ENFORCEMENT OF FEDERAL ESPIONAGE LAWS

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

JANUARY 29, 2008

Serial No. 110–133

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE
40–456 PDF WASHINGTON : 2008

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 THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SÁNCHEZ, California
STEVE COHEN, Tennessee
HANK JOHNSON, Georgia
BETTY SUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota
LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

PERRY APELBAUM, *Staff Director and Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

ROBERT C. "BOBBY" SCOTT, Virginia, *Chairman*

MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
JERROLD NADLER, New York
HANK JOHNSON, Georgia
ANTHONY D. WEINER, New York
SHEILA JACKSON LEE, Texas
ARTUR DAVIS, Alabama
TAMMY BALDWIN, Wisconsin
BETTY SUTTON, Ohio
LOUIE GOHMERT, Texas
J. RANDY FORBES, Virginia
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California

BOBBY VASSAR, *Chief Counsel*
MICHAEL VOLKOV, *Minority Counsel*

CONTENTS

JANUARY 29, 2008

ENFORCEMENT OF FEDERAL ESPIONAGE LAWS

TUESDAY, JANUARY 29, 2008

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:06 p.m., in room 2237, Rayburn House Office Building, the Honorable Robert C. "Bobby" Scott (Chairman of the Subcommittee) presiding.

Present: Representatives Scott, Sutton, Forbes, Gohmert and Coble.

Staff Present: Bobby Vassar, Subcommittee Chief Counsel; Ameer Gopalani, Majority Counsel; Mario Dispenza (Fellow), ATF Detailee; Veronica Eligan, Majority Professional Staff Member; Kimani Little, Minority Counsel; and Kelsey Whitlock, Minority Staff Assistant.

Mr. SCOTT. I would like to welcome my colleagues to the first hearing of the Subcommittee on Crime, Terrorism, and Homeland Security for the second session of the 110th Congress.

I would also like to thank former Ranking Member Forbes for his initiative and foresight in helping to put this hearing together. Because of his initiative, he is going to be serving today as the Ranking Member *pro tem* at the request of the gentleman from Texas, Mr. Gohmert.

The topic of today's hearing extends back to the 106th Congress, when espionage was one of the most crucial concerns of that time, as the Cox Committee had released its findings on U.S. technology transfers to China. I was on that select Committee, which found that China had acquired classified information on the most advanced U.S. thermonuclear weapons, giving them design information—significant design information.

The report noted that information on the United States nuclear weapons was obtained through espionage, a rigorous review of unclassified technical and academic publications, and extensive interactions with United States scientists and Department of Energy laboratories. We found that much of this information was obtained due to lack of adequate safeguards and lack of security in our laboratories and inadequate controls of technology transfers, in addition to espionage.

The Cox Committee report has enormous relevance today, as individuals here in the United States continue to export technology

and secrets abroad. Today's technology targeting differs from classic Cold War era spying, which pitted American Cold War intelligence agents against their KGB counterparts and their surrogates. Along with using intelligence professionals, foreign countries now seek to capitalize on some of the thousands of foreign engineers, researchers, scientists, and students who fill key positions in United States industry and academia.

One of the most prevalent forms of espionage in the United States is economic espionage, which is prohibited under the Economic Espionage Act of 1996. That Act prohibits the theft of trade secrets in which the perpetrator acts intending or knowing that the offense will benefit a foreign government.

A number of countries have mounted aggressive economic espionage campaigns here that vacuum up advanced United States technology secrets from defense and civilian companies alike. The rationale is that if you can steal something rather than figure it out yourself you save years and gain a real advantage.

The Department of Justice has had some success in fighting this type of espionage. I look forward to hearing their testimony today.

But it would be a gross mistake to believe that the espionage problem lies only with China. This is an international problem.

In sum, we need to make sure that we are doing everything we can to strengthen the Nation's national security. We want to make sure that we are not in a situation where our own government's lax security, indifference and incompetence results in damage to our national security. During the time of the Cox report, the loss of much of the nuclear weapons information to China was an embarrassment and an incredibly important loss.

So we look forward to hearing from our witnesses today to see how we can improve the situation; and there are going to be, obviously, many things that we can do, many of which will be under the jurisdiction of the Committee on Foreign Affairs, some in Intelligence, some Armed Services, some Commerce and maybe Education. Our focus is what we can do on the Judiciary Committee.

With that said, I now recognize my colleague from Virginia, the former Ranking Member of the Subcommittee, the gentleman from Virginia, Mr. Forbes.

