speed with which science and new technology move forward these days, we simply cannot keep absolutely everything closed and secret, nor do we want to. So I still contend that the leaky bucket approach is correct today even though the numbers are getting larger and the areas of interest are getting larger. We have to focus on the things that are critical and help our laboratories and our universities to remain as open as possible so that we transmit our values, learn from each other.

Every company I know anything about now does research, serves markets virtually everywhere in the world. I gave in my testimony an example of the new Boeing aircraft that is built in 535 different places. We can't just keep everything on our shores totally closed up. And I think it is up to the universities, by the way, to do some of their own drawings of lines and simply not do research that they believe needs to be classified or thought of in some different way.

Chairman BROUN. Well, Dr. Vest, I hope that the bucket still has a bottom to it and it is not just a sieve, but I agree with you.

Communication between the science and security communities to deal with the questions raised by this hearing is critical. What are the examples of effective methods for conducting such a dialogue, Dr. Vest?

Dr. VEST. Well, I think that after 9/11, there was actually some very productive dialogue back-and-forth between the universities, the National Academies, the security establishment, and some of

those things went pretty well, things such as defining the so-called select agents, the biological materials that everybody agreed needed to be restricted in their use on campuses and under secure facilities and so forth. But on the other hand, during that period we also saw things like technology alert lists that didn't want to let people in the country who had studied fields like landscape architecture. So we got a little bit over the map.

I think the dialogue is the important thing because in my relatively modest forays into engagement with the intelligence community, these—as we know from the table—are very intelligent, very thoughtful, very patriotic people, and so are most of us in universities and independent research laboratories. So to me, ongoing dialogue is the key to trying to find somewhere where that fuzzy line that Dr. Wortzel referred to is. And then I think universities need to adhere to it.

Chairman BROUN. Well, my time is expired, but if any of you all have any suggestions about creating more dialogue between the communities, I would appreciate it.

Now, I will recognize Mr. Maffei for five minutes.

Mr. MAFFEI. Mr. Chairman, thank you. I want to thank again this panel for your testimony. I haven't been on this Committee very, very long yet, but we have—already had a lot of distinguished witnesses. But I think this is probably the most distinguished panel that we have had.

Nonetheless, only one of you, Mr. Major, actually has a degree from Syracuse University, so I am going to start with you, Mr. Major.

Chairman BROUN. But we have a Marine.

Mr. MAFFEI. Well, that is good. That is—they are—that is very important. But what advice would you give scientists, people working at these labs in order to ward off these practices? And I don't know—we don't have a lot of time here but is there a best practices that could be followed? Does your company ever do that kind of training? And if they are not being followed, why not or how can we get a better—are there simple things that maybe can be done to at least ward off some of these intrusions, these espionage efforts?

Mr. MAJOR. Well, thank you for your question. First of all, it is Syracuse University in biochemistry and I—go Orangemen. And I was in the United States Army, I should tell you also, but I am not a Marine.

We—

Chairman BROUN. Thank you for your service.

Mr. MAJOR. Thank you, sir.

You know, this idea of education of espionage is not a new problem but some of the hardest targets are trying to—targets to educate are academics and people in laboratories. Department of Energy has been struggling with this problem for many, many years, as is anybody who ever deals with the universities. When I was a supervisor in Baltimore, I had trouble with the universities up there to explain to them the reality of what was happening with some of their students that were coming there, because we know that students represent a particular problem when they come in there.

We actually had a dean go in and tell the Chinese students—he said the FBI may come in here to talk to you. If they do, come to me because you have no obligation in this country to talk to the FBI. Well, I went in and had a discussion with him and I said it is my responsibility to worry about this regardless of what you say, Mr.—as the dean there. So this is always a long, long problem. It is an education problem and you have to do it in a creative way. You have to be very realistic. You have to be pithy. You have to let them know the facts. You can't just go in and say there is a problem.

And I will tell you this in follow-up to the last discussion is that we can sometimes make a mistake and we said the problem is primarily in classified national security information, but our empirical evidence shows us that across the board the United States is being targeted, and some corporations are having them on themselves to create meaningful protection programs because it can be worth an awful lot of money. I mean DuPont had a major case where they were trying to steal titanium oxide, which is worth billions of dollars, this white paint. But that is worth a lot of money, and yet we have espionage cases trying to steal those kinds of information.

So you have to really educate people on it. You have to be realistic, but you have to invest in it. And this is a problem. It is a problem in a government and it is a problem in corporations. Corporations—there is a movement in some corporation to create their own internal counterintelligence cells to do a better job of educating them on this, probably the single-best thing you can do. And then there is a lot of other things you have to do that have to do with cyber security and the failures—mistakes people make.

When we go through and talk in our courses and we do that as one of the products that this company does is that we try to explain what has happened in the past and where it broke down and where it failed and what you can do, and the people are very shocked when they realize that despite the policies that were set up, the human errors that allowed someone to come in there and still operate.

There was a man—there was a Chinese student who was stealing just recently information on cancer research and they fired him. He went home and they never took him off the server and he went back in the server and got information. Well, he should have been taken off the server immediately after that took place.

So you see these kind of human failures that can—that break in on a repeated basis when you are trying to create an environment that is both open but realizing there are a lot of collectors out there. And as I said, this is a bigger problem from corporate America today than it has historically, partly because the House passed the law on economic espionage. And that was an issue that we couldn't—we didn't have a way to deal with when that law was passed in '96. We are dealing with it and that is the growth area in espionage in the United States.

Mr. MAFFEI. Good. And I do note that in your written testimony you mention that 555 individuals that have engaged in espionage-related activities since 1945, all but—all of those cases, there was only one case involving the Department of Energy, one involving

NASA, six cases involving university employees, but 252 cases involving the private sector, so I think that is interesting.

I do—I know that Ms. Van Cleave mentioned sort of the cost of this. Do you have any estimates of it? You said that \$12 billion was probably too low. Do you have any reliable estimates of how much this is costing us every year?

Ms. VAN CLEAVE. It really is not possible to calculate how much this in fact is costing us because it depends on the assumptions that you build into that. The Bureau's estimate of \$13 billion in 2012 was based on the cases that they had an economic espionage and what was involved in those particular losses and their estimates of what they may have missed. But my concern is—and I think there is with you, too—that there is a great deal of under-reporting in that area and that the real cost to the economy is something far beyond that because what you are talking about is loss of the basic idea factory. R&D is the idea factory and so what happens with the ideas that are lost competitively to others?

Mr. MAFFEI. All right. Thank you. Well, Mr. Chairman, my time is up but the only thing I might observe is that so much of this is economic in that we do have a trade deficit problem with the People's Republic of China in addition to some of the other countries out there, but this actually could be one of the major factors since they are not paying for it. They are stealing it or their companies are stealing it or particular individuals are stealing it. And that could be one of the major factors why we are not selling more to China. It may not just be a security issue.

Chairman BROUN. Well, the gentleman's time is expired. And I think that is a good point and that is part of the reason for this hearing.

Now, the Chairman recognizes Mr. Posey.

Mr. POSEY. Thank you very much, Mr. Chairman. And thank all four of you for your excellent presentations, very interesting. You know, if Americans focused more on the many, many threats to their futures, we would be, I think, a much more united country. You know, unfortunately, we are only united like we should be for a short period of time following 9/11, a short period of time following Boston, and completely another subject. But anyway, sometimes the best defense is an offense, and so, you know, any of you feel free to answer whether or not we have an offensive program toward those who are threats to us.

Ms. VAN CLEAVE. Sir, if I might take that one, I think that is a superb question. Really, the efforts that we have made to try to protect our technology and science base have been largely defensive in nature, which is to say we promulgate security regulations. We have export controls over the things that we permit to go out. We have classification protection around sensitive information. But what we don't have, as much as we need to have, is an offensive capability that can go inside the foreign intelligence service that is targeting us in order to be able to actively defeat their activities against us.

One of the reasons we don't have that harkens back to my opening explanation today, which is we have never had really a unified counterintelligence strategic capability in the United States. We have done things defensively to protect certain operations abroad

against foreign intelligence attacks. We have enforced espionage laws here at home, but offensively, to get inside that foreign intelligence service to understand how they operate, how they are tasked, what their liaison relationships are, the things that may make them vulnerable to us, that is what we really need. So I think it is a great question.