Mr. FORBES. Thank you, Mr. Chairman; and, Mr. Chairman, with your permission, I would like to put my statement in the record. But I would like to just say a couple of opening statements.

First of all, I want to personally thank you for holding this hearing, and your leadership in this matter. And I want to echo what you said, and that is that our desire is to try to see how we can improve the situation. It is not designed to be a finger-pointing expedition. It is designed to say how can we come together, bring individuals and Congress together so that we can help protect the United States of America.

I also want to thank my good friend from Texas, Congressman Gohmert, who is the Ranking Member of this Subcommittee, for his leadership and for allowing me to participate in this capacity today.

And, to our witnesses, we particularly thank you for taking your time, your expertise and energy to be here with us. There are so many people that work in this area and do great jobs. We have the FBI, DOD, Homeland Security, Justice, U.S.-China Economic and

Security Review Commission. All of them do wonderful work, and we just appreciate what you are doing.

The one thing I would just encourage our witnesses at some point in time, whether it is in your presentation or your answers today, is if you could just kind of address also what you think the scope of this problem is. You know, if we try to fight today's wars with yesterday's strategies, we lose. If we try to deal with espionage today the way we did deal with it yesterday, sometimes we are not successful. So we would love for you to kind of give us an idea, your opinion from your experience what the scope of the problem is.

And then the other thing is, just kind of for lack of being able to articulate it any other way, when you go to bed at night and you think about some of these issues, what is it that keeps you awake? What is the thing that you worry about that we need to be worried about? Because if you are worrying about it, we probably need to be worrying about it, too.

The third thing is, what do you think the government is doing right today? But, also, what do you think they are doing wrong in terms of dealing with some of these problems?

And the final thing is what the Chairman alluded to: How can we improve? What is the direction we need to go so that we are protecting the United States and making it a safer place for our citizens?

With that, Mr. Chairman, I yield back, and once again thank you personally for holding this hearing today.

Mr. SCOTT. Thank you very much.

[The prepared statement of Mr. Forbes follows:]

PREPARED STATEMENT OF THE HONORABLE J. RANDY FORBES, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA, AND MEMBER, SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

I would first like to thank Chairman Scott for scheduling this hearing and Ranking Member Gohmert for his cooperation and interest. I would also like to thank the witnesses for being here today. I look forward to your testimony.

As the former Ranking Member of this Subcommittee and the Chairman of the Congressional China Caucus, I look forward to hearing the witnesses discuss the methods by which espionage is conducted in the U.S., the role of the various departments and agencies in the U.S. Counterintelligence Community in identifying, investigating and prosecuting cases, and the adequacy of current federal espionage and export control laws. Furthermore, through this hearing and the classified briefing we just heard, the Subcommittee should gain a better understanding of the extent to which Chinese espionage and cyber-attacks threaten the security of the United States and what legislation and resources may be useful to aid law enforcement activities in this area.

Chinese military doctrine considers computer network operations as a force multiplier in the event of a confrontation with the United States or any other potential adversary. We know that Chinese cyber-warfare units are attacking computer systems in the United States today. In 2006, there were several attacks on U.S. government sites traced back to the People's Republic of China. In fact, the Department of Defense confirmed a cyber-attack on the offices of Defense Secretary Robert Gates in June of 2007.

The Attorney General has testified before this Committee that China represents the number one espionage threat to the United States. It is estimated that there are between 2,000–3,000 Chinese front companies operating in the U.S. to gather secret or proprietary information. Foreign intelligence operations gather sensitive information through legal and illegal means, such as: business solicitations; circumvention of export controls; and university research and product development; attendance at seminars and conventions; and acquisition of American companies.

Furthermore, in testimony before the House Judiciary Committee on September 18, 2007, Mike McConnell, the Director of National Intelligence, stated that "China and Russia's foreign intelligence services are among the most aggressive in collecting against sensitive and protected U.S. systems, facilities and development projects, and their efforts are approaching Cold War levels." The most recent Annual Report to Congress on Foreign Economic Collection and Industrial Espionage *(published August 2006)* states that "the Counterintelligence Community is unanimous in the view that this illegal outflow of technology imposed huge costs on the United States."

While our enemies have been developing new intelligence and techniques to spy against American interests, our criminal laws have not been changed to adapt to the new threat. Criminal penalties are negligible and criminal statutes are archaic and in need of reform. That is why Judiciary Committee Ranking Member Smith and I have introduced the "Supporting Prosecutions of international Espionage Schemes Act of 2007" or "SPIES" Act.

The SPIES Act:

(1) reforms existing espionage laws to respond to criticisms by courts and commentators concerning the outdated statutes and the need for reform; (2) increases criminal penalties for espionage crimes;

(3) moves criminal prohibitions from title 22 and The Atomic Energy Act to the criminal code;

(4) expands coverage of espionage laws to terrorist organizations not just foreign nations;

(5) increases penalties for violations of the Arms Export Control Act and the Export Administration Act of 1979; and

(6) improves coordination among the Justice Department, DHS, State and Commerce on enforcement of export controls.

The recent recalls and safety concerns with products imported from China, including pet food, toothpaste, and toys, should remind us that the United States is ultimately responsible for protecting its citizens from any and all threats. In light of China's expansive military modernization and its tremendous economic growth, we cannot afford to ignore the threat that espionage and cyber-attacks directed by China towards the United States poses to our national security.

I yield back the balance of my time.

Mr. SCOTT. Mr. Gohmert, do you have a statement?

Mr. GOHMERT. Not other than to say how much I appreciate Chairman Scott having this hearing. It obviously is such an important issue. And for the continued diligence of my friend, former Ranking Member Randy Forbes, for pushing the matter forward. Thanks so much, Chairman.

Mr. SCOTT. Thank you.

Mr. Coble.

Mr. COBLE. Mr. Chairman, very briefly, I, too, thank you for holding the hearing. Mr. Chairman and Ranking Member, I know of no issue any more significant than the one we will discuss here today. Yield back.

Mr. SCOTT. Thank you.

We have a distinguished panel of witnesses here to help us consider the important issues currently before us.

Our first witness will be J. Patrick Rowan, who is the Principal Deputy Assistant Attorney General in the National Security Division of the Department of Justice. As the Principal Deputy, Mr. Rowan leads the NSD's prosecutors in the counterterrorism and counterespionage sections and focuses on the Department's efforts to disrupt terrorists and other national security threats through investigation and prosecution. Prior to his current position, he served as the Associate Deputy Attorney General and assisted in the management of national security functions at the Department of Justice.

Next witness will be David G. Major. He is the President of the Centre for Counterintelligence and Security Studies. Mr. Major is a retired senior FBI supervisory Special Agent who served in the Bureau from 1970 to 1994, where he specialized in working, supervising, and managing counterintelligence and counterterrorism cases. During the Reagan administration, he was appointed the first Director of Counterintelligence and Intelligence Programs to the National Security Council staff and briefed and advised President Reagan on counterintelligence policy and operations matters from 1985 to 1987.

And our last witness will be Dr. Larry Wortzel, Chairman of the U.S.-China Economic and Security Review Commission. He is a leading authority on China and Asia, with more than 37 years of experience in intelligence, foreign policy, and national security matters. He had a distinguished 32-year military career, retiring as an Army colonel in 1999. He has previously served as an Army attache to the U.S. Embassy in China and has written numerous books on China's military.

Each of the witnesses' written statements will be made part of the record in it's entirety. We would ask that the witnesses summarize your testimony in 5 minutes or less. And to help you stay within that time there is a timing device which will start green. With 1 minute left, it will turn to yellow and finally red when the 5 minutes are up. So we would ask you to stay within 5 minutes.

We will begin with Mr. Rowan.

TESTIMONY OF THE HONORABLE J. PATRICK ROWAN, PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION, UNITED STATES DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. ROWAN. Thank you, Mr. Chairman.

Chairman Scott, Ranking Member Gohmert, Congressman Forbes, Congressman Coble, thank you for having me here today.

I am testifying on behalf of the Department of Justice and, specifically, the National Security Division, which, as you well know, was created by the Congress as part of the Patriot Act reauthorization in 2006; and I, at the outset, want to thank you for your role in creating the new division.

As you know, the National Security Division is comprised of the counterterrorism and counterespionage prosecutors in the Department of Justice, as well as our Office of Intelligence and Policy Review attorneys. Those are the attorneys that work on FISA matters. We are the Department's liaison to the intelligence community, as well as being the prosecutors who are supervising or actually engaging in the terrorism and counterespionage prosecutions across the country. It is my pleasure to appear before you today to discuss the Department's enforcement of Federal espionage laws.