Mr. POSEY. Well, I am really sad about the answer. I mean I thank you for the frank answer but I am sad about it. I mean I was hoping you would say, yeah, we have all kinds of those programs but we can't talk about them. I am sad to learn that we don't. I mean there is one reason this country hasn't been overtly attacked and that is because people who might attack us realize the cost of retaliation and it is unbearable to them. That doesn't seem to be the case in cyber warfare.

Ms. VAN CLEAVE. When it comes to cyber warfare, that is an interesting and challenging calculation in and of itself, and I think that there are lots of conversations, studies underway to try to better understand what we can do consistent with, you know, our values and the laws of war in offensive cyber operations, so that is a great question in and of itself.

But beyond that, there are all of the other operations of foreign intelligence services against us where again having capability to get inside those services and to degrade what they are doing would be of great benefit to us.

Mr. POSEY. And doesn't it seem like it makes an awful lot of good sense to you to unilaterally disarm when you make agreements with these countries that are robbing you blind in the left pocket and you are going to voluntarily disarm any defense you have in the right pocket? I mean is there something wrong with that theory that—or something right about that theory that we don't see?

Ms. VAN CLEAVE. I am not sure what you mean by unilaterally disarm but I know I don't like it.

Mr. POSEY. Yeah, well, you know, supposedly friendly countries, you know, don't hack you, don't rob you. You know, they don't go into your Pentagon, they don't go into your banks, they don't—you know, they don't cause the havoc that they have caused.

Mr. Major, you are waving your pencil there.

Mr. MAJOR. Yeah, I did. The Bureau in the last few years has a very aggressive program to try to educate the private sector in economic espionage. They have reached out significantly to try to—they have even made bulletin boards to tell people about this particular problem. So taking an offensive standpoint they have.

On the other side, the FBI can speak from them is—has always had an aggressive program to target foreign intelligence services that operate in the United States to penetrate them to try to find out what they are doing. And one of the things you see reflected in the numbers I showed you, you don't just find an espionage case. Almost always when you find an espionage case that I showed you, it is because you have penetrated that service in some manner either from a technical standpoint or a human standpoint. They have told you about the fact that you have been under attack.

The first target of the Chinese was made by the CIA in 1982. It was the first western service to ever penetrate the MSS. We didn't understand what China did for many, many years. One of the re-

flections we have seen with the 100 cases is two things: you are seeing a more aggressive service, a better understanding of how they are operating, and I would suggest also a better penetration of some of these services that you can't talk about in this environment because the counterpart of no more espionage cases is more understanding of espionage cases usually through operations being done by the intelligence community. And I know at least in my experience I spent most of my career running offensive operations against intelligence services that operated here.

Mr. POSEY. Mr. Chairman, I would like sometime maybe we could have a closed hearing and have some of the discussions about things we can't have in an open public hearing like this.

Chairman BROUN. Mr. Posey, that may be a very good idea and we will see about looking into that.

One quick question, Mr. Major, are you suggesting more human and counterintelligence, more boots on the ground?

Mr. MAJOR. Oh, yes. I mean the more you do this, the more aggressive you operate this, it is successful. One downside is happening right now, however, is that a lot of education programs are being cancelled because when you have a sequestration problem, the first thing you cancel are training and travel and that is what is happening across the board right now.

Chairman BROUN. Thank you, Mr. Major.

Mr. Swalwell, you are recognized for five minutes.

Mr. SWALWELL. Thank you, Mr. Chair. And thank you, Ranking Member Maffei, for holding this hearing.

And Mr. Major, I think you make a great point. We are talking about important threats that are facing our country right now and the need to protect and defend against them, especially against outside actors and nation states who are very aggressive in going after our intellectual property, going after our government networks. But on the other hand, we have the sequester and that, I can imagine, you would agree makes it difficult. I mean it is nice to hold a hearing and say, you know, these are the threats. We need to, you know, be more secure, but there is no money to pay for doing that. It is just, you know, we need to do that. And would you agree?

Mr. MAJOR. One of the first things that is always cut is that. I have been around long enough to see this happening over and over again. It is a trend and it is happening right now.

Mr. SWALWELL. Also, I think we can agree that international collaboration has served our country well, and I for one want to emphasize the role that scientists of Asian and Middle Eastern descent have played at our National Laboratories. I have two National Laboratories in my Congressional District—Lawrence Livermore labs—Laboratory and Sandia Laboratory. And also we know the role that immigrants have played in our country. Forty percent of the largest companies in our country were founded by immigrants or the children of immigrants. So I think it is important that we balance the need to protect against espionage against the role and understanding that immigrants come here and they create jobs, they participate and engage in the type of innovation we need.

And so that leads me to my question, which is in Livermore we have what is called the Livermore Valley Open Campus. This is a

collaboration between Lawrence Livermore National Laboratory and Sandia National Laboratory working to create an open, unclassified research and development space. And the challenge right now, of course, is you have laboratory workers who—inside the laboratory they have to be cleared to work there. It is a largely inaccessible place for the public, and because of shrinking budgets, the laboratories are having a hard time continuing to meet the needs and demands of their clients, principally, the NNSA for Lawrence Livermore. And so they are looking at using outside contractors very often. But getting those outside contractors screened and cleared is often a challenge.

But we know the role that private industry can make, and I have never been one to believe that the government should be the only one at the table when it comes to innovation. I think we have to partner with private industry.

So is there a way that we can continue to see these open campuses thrive and work in an unclassified manner on perhaps high-performance computing and cyber security research and development while still keeping us safe from espionage, Mr. Major?

Mr. MAJOR. First of all, let me say that of the 565 people that we know have been indicted and arrested, the vast majority have been Americans; they are not immigrants. But we are all immigrants in one way or another, but that is the vast majority committing espionage.

However, we have both sides of the gamble taking place. What you do have in your environment is you have a mix and match. You have one person who is working in a totally open environment that—when you are working a material, you don't care where it goes and who has access to it. That is one thing. But if what that same person is working on a sensitive program or a classified program and they start interfacing, it is very easy to lose the connectivity; who am I speaking to right now? And that is really an education problem and it is also an organization problem. Do I want to have people that are working in these sensitive programs also interfacing with these people in these totally open programs? Because very quickly, that line will blur between the—that individual and who is my friend and who do I talk to and what can I say? So that is an organizational issue. Yeah, sure, they can exist separately but it has to be done I think in a calculated way.

Mr. SWALWELL. So you believe if the open campuses are able to have that bright line that distinguishes between the classified work and the unclassified work and knowing that in the unclassified areas we can still make great strides and progress in energy security and national security without giving the individuals working in those areas anything that would be sensitive or compartmentalized, do you think that is possible?

Mr. MAJOR. You look at it and you say I am going to—if you color it gone and said soon after we do it, it going to go someplace else, then it—you don't have a problem. But then the people that are working on it, they also have information that you don't want to have color gone. And you got to figure out is that the same people or is that different people?

By the way, in your comment about economics, let me just—one other thing. We often say to corporations, however, that if they are

going to go to China and you are going to open up a business in China, this is an economic issue, color it gone because it won't take long before whatever you have there will be copied by that society and you will be out of business there. And so corporations have to look very carefully because it is a big market, but they are not—it is a Delta T, a period of time in which you can operate there before you will now have—build your own competitor.

Mr. SWALWELL. Great. Thank you, Mr. Chairman. I yield back.
Chairman BROUN. Thank you, Mr. Swalwell.

My good friend from Arizona, Mr. Schweikert, you are recognized for five minutes.

Mr. SCHWEIKERT. Thank you, Mr. Chairman.

Is it proper to say Professor Vest?

Dr. VEST. Chuck is fine.

Mr. SCHWEIKERT. Well, okay, if you say so. Professor Chuck, if this were the 1980s—if I remember the language we used back then—it was called the run-fast theory very similar to your bucket. If anyone goes back that long, the old—we were going to produce, particularly in military technology—this much faster than the Soviet Union. In today's world where everything is ultimately sitting out there on a server somewhere, can you ever run fast enough that our technological value, both—whether it be military, whether it be economic, data research—is produced in a way where you can truly have, you know, something—at MIT or other fine universities a truly open platform?

Dr. VEST. That is a really good question, and it seems to me that when it comes to the distinction you made, I suspect that under today's contracting laws and everything else, literally military technology could not run fast enough to stay ahead if it were as you have said.