As you know, the clandestine intelligence collection activities of foreign nations include not only traditional Cold War-style efforts to obtain military secrets but increasingly sophisticated operations to obtain trade secrets, intellectual property, and technologies controlled for export for national security reasons. Accordingly, these activities and others implicate a wide array of Federal criminal statutes. But no matter what form of espionage is being used or

which statutes are implicated, there is one common denominator: Our national security is always at stake.

The Federal Criminal Code gives the government a variety of different tools to prosecute different types of espionage, and I thought I would just briefly summarize for you sort of the different sets of statutes that we are primarily using to attack this problem.

The first set of statutes are those for the traditional espionage involving national defense information or classified information. The primary two statutes in that area are 18 U.S.C. Section 793 and section 794.

18 U.S.C. Section 793 generally prohibits anyone from willfully communicating information relating to the national defense to any person not entitled to receive it. The term "information relating to the national defense" has been defined by case law to mean information that is closely held by the government, usually through proof that the information was classified. Section 794 is more narrow. It criminalizes the communication of national defense information to foreign governments.

Now, in addition to those two statutes, which are the traditional statutes, obviously, that most people think about when they talk about espionage, we have a number in different parts of the Code that we often use. In particular, in instances where we identify individuals or groups that are engaged in activities in the U.S. on behalf of a foreign government, but we cannot actually show that they are collecting classified or national defense information, we use 18 U.S.C. Section 951, which prohibits anyone from acting in the U.S. as an agent of a foreign government without first notifying the Attorney General.

18 U.S.C. Section 951 has been used successfully a great deal recently, including to prosecute individuals who had been affiliated with the Iraqi Intelligence Service under Saddam Hussein and who had been sent to the United States to conduct activities on behalf of Hussein's government.

One example of this is Khaled Abdul-Latif Dumeisi, who was convicted in Chicago of violating section 951 for his activities spying on Iraqi dissidents in the United States for Saddam Hussein. We have had access to some Iraqi intelligence files and have used those files to help us in making these cases. Dumeisi is a good example of how we can use 18 U.S.C. Section 951 against somebody who wasn't involved in collecting classified information but was nonetheless working in this country on behalf of a foreign government.

Of great concern recently is the substantial and growing national security threat posed by illegal foreign acquisition of restricted U.S. military technology. The National Security Division launched a new initiative this past October to bolster our enforcement efforts on that front.

In a general sense, the technology at the heart of the initiative includes U.S. military items, dual-use equipment, and other technical expertise or know-how, some of which have applications in the weapons of mass destruction. These materials are generally restricted and may not be exported without a license.

China and Iran pose particular U.S. export control concerns; and recent prosecutions have highlighted illegal exports of stealth mis-

sile technology, military aircraft components, naval warship data, night vision equipment, and other restricted technology destined for those countries.

In one recent case, a former engineer with a U.S. Navy contractor in California was convicted by a jury in May of 2007 for exporting sensitive defense technology to China. The individual, Chi Mak, had been given lists from co-conspirators in China that requested U.S. naval research related to nuclear submarines and other information. Mak gathered technical data about the Navy's current and future warship technology and conspired to export this data to China. His four codefendants also pled guilty. He is scheduled to be sentenced in March of this year.

The export control laws are the third set of laws that we use as a critical tool for addressing national security threats. These include the Arms Export Control Act, which prohibits the export of defense articles and services without first obtaining a license from the Department of State; the Export Administration Act, which has lapsed but is currently enforced through IEEPA. That prohibits the export of certain dual-use technology without first obtaining a license from the Department of Commerce. And then the International Emergency Economic Powers Act, or IEEPA, which authorizes restrictions or prohibitions on transactions involving particular countries such as Iran.

The National Security Division in October of last year launched an export enforcement initiative to ensure that prosecutors around the country have the training, tools, and support from other agencies that they need to bring cases under these statutes. This effort involves expanding our training of prosecutors around the country, the creation of multi-agency counterproliferation task forces in U.S. attorneys' offices around the country, the designation of an 18-year veteran Federal prosecutor to be a coordinator, our National Export Control Coordinator, to ensure that we are working hard and moving this effort forward across the country, and then greater coordination between our prosecutors, export licensing officials at the State Department and the Commerce Department and the enforcement agencies, to include the Department of Homeland Security, the FBI, the Commerce Department and DCIS.

That effort has already begun to pay off. We are very happy with the success we have had so far, although we believe there are more cases to be had out there, and we expect to see additional prosecutions in the near future.

I appreciate the opportunity to appear before you today and testify on behalf of the Department of Justice regarding enforcement of Federal espionage laws. We look forward to working with the Committee to improve our enforcement capabilities in this area.