I do think, however, that basic advances in information technology and life sciences and manufacturing and so forth, in new chip design, new materials, bioinformatics and so forth, these things in fact do move fast enough that we ought to be able to claim them for a significant period of time, perhaps start initial manufacturing in the United States, and then it is probably going to drift off.

Dr. VEST. But if you don't try to stay out ahead of the curve, then you know you are dead.

Mr. SCHWEIKERT. Well, what is the United States ultimately resource?

Dr. VEST. It is our free market.

Mr. SCHWEIKERT. I will make the argument it is our entrepreneurship.

Dr. VEST. It is our free markets and entrepreneurship.

Mr. SCHWEIKERT. Yes, it is that we do creative destruction really well, really fast.

Ms. Van Cleave, I have sat through a series of these hearings on sort of the banking finance side and learning, you know, the networks that are attacking bank accounts and collecting credit cards number and these—and fascinating and I am not breaking any rules because a couple of those were inside the tank—that we literally have criminal organizations, criminal entrepreneurs that are not nation states. They are literally—they collect the data and it

is up for sale for whoever will pay for it. Are we now seeing that in the science and technology and military espionage world where I am not a state actor; I am in it for the money and I am going to collect the data and put it up, and whoever is willing to buy it?

Ms. VAN CLEAVE. Congressman, I don't have specific insights into the kinds of entrepreneurial criminal organizations that might be going against our S and T base in that way, but I can tell you that I do know that there is a third country market if you will in things that get stolen by other governments.

Mr. SCHWEIKERT. Well, that was going to be—well, in—

Ms. VAN CLEAVE. So it wouldn't surprise me to learn that there could be entrepreneurs who are also taking advantage of that market to be out pedaling their wares.

Mr. SCHWEIKERT. Mr. Major, in that same thread, I have heard lots of stories out there where—whether they be entrepreneurs but also literally engineers, scientists saying you—if you can steal the equipment, we will reverse it for you. We will reverse engineer it.

Mr. MAJOR. There are specific cases of that. Of the ones we have been tracking in SPYPEDIA we find that happening. Someone may be a foreign national but they see the technology and say, hey, I can compete against this. I can take this out and set up my own competitive business or buy someone to do that. So yes, we have empirical cases that feature it exactly. I would like to add one thing to your fast run—run-fast strategy that we had during the Reagan Administration is that that run-fast didn't work very well because we found out through a source called farewell manmade vitriol that the—as we develop new technology, immediately it was being stolen by the Russians. So they were not three generations behind us; they were about one or two generations because their espionage network was so large and so successful, it really shaped—reshaped our defense thinking as a result of that. And there is one source who told us that.

But yes, there are examples like you are talking about. In this business, you have to look at this and say whatever the—whatever someone is stealing, you know, you can't keep anything secret forever. You have to keep it what I call a Delta T. It is a period of time before it will eventually become public, but you only have to define how long and how much you want to invest in that Delta T. How long do you want to keep that secret for that period of time, and that is where you put your efforts and so forth.

Mr. SCHWEIKERT. Thank you, Mr. Major. Well, being for all of us as Members of Congress, we all know what it is like to be in an environment where there are no secrets.

With that, I yield back, Mr. Chairman.

Chairman BROWN. Thank you, Mr. Schweikert.

I want to thank the witnesses for you all's valuable testimony and I want to thank Members for you all's great questions.

Members of the Committee may have additional questions for you guys, and we will present those for you for you to respond in writing. And if you will do those please expeditiously. The record will remain open for two additional weeks for comments, for written questions by Members.

Thank you all so much, very informative, great testimony from all four of you. We really appreciate your effort. As I said in my

opening statement, I don't have a prescription to balance between openness and security, and I believe very firmly if—that property rights, whether it is real property or intellectual property, is absolutely critical for a free society. And if we have private entities or government entities that are stealing our property, whether it is military property, real or intellectual, whether it is research and development or what have you, that we are not a free people anymore and it is absolutely critical.

So if you all have a prescription of how we can balance this and how we can go about making sure that our national labs and our businesses and any other entity here in this country can remain secure but be as open as possible, I would welcome you all's suggestions for any kind of legislation that we can go forward. So please let us know.

Thank you all so much for coming today and I appreciate your valuable time. And again, I appreciate your patience and we will look forward to hearing your written answers back. If you would, please do so as expeditiously as possible.

The witnesses are excused and this hearing is now adjourned.
[Whereupon, at 4:02 p.m., the Subcommittee was adjourned.]

Appendix I

ANSWERS TO POST-HEARING QUESTIONS

Responses by Dr. Charles M. Vest

DRAFT RESPONSES
HSST COMM. OVERSIGHT HEARING
CMV 6-11-13

6/12/13 9:07 PM

Responses to Dr. Broun's Questions

- 1. As suggested by the title of the hearing, our ultimate goal is to develop sensible policies that balance scientific cooperation and security. How would you define sensible policies vs. bad policies? Further, how would we know what constitutes an appropriate balance between scientific cooperation and security?**

It seems to me that the emphasis should be on actual security programs, i.e. the real-world application of our laws and policies. Just as in good business practice, security programs need to be well thought out but then continuously improved or discontinued based on periodic data-driven evaluation. Indeed, a National Academies committee co-chaired by former Secretary of Defense William Perry and myself addressed this issue. Our recommendations included a framework for security programs that specifically included eight elements:

- a. Agency Competency
- b. Well-defined Purpose
- c. Measured Effectiveness
- d. Appropriate Authorization
- e. Appropriateness of Data
- f. Redress for those inappropriately affected
- g. Periodic Assessment
- h. Appropriate Oversight.

This framework was developed especially for information-based programs, such as those making headlines today. However, I believe the key thing is periodic, structured, and serious evaluation of the effectiveness of security programs that weighs the real (not theoretical) benefits and costs. In this case the "benefits" would be detection or disruption of damage to our security and/or economy, and the "costs" would be disruption or damage to our scientific and technological advancement and leadership and economic opportunities.

2. I understand that certain countries like China, Russia, Iran and North Korea require additional scrutiny because of what we know about their interests and attempts on our technologies and information. Keeping that in mind, how do we implement policies that protect our assets while avoiding accusations of profiling?

To the greatest extent possible, we should treat every individual who has been admitted to the U.S. to study or perform R&D the same. Sadly, Timothy McVeigh was just as evil, and his acts just as horrendous, as those of any foreign terrorist might be. Critical industrial IP and truly essential security information should be protected from domestic criminals and noncitizens alike. The criteria should be the same.

On the other hand, when things like cyber intrusions occur, we must counter where the source wherever it is. If the source is dominantly in one of the countries mentioned in your question, I don't consider that to be profiling. At the same time, we don't want to blindly shut our doors. Many of our best researchers and entrepreneurs have come here from China, Russia, and Iran.

3. Do you have any recommendations on what steps our academic institutions and labs can take to defend attacks directed specifically at our cyber infrastructure, and can we share or apply those suggestions to American businesses and government agencies which are constantly bombarded by cyber-attacks from foreign nationals?

This is a very important matter, but the specific answer to your question is a technical matter beyond my expertise. However, there are a couple of points I would like to make:

First, cyber attacks and intrusions are simply facts of modern life. They can be, and are, effectively carried out by individuals with widely varying motivations as well as by state actors. Second, for the foreseeable future, there will be a continuous escalation in the nature and sophistication of such attacks, and therefore, countermeasures must also advance dynamically; there will be no one-time fix.

There is a lot of cyber security expertise in our universities and in small companies. My colleagues and I would be glad to point your staff toward some of these if that would be helpful.

4. The classification system is an important tool to keep truly sensitive information safe and secure. But overclassification can jeopardize national security by preventing federal agencies from sharing information internally, with other agencies or with non-governmental organizations. How can we prevent overclassification and ensure that classifiers comply with existing criteria for classifying documents?

I believe that we have serious problems of overclassification and mission creep. According to a 2011 report by the Director of National Intelligence, over 4 million people held security clearances, and of this group, 1.2 million held Top Secret or TS/SCI clearances. Beyond that, there is an unnecessary and confusing proliferation of categories like "sensitive but unclassified," and an overly broad and badly outdated export control regime.