Mr. SCOTT. Thank you, Mr. Rowan.

[The prepared statement of Mr. Rowan follows:]

PREPARED STATEMENT OF THE HONORABLE J. PATRICK ROWAN

Statement of
J. Patrick Rowan
Deputy Assistant Attorney General
National Security Division
U.S. Department of Justice

Before the
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United States House of Representatives

Concerning
"Enforcement of Federal Espionage Laws"

January 29, 2008

Chairman Scott, Ranking Member Gohmert, and members of the Subcommittee:

It is my pleasure to appear before you today to discuss the National Security Division's enforcement of Federal espionage laws. As you know, the clandestine intelligence collection activities of foreign nations include not only traditional Cold War style efforts to obtain military secrets, but, increasingly, sophisticated operations to obtain trade secrets, intellectual property, and technologies controlled for export for national security reasons. Accordingly, these activities and others implicate a wide array of Federal criminal statutes. But no matter what form of espionage is being used, or which statutes are implicated, there is one common denominator: our national security is always at stake.

Unfortunately, espionage did not end with the end of the Cold War, and in fact, we have investigated espionage activities relating to more countries now than in the past. Recent cases have involved efforts to get information or technology to countries like China, Cuba, the Philippines, and South Korea, for example:

- Noshir Gowadia is a former design engineer from Northrop Corporation who has been charged in an 18-count superseding indictment in the District of Hawaii with espionage and export violations stemming from substantial defense related services he allegedly performed for the Peoples Republic of China. This includes his illegal sale of U.S. military technology secrets to China. Gowadia allegedly agreed to design, and later designed, a "low observable" cruise missile exhaust system nozzle capable of rendering the missile less susceptible to detection and interception. The case is set for trial in the District of Hawaii in October 2008.

- Carlos Alvarez, a psychology professor at Florida International University, admitted in a guilty plea in 2006 that he had worked for nearly 30 years as a

covert intelligence agent on behalf of the Cuban government. He was sentenced to 60 months imprisonment.

- Leandro Aragoncillo, an FBI analyst, pleaded guilty in 2006 to espionage and other charges, admitting that he took and transferred classified information, including national defense documents, to senior political and government officials of the Republic of the Philippines. He was sentenced to 10 years imprisonment.

- Robert C. Kim, a South Korean native who had become an American citizen and had worked as a computer specialist for the U.S. Navy, pleaded guilty in 1996 to conspiracy to commit espionage for South Korea. He admitted to having given secret Pentagon and State Department documents to a South Korean naval attache at the South Korean Embassy in Washington. He was sentenced to 9 years imprisonment.

- Brian Patrick Regan, a former Master Sergeant in the United States Air Force who worked as a signal specialist at the National Reconnaissance Office, was convicted in 2003 of offering to sell U.S. intelligence secrets to China and Iraq. He was sentenced to life imprisonment without parole.

Of great concern recently is the substantial and growing national security threat posed by illegal foreign acquisition of restricted U.S. military technology. On January 22nd the President issued an Export Control Directive to ensure that U.S. defense trade policies and practices better support the National Security Strategy of the United States. One key element of this White House directed effort is the establishment of a multi-agency working group to support the Department's export enforcement investigations. The National Security Division will play a key role in this effort. Strict enforcement of our country's export control laws is a critical tool in stemming this somewhat non-traditional espionage-related threat. The National Security Division launched a new initiative this past October to bolster our enforcement efforts on that front. I'll discuss that initiative in greater detail shortly, but in a general sense, the technology at the heart of the initiative includes U.S. military items, dual-use equipment, and other technical expertise or know-how, some of which have applications in Weapons of Mass Destruction. These materials are generally restricted and may not be exported without a license. China and Iran pose particular U.S. export control concerns, and recent prosecutions have highlighted illegal exports of stealth missile technology, military aircraft components, Naval warship data, night vision equipment, and other restricted technology destined for those countries. In one recent case, a former engineer with a U.S. Navy contractor was convicted by a jury in May 2007 of exporting sensitive defense technology to China. The individual, Chi Mak, had been given lists from co-conspirators in China that requested U.S. Naval research related to nuclear submarines and other information. Mak gathered technical data about the Navy's current and future warship technology and conspired to export this data to China. His four co-defendants all pleaded guilty. Mak is scheduled to be sentenced in March of this year.

In the National Security Division, we have a section aptly named the Counterespionage Section, where lawyers work on espionage and espionage-related enforcement efforts everyday.

The Counterespionage lawyers are in constant communication with the foreign counterintelligence personnel in the FBI and, indeed, the entire intelligence community. They evaluate pending counterintelligence investigations for potential prosecution and are highly experienced in dealing with sensitive sources and methods. Since espionage prosecutions often involve the possibility that classified information may be disclosed publicly, either as part of the defendant's defense or as part of the prosecution's case-in-chief, the lawyers in the Counterespionage Section also work extensively with the Classified Information Procedures Act, known as CIPA, which provides uniform procedures for dealing with classified information in open criminal proceedings.

As mentioned above, the Federal criminal code gives the government a variety of different tools to prosecute different types of espionage. Lawyers in the Counterespionage Section of the National Security Division deal with all of the espionage and espionage-related statutes regularly. The primary statutes concerning espionage include 18 U.S.C. § 793 and § 794. Generally speaking, Section 793 prohibits anyone from willfully communicating information relating to the national defense to any person not entitled to receive it. The term "information relating to the national defense" has been defined by case law to mean information that is closely held by the government, usually through proof that the information was classified. Section 793 also criminalizes the willful retention of national defense information, conspiracies to communicate or retain national defense information, and the negligent removal of national defense information from its proper place of custody. The maximum penalty under Section 793 is ten years imprisonment. Section 794 is more narrow than Section 793 because it criminalizes the communication of national defense information to foreign governments, where the communication of information is made with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation. Violations of Section 794 can result in life imprisonment, or, if certain criteria are met, the death penalty can be imposed.

In addition to Sections 793 and 794, there are other relevant statutes that provide felony offenses for more particularized conduct. For example, 18 U.S.C. § 798 prohibits disclosing classified information concerning communications intelligence; 18 U.S.C. § 1030(a) criminalizes obtaining of classified information by accessing a computer without authorization; 50 U.S.C. § 421 prohibits the disclosure of the identity of a United States covert agent; 50 U.S.C. § 783 makes it unlawful for any government employee to disclose classified information to a foreign government and for any agent of a foreign government to receive classified information from a government employee; and 18 U.S.C. § 951 prohibits anyone from acting in the United States as an agent of a foreign government without first notifying the Attorney General. All of these offenses generally carry a maximum penalty of ten years imprisonment. In addition to these felonies, Title 18 U.S.C. § 1924 provides a misdemeanor offense for retaining classified information.

One point of note with respect to one of the statutes mentioned above,18 U.S.C. § 951, is that it has been used successfully in recent cases to prosecute individuals who had been affiliated with the Iraqi Intelligence Service under Saddam Hussein, and who had been sent to the United States to conduct activities on behalf of Hussein's government. One example of this is Khaled

Abdel-Latif Dumeisi, who was convicted in the Northern District of Illinois of violating § 951 for his activities spying on Iraqi dissidents in the United States for Saddam Hussein. On March 31, 2004, Dumeisi was sentenced to 46 months imprisonment.

The Dumeisi case also provides just one example of how electronic surveillance under the Foreign Intelligence Surveillance Act ("FISA") is a key tool in combating intelligence collection activities by foreign governments here in the United States. Dumeisi had previously been the subject of an FBI intelligence investigation for several years, which had included electronic surveillance under FISA . In 2003, when FBI agents were able to share that information from their investigation with prosecutors, the prosecutors were able to use it to build the case against Dumeisi. Electronic surveillance and physical searches under FISA are indispensable in espionage cases, which by their very nature usually involve clandestine activities that are difficult to detect.

As discussed earlier, export control laws are also critical tools for addressing the national security threat posed by sensitive U.S. technology getting into the wrong hands. These include:

- the Arms Export Control Act, 22 U.S.C. §§ 2751-2799, which prohibits the export of defense articles and services without first obtaining a license from the Department of State, and carries a penalty of up to 10 years imprisonment;

- the Export Administration Act of 1979, 50 U.S.C. App. §§ 2401-2420, which has lapsed and is therefore currently enforced through IEEPA, prohibits the export of certain "dual-use" goods and technology without first obtaining a license from the Department of Commerce, and carries a penalty of up to 5 or 10 years imprisonment depending on the violation;

- the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1706, which authorizes restrictions or prohibitions on transactions (including comprehensive trade embargoes) involving particular countries, such as Iran, or specified individuals or entities, such as terrorists, and carries a penalty of up to 20 years imprisonment; and

- the Trading with the Enemy Act of 1917, 50 U.S.C. §§ App. 1-6, 7-39, 41-44, which authorizes prohibitions on nearly all transactions involving Cuba and on participation in transfers of certain strategic goods to North Korea, and carries a penalty of up to 10 years imprisonment.