In a technological world that moves as fast as today's, it seems very clear that we need to narrow the scope of classification by narrowing the criteria which classifiers apply to better represent those things that are truly critical to our security. In my view, it would be good practice to do periodic post audits of representative samples of classified materials and activities to honestly assess whether the initial decision to classify was justified in retrospect. The system could then be continuously improved and narrowed over time.

My experience observing and working with private industry suggests that they are much better and more focused than the government about what IP really needs to be protected. Their domains of interest are often quite different than that of the national security community, but I think the federal sector could learn from the business sector.

Finally, especially in the commercial context, I continue to believe that it truly is more important to fill our proverbial bucket of new knowledge and technology than to obsessively plug leaks. If we can reduce

DRAFT RESPONSES
HSST COMM. OVERSIGHT HEARING
CMV 6-11-13

6/12/13 9:07 PM

unnecessary bureaucracy and security, we can get new things into the hands of our entrepreneurs to create jobs and get them to market. Speed is really important today.

Responses by Dr. Larry M. Wortzel

HALL OF THE STATES, SUITE 602
444 NORTH CAPITOL STREET, N.W.
WASHINGTON, D.C. 20001



PHONE: 202.624.1407
FAX: 202.624.1406
E-MAIL: contact@uscc.gov
www.uscc.gov

U.S.-CHINA ECONOMIC & SECURITY REVIEW COMMISSION

WILLIAM A. REINSCH, CHAIRMAN
DENNIS C. SHEA, VICE CHAIRMAN

Representative Paul Broun, M.D.
Chairman
Subcommittee on Oversight
Committee on Science, Space and Technology
U.S. House of Representatives
2321 Rayburn House Office Building
Washington, DC 20515-6371

Dear Chairman Broun,

I am pleased to respond to your questions regarding my testimony before the Subcommittee on May 16, 2013. These responses represent my own views and not those of the U.S.-China Economic and Security Review Commission.

1. Does the U.S. have a comprehensive strategy of its own to counter China's robust, nationally-directed strategy to steal American technology and ingenuity? If not, what more should we be doing?

The United States has a comprehensive national counterintelligence strategy as provided for in the Counterintelligence Enhancement Act of 2002 (Public Law 107-306 of November 27, 2002). The National Counterintelligence Executive (NCIX) serves as the head of counterintelligence for the United States Government and reports to the Director of National Intelligence. The law also informed the Director of National Intelligence that it is the sense of the Congress that the DNI should seek the views of Attorney General, the Secretary of Defense, and the director of the Central Intelligence Agency in selecting the National Counterintelligence Executive.

The NCIX is responsible for producing a strategy for the counterintelligence programs of the United States, and that strategy must be updated every three years. The last update I was able to locate was dated 2009 (although it does not seem to have been published until 2010); therefore a new strategy may be in development. The 2009 counterintelligence strategy does not mention China specifically. However, I have met with the staff of the NCIX section responsible for China and East Asia a number of times. They are highly competent counterintelligence professionals drawn from across the intelligence community. In general, the strategies and reports to Congress from NCIX identify, characterize, and seek to address pervasive and global threats. Internally, and in classified strategies inside the intelligence community, the NCIX develops strategies specific to China. Some examples of NCIX documents are:

- The U.S. for the first time published the Counterintelligence National Strategy in 2005 to focus resources on the most serious current and emerging threats to U.S. technology and ingenuity. The strategy has several goals, one of which is to protect "U.S. advanced technologies and sensitive information in the defense, intelligence, economic, financial, public health, and science and technology sectors."
- In 2007 and 2009, the NCIX developed National Counterintelligence Strategies.

- In May of 2010 the National Counterintelligence Executive released the 2009 National Counterintelligence Strategy that identified the “protection of U.S. economic advantage, trade secrets and know-how” as a key component of the strategy.
- The Office of the National Counterintelligence Executive publishes a biannual report to congress titled Foreign Spies Steal U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic and Industrial Espionage, 2009-2011.

China’s espionage has become a far greater threat to the United States since the mid-1990s. This expanded threat is a result of Beijing’s increasing demand for strategic intelligence, its reliance on technical intelligence collection to support its national industrial development and science and technology plans, and expanding collection capabilities. As the number of Chinese students, researchers, academics, and businessmen working in the United States increases, it will become more difficult to discern a Chinese traditional or nontraditional collector from a legitimate entity due to the openness and ease with which academic and commercial business is conducted in the United States. Therefore, it is imperative that the U.S. develop a comprehensive and dynamic classified list of nations and actors that pose the most serious espionage threat to the U.S. government and industry.

Development of this list would require input and maintenance from throughout the U.S. Department of Defense and Intelligence Community. It almost certainly would include China, which was identified in the 2009 NCLX report on the theft of U.S. Economic Secrets as “the world’s most active and persistent perpetrators of economic espionage.” From this list, additional limitations on access to sensitive research or technology could be imposed on foreign individuals from those nations of concern. Though the entire document should remain classified, its key conclusions and recommendations should be released to the public when such release would not compromise intelligence sources and methods. Releasing as much of the document to the public as possible would help educate the staffs at academic institutions and laboratories and ensure they are aware of the threat posed by China.

I note that in the Reagan Administration, the Interagency Groups designed to coordinate national policy operated directly under the National Security Advisor. At that time there was an Interagency Group, Counterintelligence (IG/CI) with a full time director on the National Security Council (NSC). So far as I know, at the present time, there is no full-time NSC official with responsibility for U.S. counterintelligence (although there is a full-time cyber security director on the NSC).

Finally, Congress might want to examine the budget elements of the Foreign Counterintelligence Program (FCIP), which is under the budgetary control of the DNI to see if enough attention is devoted in the Program to China.

2. Concerning U.S. efforts to balance scientific cooperation and security, how would you define sensible policies vs. bad policies?

Sensible policies must promote open and collaborative academic and scientific research and exchange while protecting information that is moving from fundamental research into defense or industrial applications. If laboratories or academic institutions are engaged in fundamental research and at the same time are involved in research on proprietary, export-controlled or classified matters, it is incumbent on the government or industry to ensure that foreign nationals do not get unauthorized access to export controlled or classified research. Also, the information systems of institutions involved in controlled or classified research should be separate from those that are open to all researchers. Also, sensible policies should recognize that certain nations have targeted programs to steal foreign technology.

Bad policies place too much weight on arguments that all scientific exchange must be open and do not recognize that there may be new, cutting edge innovations or research that has near-immediate application in the defense or national security sector. Finally, in my experience, bad policies often are associated with a bureaucratic approach by administrators who have no practical experience in the production of materials or systems and who do not understand the transition from fundamental ideas and research into applied experimental development.

3. How does the U.S. implement policies that protect our technologies and information while avoiding accusations of profiling?

In general, U.S. policy should focus on protecting technologies and information. For example, the U.S. could take the following measures:

- Ensure U.S. businesses are fully aware and compliant with laws and regulations pertaining to the release of export-controlled technologies to foreign nationals in the United States.
- Clearly codify distinctions between different levels of research, and then define security requirements – with consequences for negligence – for each level. With respect to China, and other countries with strong records of economic espionage, cyber espionage, theft of intellectual property, reverse engineering, and the proliferation of weapons, the U.S. should expand and refine the export-control system to refine the licensing and export of materials, equipment, and forms of technology, including dual-use technology. My view is that if a particular technology is ubiquitous, there is little reason to try to protect it under license. Whereas, if the U.S. or U.S. allies are far ahead in a technology area with direct military application, or a dual-use technology, then that technology may deserve protection.

However, I have no philosophical problem with profiling in counterintelligence programs. Indeed, decades of experience in intelligence collection and counterintelligence lead me to conclude that it is pretty dumb not to profile. If a nation has an established record globally of stealing intellectual property, abusing its citizens, coercing its citizens to steal property, and has no strong rule of law, it is fair to pay more attention to the nationals of that country.

Also, in intelligence collection, for decades the preferred method of operation for China's intelligence services has been to target Chinese nationals, ethnic Chinese in foreign countries, and the citizens of foreign countries with a strong attachment to China because of family connections, business investments, cultural interest, or academic interest. However, China's intelligence services recently has shown increased willingness to target individuals without ties to China who have access to information Beijing wants to collect. Therefore, in counterintelligence programs, it makes no sense to ignore these traditional methods of operations.