The National Security Division's export enforcement initiative I described earlier is a major effort to ensure that prosecutors around the country have the training, tools, and support from other agencies that they need to bring cases under these statutes. The Department of Justice and the National Security Division are fully committed to the success of this important initiative. Steven Pelak, an 18-year veteran Federal prosecutor, has been appointed as the National Export Control Coordinator responsible for leading the efforts under the initiative. Mr. Pelak is creating multi-agency counter-proliferation task forces in U.S. Attorney's offices around

the country. These task forces are taking many of the concepts used in combating terrorism – namely, prevention, cooperation and coordination – and applying them to the efforts to prevent the illegal export of sensitive U.S. technology. The FBI, the Departments of State and Commerce, the Department of Homeland Security, the Defense Criminal Investigative Service, and others are all part of this effort. Training for prosecutors is of course an essential aspect of the initiative, since export prosecutions are by their very nature complex: they involve intricate laws, sensitive international issues, agencies with different authorities, and, often, classified information. Earlier this month, Mr. Pelak held a training symposium on export control for over 30 prosecutors from around the country at the National Advocacy Center. From the strides Mr. Pelak has already made in carrying out the National Security Division's export control initiative, we are confident that it will significantly bolster our country's export enforcement efforts.

Before I conclude I would be remiss if I did not point out that our efforts to disrupt clandestine intelligence activities of every form – from traditional spying to illegal exports of technology – have been enhanced by the establishment of the National Security Division within the Department of Justice, which brought the Counterespionage Section, the Counterterrorism Section, and the Office of Intelligence and Policy Review together in one Division. This Division was created by the Congress as part of the reauthorization of the Patriot Act in 2006, and we believe that it has already begun to pay dividends.

Thank you for the opportunity to appear before you and testify on the National Security Division's enforcement of Federal espionage laws. We look forward to working with the Committee to improve our enforcement capabilities in this important area.

Mr. SCOTT. Mr. Major.

TESTIMONY OF DAVID G. MAJOR, PRESIDENT, THE CENTRE FOR COUNTERINTELLIGENCE AND SECURITY STUDIES, ALEXANDRIA, VA

Mr. MAJOR. Mr. Scott, Mr. Forbes, Members of the Subcommittee, I already submitted my testimony. I would like to make some general comments, if I could, about this, the bigger issue of espionage.

It is one of these things that we have had a tough time in our Nation to put our hands around and taking serious; and so we have periods historically of being very serious about it, other times kind of ignoring the reality of this problem. When you ask the question what is the scope of the problem, that is another example of difficulty we have had as a Nation trying to come to grips with it.

The CI Centre was established in 1997 as a center of excellence, and we primarily do counterintelligence training for people in the intelligence community. And we do about 8,000 people a year and trained about 67,000 people in the last 11 years. These people are from everywhere within the intelligence community.

And one of the things we learned is that our understanding of both this discipline and counterintelligence is about as deep as a puddle. Most people do not have a deep, rich understanding of this, nor where it came from, nor how to address it. One of the greatest things you can do to try to address it is truly educate people, and this is one of the great challenges we continue to have.

Counterintelligence historically in the United States is a problem that we have tried to buy on the cheap. We spend a lot of money on other issues, but counterintelligence is one that we have never made—we vary in our ability to make a serious commitment to make sure our personnel are fully trained and fully capable of dealing with the problem.

If I go back historically and give you a sense of the problem, there are 28 nations that have been involved in legally identified espionage prosecutions in the United States. These are members of NATO. These are adversaries. These are friends. When you look at how big the problem is, since 1945 to today there are 247 people who have been prosecuted or charged with espionage in the United States. In the 21st century, since 2000 to this time, there have been 37 people who have been charged with espionage or espionage-related crimes; and that includes 794, 793, and 951, which was actually passed in 1938, the agent of foreign powers legislation, which is very effective today and one of the techniques that has been used to try to deal with the reality of this issue.

Forty-nine percent of the 247 people who have been charged with espionage since 1945 are, in fact, Russian cases. So we learned our craft of counterintelligence by dealing with the KGB and the GRU, who have run operations against us. One hundred and twenty-one cases actually of the 247 are Russian-based cases.