The U.S. should increase the public's awareness of China's use of students, scientists, and scholars attending U.S. universities and research universities as collectors on behalf of China, whether witting or unwitting. Beijing likely encourages Chinese students to study specific technology areas in the United States that support China's national research and development objectives. Any Chinese organizations associated with intelligence activities that sponsor academic research activities, social development, or international exchanges should be monitored and investigated.

4. What steps can our academic institutions and labs take to defend from attacks directed specifically at their cyber infrastructure, and can we share those suggestions to American businesses and government agencies?

Implementing security “best practices” almost certainly would reduce the effectiveness of Chinese cyber efforts. While not ensuring perfect security, such practices would make it more difficult for cyber actors to gain an initial foothold and maintain persistent access in the networks of academic institutions and labs. In particular, information systems housing research and development data that is likely destined for use in classified or unclassified national security programs (such as weapons) should be encouraged, or even required, to implement these best practices.

- Placing sensitive information on stand-alone networks rather than Internet-connected computers would cut off the most common method used by intruders to compromise and steal data from computer systems.
- Using multifactor authentication – generally a password in combination with a piece of hardware of biometric identifier – makes using stolen passwords difficult or impossible without also stealing or copying the physical authentication token.
- Encrypting data at rest and disabling unused ports and computer media would make it more difficult for intruders to conduct cyber-attacks.
- Enhancing user awareness of common social engineering tactics would help lessen the number of successful compromises.

China probably has the technical capability to compromise and extract data from closed academic and scientific institution networks by exploiting users who transfer files between Internet-connected and closed networks with removable media devices. China could face challenges conducting these “air gap attacks” against closed U.S. networks that have strong policies and procedures for moving data via removable media and examining it for malicious content.

Academic institutions and labs could cancel or limit their interactions with Chinese institutions and labs that are linked with Chinese cyber actors or who are known to have benefited from Chinese cyber activity or intellectual property theft.

The U.S. Government should publish and make available to laboratories and academic institutions a list of the known cover or proprietary organizations used by Chinese intelligence services as places of employment or study for intelligence collectors.

5. How can we prevent over classification and ensure that classifiers comply with existing criteria for classifying documents?

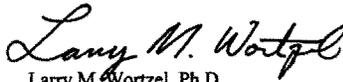
President Obama’s 2009 Executive Order No. 13526 acknowledges the need to prevent over classification. Nevertheless, there remains a significant gap between written guidelines on proper classification and the actual practice of classification. In recent reports addressing the issue, both the Brennan Center for Justice at New York University School of Law and the Public Interest Declassification Board suggest this gap is attributable to an environment that incentivizes risk-avoidance and over classification and provides no incentive to refrain from or challenge over classification. These reports make a number of recommendations, of which I believe the following are the most important:

- Introducing a minimal administrative burden upon original and derivative classifiers, such as a brief questionnaire asking these individuals to justify their classification, to counteract the tendency of rote classification.

- Incorporating occasional audits by the agency's Office of the Inspector General and stronger training programs to increase accountability into the accounting process.
- Implementing "safe harbor" or "hold harmless" rules for derivative classifiers who fail to follow original classification decisions when those decisions are not clearly conveyed. Distinguishing under classification in these instances with willful or negligent unauthorized disclosures. This recommendation could alter the tendency for such an individual to avoid the risk of and sanctions associated with under classification.
- As a corollary to the above, clarify the specific protections afforded intelligence sources and methods, particularly to derivative classifiers.

Thank you for the opportunity to respond to these questions. If I can be of any more assistance in matters regarding espionage threats against federal laboratories of federally funded research in academia please contact me.

Sincerely,


Larry M. Wortzel, Ph.D.
Commissioner

Responses by Hon. Michelle Van Cleave

House Science Committee, Subcommittee on Oversight
Hearing on "Espionage Threats at Federal Laboratories: Balancing Scientific
Cooperation while Protecting Critical Information"
May 16, 2013

Michelle Van Cleave
Answers to Questions for the Record to Dr. Broun

1a. In as much detail as you can provide without compromising classified information, what actions are the counterintelligence and law enforcement communities taking to detect, deter and neutralize intelligence threats to the science and technology communities?

From my past experience, I can tell you that foreign intelligence threats to the U.S. science and technology base are a serious concern to U.S. counterintelligence and law enforcement. Security awareness training is routinely practiced at federal laboratories and among cleared personnel. Technology control laws and regulations are properly enforced. The FBI maintains outreach programs to bring threat information to U.S. business and industry and academia engaged in S&T activities that may be of interest to adversaries or competitors.

For a more complete answer, I would urge the Committee to request a briefing from the incumbent National Counterintelligence Executive. I think the Committee will find that, under the current case-by-case business model, counterintelligence and law enforcement are performing at very high levels of professionalism, under the resource constraints imposed by competing national priorities. It is the business model itself that is the limiting factor, as I explain below.

1b. Do we have a comprehensive strategy of our own to counter China's robust, nationally directed strategy to steal American technology and ingenuity?

No. In the first place, to my knowledge there is no national strategy governing our overall relations with China. Nor do we have broad policy guidance to integrate the instruments of state power – intelligence, law enforcement, diplomatic, economic, military and others – to address Chinese S&T acquisition activities.

In the second place, the U.S. counterintelligence enterprise is not postured globally to detect, deter or neutralize the intelligence activities of China or any other foreign power, or to execute strategic counterintelligence operations. Indeed, we know surprisingly little about adversary intelligence services relative to the harm they can do. Under the current business model, there is no national level system that enables the integration and coordination of the diverse activities of U.S. counterintelligence to achieve common strategic objectives. No single entity has a complete picture to provide warning of possible foreign intelligence successes, to support operations, or to formulate policy options for the president and his national security leaders.

1c. If not, what more should we be doing?

In my opinion, it would be extremely helpful to have a clear national strategy to bring coherence to U.S. policies and programs concerning China. If President Obama follows the path of his predecessors and fails to issue one, the Congress could undertake to do so at least for the purpose of providing standards against which authorization, appropriations and other legislative matters might be measured. For example, here is a sample bill, which I offer for the Committee's consideration:

H.Res. _____ U.S. RELATIONS WITH CHINA***Setting forth a strategic policy framework for U.S. relations with the People's Republic of China to guide matters before the House of Representatives.******Whereas***

Relations between the United States and China will be key to Americans' peace and prosperity for decades to come, but successive U.S. administrations have failed to provide a guiding strategy or framework for U.S. policy toward China, inviting conflicting and internally contradictory policy pursuits;

There is a time-honored bond of friendship between the American and Chinese peoples, but the Government of China has continued to oppress the people of China by denying basic human rights, such as freedom of speech and religion, and suppressing minority groups;

The PRC has become a formidable economic power and a significant trading partner to the betterment of American consumers and businesses who enjoy access to decent quality, low-cost Chinese goods, but the PRC has repeatedly violated WTO rules and U.S. export controls laws, engaged in industrial and cyber espionage, and infringed U.S. patent and other intellectual property rights;

The U.S. has a historic commitment to freedom of the seas, strategic partnerships with Japan and Taiwan, strong defense alliances and cooperation with regional allies, but the PRC is pursuing a rapid military buildup that challenges U.S. defense capabilities and the stability and security of friends and allies in East Asia and the Pacific.

Successive U.S. administrations have worked to achieve more transparency and confidence in China's relationship with the U.S. and Chinese activities worldwide, but China continues to regard the United States as its principal strategic adversary and to expand its military, intelligence and economic reach globally, including a significant intelligence presence within the United States.

Therefore be it Resolved, that House of Representatives shall measure such bills and resolutions as may be considered by this Body or its Committees of jurisdiction concerning or affecting U.S. relations with China against these guiding strategic U.S. objectives:

To sustain and deploy clear and unambiguous defense and intelligence capabilities to resist any resort to force or other forms of coercion that would jeopardize the peace and stability of the Asia/Pacific region or the security of U.S. friends and allies;

To exert internal pressure on the Chinese government to support liberalization, transparency, democratization and human rights;

To engage with the Chinese government to eliminate, on the basis of strict reciprocity, outstanding disagreements;

To convey clearly to Beijing that responsible behavior on their part will create the possibility for a genuine partnership to our mutual advantage, while any unacceptable behavior will incur costs that would outweigh any gains;

To prevent the transfer of technology, intellectual property or equipment that would make a substantial contribution to Chinese military capability; and

To ensure a robust economy and self-sufficiency at home as the surest means of providing leverage to deal with China on all fronts.

Resolved further, that any and all Authorization or Appropriations Bills reported to the Full House for consideration shall be accompanied by a Report setting forth their compliance with these principles.

The U.S. government also needs to establish a strategic counterintelligence program to integrate and coordinate U.S. counterintelligence assets to achieve strategic objectives – not to supplant current case-by-case operations but to add a new strategic dimension to the national CI enterprise. While the creation of such a program goes beyond the jurisdiction of this Committee, the Oversight Subcommittee might consider addressing their concerns over the vulnerability of U.S. S&T to the House Permanent Select Committee on Intelligence (HPSCI) for follow up. I am unaware of a precedent for a sister Committee of the House referring a matter to the HPSCI, but the logic behind its creation suggests that the Chairman should be receptive to such a request.

2) As suggested by the title of the hearing, our ultimate goal is to develop sensible policies that balance scientific cooperation and security. How would you define sensible policies vs. bad policies? Further, how would we know what constitutes an appropriate balance between scientific cooperation and security?

As I see it, in this context security is a risk management function that exists to support the goals of scientific cooperation. Part of the answer to developing sensible policies includes educating S&T personnel about security in order to give them a true understanding of the several security disciplines, how they work and why they matter, rather than just handing them a list of rules to follow.

Secondly, if we had better insights into foreign intelligence threats and better means of dealing with those threats (i.e., more effective counterintelligence programs and capabilities), then the risks associated with international S&T cooperation would go down. The former Administrator of NASA Mike Griffin and I co-authored an article on the subject of US-Chinese cooperation in space, which speaks to this question. I am providing the text so that it might be included in the record:

The Washington Times**GRIFFIN & VAN CLEAVE: Working with China opens door to espionage****Cooperating in space: Time for a timeout**

By Michael Griffin and Michelle Van Cleave July 7, 2011

It was an awkward moment, to say the least. Testifying before a House Appropriations subcommittee, President Obama's science adviser, John P. Holdren, was describing the Obama administration's ongoing discussions with China to develop joint space projects.

Problem is, a law Mr. Obama had signed just weeks before prohibits NASA or Mr. Holdren's Office of Science and Technology Policy (OSTP) from engaging in any bilateral activities with China.

When challenged ("Do you understand the meaning of the word 'prohibits?") Mr. Holdren asserted on advice of counsel that the president was construing the law as consistent with his inherent constitutional authority to conduct negotiations (lawyer-speak for "You can't tell us what is off limits").

Mr. Holdren may pay the price (literally) for this novel interpretation. Now Frank R. Wolf, chairman of the subcommittee on commerce, justice, science and related agencies is threatening to force compliance with the law by cutting OSTP's budget when his subcommittee meets today to mark up next year's appropriations bill.

Leaving aside the "who's-in-charge" issue, the larger question is: Is this a good law or a bad law?

As the former head of NASA and the first to visit China, and the former head of U.S. counterintelligence, we might be expected to reach different answers. Yet we are both in the realist camp. There are two schools of thought about space cooperation with China, each with its own self-fulfilling prophecy:

- o The Chinese are determined to steal our technology and get ahead militarily at our expense, so any cooperative space projects are a lose-lose for us. (The national security realists.)
- o Chinese espionage will succeed no matter what we do, so we might as well get what we can out of cooperative projects. (The science and technology "realists.")

We think both of these views are overly simplistic.

As America prepares to box up the last space shuttle for museum display, China is on a trajectory of explosive growth in space - under a highly disciplined veil of secrecy. We have precious few insights into what the Chinese are doing or why. Based on our experience with the Soviets during the Cold War and with Russia since, we think carefully managed cooperative space projects - not putting partners into the critical path, just selective joint efforts on interesting things - could be the single best window into Chinese plans and capabilities in space.

MICHELLE VAN CLEAVE

ANSWERS TO QUESTIONS FOR THE RECORD

At the same time, the Chinese have a far-reaching, multilayered program for illicit technology acquisition from the United States. They are keenly interested in space technology, in which America is still the world's unquestioned leader. Just ask 30-year spy Dongfan Chung (Orange County, Calif.) or Shu Quan-Sheng (Newport News, Va.) or Lian Yang (Seattle), now serving time for passing inter alia space-shuttle communication technologies, space-launch cryogenic fuels data and satellite semiconductor devices, respectively. And that's just the tip of the iceberg.

We want to open channels that allow the possibility that in the long run, a potential adversary can become a partner and ally. Joint space projects characterized by transparency, reciprocity and mutual benefit can be an excellent way to begin. Is it possible to manage the inherent risks while pursuing our larger goals?

If we had an effective counterintelligence capability to identify and disrupt Chinese collection activities, this would be an easier call. Timely tripwires that signal when the other side is stepping across the line would enable us to manage the risk of close interaction and gain the advantage of rare insights into China's space program. Unfortunately, U.S. efforts to build such a strategic capability against foreign intelligence threats have fallen by the wayside, while Chinese espionage continues to grow.

We believe the United States is paying an opportunity cost by walking away from possible joint space projects with China, but without a more robust counterintelligence capability, we stand to lose more than we would gain. Nor does it make sense to venture into cooperative activities that may contribute to China's military modernization or global strategic ambitions.

The statutory prohibition against bilateral space projects wisely puts the brakes on a downhill rush to engage with the Chinese. In the absence of a larger strategy guiding policy and programs on China, it is unclear whether cooperative space projects would advance or hinder U.S. interests. The Obama administration should use this timeout to take stock and then return to Congress with a coherent approach to space cooperation with China that is more than a raw assertion of the president's authority to conduct foreign affairs as he may please.

Michael Griffin was the administrator of NASA under President George W. Bush. Michelle Van Cleave was the national counterintelligence executive under President Bush and assistant director of the White House Office of Science and Technology Policy under Presidents Reagan and George H. W. Bush.

© Copyright 2011 The Washington Times, LLC.

3) I understand that certain countries like China, Russia, Iran and North Korea require additional security because of what we know about their interests and attempts on our technologies and information. Keeping that in mind, how do we implement policies that protect our assets while avoiding accusations of profiling?

China's intelligence services routinely target overseas Chinese for recruitment; they are the ones doing the profiling, not the U.S. government. I am unaware of the other countries cited following similar practices.

4) Do you have any recommendations on what steps our academic institutions and labs can take to defend from attacks directed specifically at our cyber infrastructure, and can we share or apply those suggestions to American businesses and government agencies which are constantly bombarded by cyber-attacks from foreign nationalists?

Academic institutions and research facilities can begin by understanding that they are targets for foreign collection, and protect their information systems accordingly. Business and industry have additional commercial incentives for protecting their proprietary information, and our entrepreneurial society is responding by providing ever more and better cybersecurity solutions. The legal system and the insurance industry also have an increasingly significant role to play in allocating risk for cyber-related losses ("who pays, protects"). But history has shown that the offense will always have an advantage over the defense, which means that security measures alone will never be enough. At the national level, the United States also needs robust capabilities to identify, assess and defeat cyber operations directed against us.

5) The classification system is an important tool to keep truly sensitive information safe and secure. But overclassification can jeopardize national security by preventing federal agencies from sharing information internally, with other agencies or with non-governmental organizations. How can we prevent overclassification and ensure that classifiers comply with existing criteria for classifying documents?

One of the most-cited lessons coming out of the September 11 terrorist attack was a failure to "connect the dots" – *i.e.*, to bridge what was known from foreign intelligence sources with law enforcement or other domestic information about potential threats. The hurried conclusion was "we need to share more" when the conclusion should have been "we need dedicated, discrete intelligence fusion capabilities" as well as assigned responsibilities to take action. As a result, the current system for protecting intelligence sources and methods and other sensitive national security information has become distorted in two ways.

First, the move from a standard of "need to know" (pre-9/11) to "need to share" (post 9/11) has resulted in an exploding population of people with security clearances, overwhelming the resources of the personnel security system to keep up. I have seen statistics showing that 5 million people – one in every 50 American adults – now hold security clearances. Security challenges are close to impossible to meet with a population that large; at best, there will be serious gaps, indiscriminate enforcement and escalating risk. Among other things, we see the

emergence of destructive individuals like Bradley Manning and Edward Snowden -- bit players on a quest to prove their own importance, taking advantage of their overly broad access to sensitive information.

Second, all of the incentives are to "dumb down" classification standards, *i.e.*, to classify more and broader categories of information as "secret," reserving "top secret" for what was previously "secret." In turn, more people need security clearances to access mundane "secret" information to do their jobs, putting them in line for moving up the ladder to higher levels of clearance. Along the way, it's not difficult to imagine how individuals who see relatively innocuous information labeled "secret" may acquire a casual disregard for the weighty responsibilities that adhere in protecting information which, if disclosed, in fact would cause serious harm to the nation's security.

A far better approach would be to decide what truly needs to be protected and to protect that extremely well, including returning to clear "need to know" standards that can be responsibly implemented while facilitating the operations they exist to support.

Responses by Mr. David G. Major

House Committee on Science, Space and Technology

Subcommittee on Oversight

Answers by David Major, President of CI Centre and SPYPEDIA®

- 1) What should the Science and Technology Community (STC) be on the look for? Are there specific cases you can reference that clearly demonstrate the methods used by foreign entities to acquire sensitive information?

The first part of this question is extremely broad and thus difficult to provide a definitive response and it is unclear what specifically is being asked. Indications of espionage and loss of information can sometimes be reflected in observable actions on the part of the intelligence collector. In the intelligence and counterintelligence profession there is an axiom that states "the worst situation is not to have a source but the second worst situation is to have a source". This is true because if sensitive (classified) information is collected and it is of value the collector is faced with the need to take action on the collected information. This is actionable intelligence. If the collector takes action it must do so in a way that does not reveal the information in is the possession of the collector. Sometimes the information is so important it must be acted upon and when this action takes place the "owner/originator/victim" observers that action and knows the information has been compromised. When the STC becomes aware information is compromised they know it has been lost because of technical collection (SIGINT) or someone has compromised the information (the HUMINT betrayer). When the STC becomes aware of this they will (must) take action to look for the source of the compromise and change their procedures, thus resulting in the loss of the sources by the collector. Thus the conundrum that faces intelligence collectors "the worst situation is not to have a source but the second worst situation is to have a source". The prevention formula for the security professional is the creation and staffing of a "what's going wrong center" to monitor apparent compromises.

The second question addresses the method used by foreign entities to acquire sensitive information. This is also a very broad question as the heart and soul of the counterintelligence community is to answer this question for every foreign entity that collects against the STC. The correct answer is, it depends on the foreign entity conducting the collection. There are some broad answers to the question. Information is lost because of technical collection (TC) directed against the STC including but not limited to internet mistakes. Technical collection operations in the USA, in third countries and in the home country of the foreign collection entities will vary significantly. Access to buildings, individuals, and transportation methods all carry their own vulnerabilities and opportunities. Any technical device is the potential target of a collection operation from a telephone, cell phone, computer, tablet, copy machine. The key is access to the device and how aggressive and risk taking the collector is will to be in gaining access to

devices. An axiom of the counterintelligence community is the farther the target is from the domestic base the higher the threat level. The threat is lowest in the USA, it increases when TDY or PCS overseas in a third country and still higher when the target is in the collectors country. While TC is always present as a threat the second threat and collection method is the insider human source. The human source (betrayer) is either recruited to be a "spy" or volunteers to the foreign entity to betray trust and provided information. The ability of a foreign entity to obtain and handle the betrayer will vary greatly and thus the method used to conduct this collection is varied. Every case has its own unique method of operation (MO) but some generalizations are universal. Everything being equal the foreign collection entities will try not to meet the betrayer often and when they do meet with the human source (betrayer) in will occur in the following preference:

1. In the foreign collection entities home country.
2. In a friendly third country (foreign to the collector entity).
3. In any third country.
4. In a USA city where the collection entity has a diplomatically protected facility and the collector has diplomatic immunity.
5. In a USA city the betrayer and the diplomatically protected collector can both travel to.
6. In a USA community in which the betrayer lives and the diplomatically protected collector can travel to.
7. In any city the betrayer can travel to and a non-diplomatic protected foreign collector entity and travel to.

Any collection operation requires the passage of information. Currently this is almost completely conducted digitally with the betrayer e-mailing information out from the place of employment or placing the information on a foreign storage device such as a thumb drive and taking the material out of the facility in which the material is stored. The information today is often e-mailed to the collector or placed in a draft e-mail account used by the betrayer and the collector.

We track this daily in detail on SPYPEDIA®, our open source membership data base, www.spypedia.net

- 2) As suggested by the hearing, our ultimate goal is to develop sensible policies that balance scientific cooperation and security. How would you define sensible policies vs. bad policies? Further, how would we know what constitutes an appropriate balance between scientific cooperation and security.

The core of this question involves the question "what scientific information should be protected, why it should be protected, how should the information be protected and how long should it be protected". Clearly this is a judgment decision that requires professional oversight experience. During the hearing the concept of "the leaky bucket theory" to security surfaced. I do not and never have ascribed to this halfhearted approach to security. It assumes information will always be lost so just create new information of greater value faster than you are losing it. It also assumes you will lose old information (bottom of the bucket) and keep secure the "new" information being added to the bucket. No assurance of this magnitude could or should be assumed to established policies and procedures. New (more important) information can be lost just as easily as old (bottom of the bucket) information. This problem needs to be approached with the concept that nothing needs or can be keep secure indefinitely. In essence everything will become public eventually; the key to this really is how long before this occurs. Trying to keep everything secure indefinitely will lead the keepers of the secret information to lose vigilance. Appropriate balance between scientific cooperation and security revolved around ensuring real secrets are kept secret with the full cooperation of those tasked with having access to the protected information. Policies that ensure appropriate resources are provided to protect this information and continued education of the keepers of the secret and the import of the culture surrounding the secret are an appropriate balance. A leaking bucket culture for protection of information will create a work force that does not take the protection seriously.

- 3) I understand that certain countries like China, Russia, Iran and North Korea require additional security because of what we know about their interest and attempts on our technology and information. Keeping that in mind, how do we implement policies that protect our assets while avoiding accusations of profiling?

Between 1989 and 1991 the FBI reassessed its strategies in defending national security, now no longer defined as the containment of communism and the prevention of nuclear war. As the FBI sets forth in its history

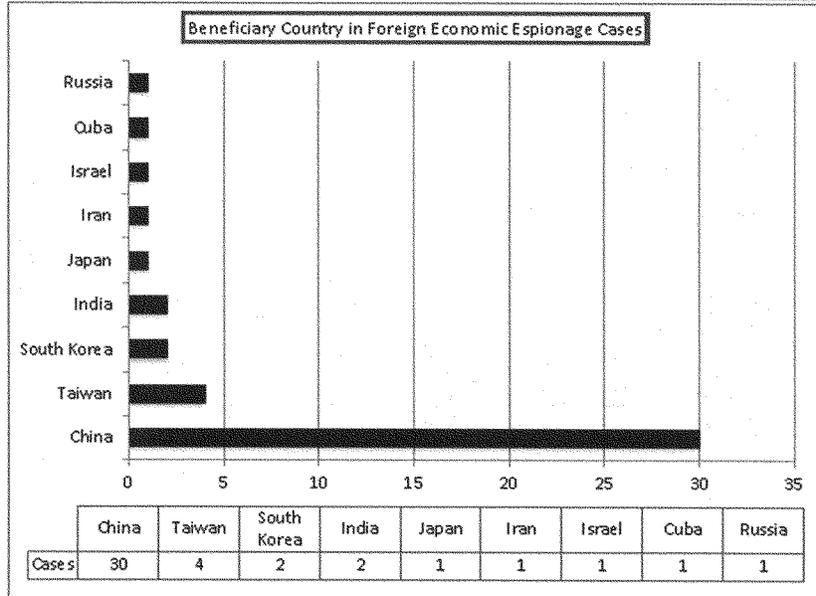
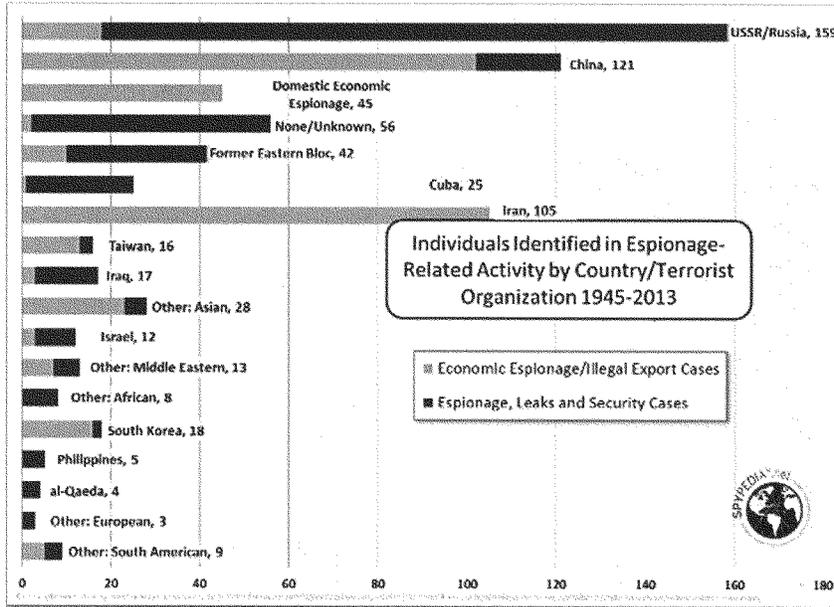
“By creating the National Security Threat List (NSTL), which was approved by the attorney general in 1991, it changed its approach from defending against hostile intelligence agencies to protecting U.S. information and technologies. It thus identified all countries—not just hostile intelligence services—that pose a continuing and serious intelligence threat to the United States. It also defined expanded threat issues, including the proliferation of chemical, biological, and nuclear weapons; the loss of critical technologies; and the improper collection of trade secrets and proprietary information.”

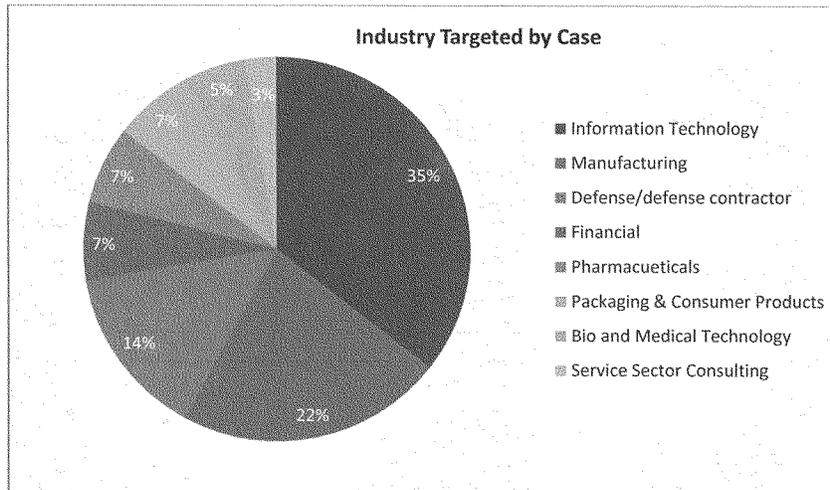
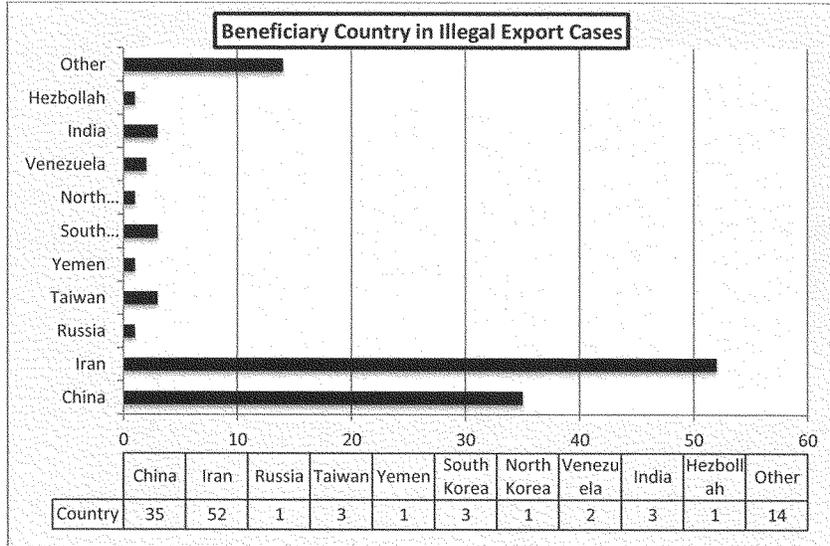
The FBI's foreign counterintelligence mission is set out in a strategy known as the National Security Threat List (NSTL). The NSTL combines two elements:

- First is the Issues Threat List -- a list of eight categories of activity that are a national security concern regardless of what foreign power or entity engages in them.
- Second is the Country Threat List -- a classified list of foreign powers that pose a strategic intelligence threat to U.S. security interests. The activities of these countries are so hostile, or of such concern, that counterintelligence or counterterrorism investigations are warranted to precisely describe the nature and scope of the activities as well as to counter specific identified activities.

Accordingly, the national counterintelligence strategy has already addressed the essence of this question. The DOJ and FBI require evidence of aggressive intelligence collection against the USA before a country can be placed on the NSTL Country Threat List. Responding to this collection threat is not driven by profiling but by facts.

As of June 2013 the number of espionage, economic espionage and technology diversion cases directed against the USA that have led to legal indictments are set forth in the charts below which included 159 USSR/Russian, 121 PRC, and 105 Iran. The majority of the PRC cases are in the private sector, and all of the Iranian cases are private sector economic espionage or technology diversion cases.





- 4) Do you have any recommendation on what steps or academic institutions and labs can take to defend from attacks directed specifically at our cyber infrastructure and can we share or apply those suggestions to American business and government agencies which are constantly bombarded by cyber-attack from foreign nationalists?

A significant number of successful cyber-attacks are made possible by two realities. Betrayers on the inside of our companies and institutions are stealing information technology to support external cyber-attacks. Thirty-five percent (35%) of all the corporate economic espionage cases involving theft of information technology is by insider betrayers many of whom are foreign nationals working within the companies. This reality is a call for enhanced security to protect this type of information and evaluating the policies of hiring foreign nationals for this type of specialized technology regardless of how gifted or competent they may be. You would not allow foreign nationals to work on classified national projects and this policy should be extended to our information technology, academic, labs and business sectors. Failure to monitor access and use of information on sensitive servers by employees (especially foreign national employees) has allowed betrayers to access servers to steal information while the employee was illegally working for a competitor or in their home country. The PRC has gained access to US based servers unnoticed using this method while offering employment in China to Chinese nationals employed in the USA while visiting the PRC.

- 5) The classification system is an important tool to keep truly sensitive information safe and secure. But over classification can jeopardize national security by preventing federal agencies from sharing information internally, with other agencies or with non-government organizations. How can we prevent over classification and ensure that classifiers comply with existing criteria for classifying documents?

This is an age old question and has repeatedly surfaced for years when government entities review US security policies and procedures. Since the September 11, 2001 terrorist attack a new culture of sharing classified information has been adopted by the entire federal government and pushed by both the Bush and Obama administrations. There are few examples of government agencies failure to share information because the information was incorrectly over classified. There have been judgment calls made not to share essential information but that was driven by an agency's cultural difference not by over classification. In addition to a new culture of "push information out" with the executive branch a new culture of "push the classification down" has also been adopted. Neither of these cultural shifts has resulted in creating a mandate to classify less. Within the bureaucracy it is easier for an employee to be criticized or disciplined for not classifying information than deciding to classified information. Thus a culture of when in doubt classify exists in all agencies and at all levels. This was true 20 and 30 years ago and remains true today. You can predict that in the future a major espionage case like Robert Hanssen (FBI spy), Aldridge Ames (CIA spy) or John Walker (Navy spy) will surface and the response will be why that betrayer had access to so much information. The push down and push out culture will surface again and calls will again be made to change the culture.

The espionage law does not address classified information. It states that "protected" national security information transferred to a foreign entity with intent to harm the US or aide that foreign entity is prosecutable espionage. The classification system is established by the President under his constitutional power of conducting foreign affairs and can be changed with a new executive order. In simple terms it is an established procedure to protect national security and a way of informing individuals with legal access to the information that this information needs to be protected. It is no more less than a coded way of alerting people that this information is special.