In 1992, the FBI changed its whole strategy of dealing with counterintelligence and went to an issue called national security threat list. The result of that is they begin to look at many other countries and have publicly stated there are now over a hundred nations that use part of their GNP to target the United States to conduct intel-

ligence operations leading toward what we would call espionage in the generic context. And the result of that is we have identified many nations, including allies, who in fact run intelligence operations against the United States because it is in their national interests to do so. This is not an adversarial issue. This is one that a nation finds in their interest to collect against us, and they do.

It was interesting that the law that we talked about today actually is traced back to 1917, when the espionage law of 1917 was passed as a result of a terrorist attack against the United States. The terrorist attack was Black Tom Island. It took place in New York City. Over $20 million worth of damage, three people killed, and it really mimicked the 9/11, except, instead of killing people, it had a huge explosion, destroyed a huge munitionary dump, and the result was we had no law to respond to that.

Actually, there were calls to court-martial citizens in the United States. Cooler heads prevailed, and they passed the espionage law of 1917, which is, just as 793 and 794, a very restrictive law. You have to do two things: to prove that national defense, which means military defense of the United States, has to be proven. That has to be proven in a courtroom. And, number two, based on the Heine espionage case of 1940, it has to be protected information. It doesn't have to be classified information, but if it meets the standard of being defense information and it is protected, it also meets the standard of being classified.

The result is that it is a very narrow, restricted aspect of espionage that you have to prove in a courtroom to get what I call "big" espionage, 793. That is why these other statutes such as 951 and 794, preparatory acts, are also important to do that.

But when you say, how do we deal with this problem and what is the scope of this, we struggle with that issue, how big is the problem. I remember when I was in the government and we started a study on that and we realized there were many nations that found it in their interests to do it.

As you certainly know, in other hearings, the Bureau is always having hundreds of actual investigative cases but to actually bring it to prosecution is very difficult to do; and there are very few cases where you find somebody actually conducting espionage. So almost always these are conspiratorial cases. It is a very rare case that has actually been caught with someone committing espionage. Bob Hanssen is an exception, when they allowed him to actually commit espionage to do it.

So it is a very complex issue and one that we have had a tough time sometimes putting our arms around.

To show you the breadth of the scope of the problem, remember during World War II when the Soviet Union was our ally and between 1942 and 1945 there were over 250 Americans who were agents of the foreign power in that one period. In fact, if you could break that down to the year 1944, every element of the U.S. Government was penetrated by our ally, the Soviet Union; and the only exceptions to that were the FBI and ONI, which the FBI made up with with the Hanssen case in the modern era. But that shows when we did not have an effective counterintelligence program in World War II that didn't mean that you won't be targeted.

But the one thing I have learned in my 38 years of studying this is you can never stop it, like you can't stop any crime, but you can address it. And you need to address it through education, you need to address it by taking it serious. And sometimes we have and sometimes we have not as a Nation.

Mr. SCOTT. Thank you very much.

[The prepared statement of Mr. Major follows:]

PREPARED STATEMENT OF THE DAVID G. MAJOR

Prepared Statement of David G. Major, President
The Centre for Counterintelligence and Security Studies (CI Centre)
Before the US House of Representatives, Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
"Enforcement of Federal Espionage Laws" Hearing
January 29, 2008

Mr. Chairman, Ranking Member and members of the Subcommittee, thank you for the opportunity to testify today at your hearing on Enforcement of Federal Espionage Laws.

The Centre for Counterintelligence and Security Studies (CI Centre) was established eleven years ago in 1997 as a centre of excellence to support the nation's counterintelligence and counterterrorism mission and concerns. We have only one mission: to provide the best possible education on the strategic and tactical importance of counterintelligence, counterterrorism and security. We offer 40 different courses on these topics ranging from one to five days.

We have a staff of 37 personnel with 25 professors and guest speakers, all of whom are intelligence experts retired from the FBI, CIA, Department of Defense, State Department, Canadian RCMP, Cuban DI and Russian KGB. One of our Professors is John Martin, the retired Chief of the Internal Security Section at the US Justice Department, responsible of overseeing the successful prosecution of 76 people for espionage. Another professor is Oleg Kalugin, a retired KGB Major General who was chief of foreign counterintelligence in the KGB and oversaw and conducted espionage operations against the USA before he immigrated to the US. We also employ recognized intelligence historians and authors to support our programs.

The majority of our students are current employees of the US national security community. We train approximately 8,000 students per year and have provided training to approximately 67,500 students in the past 11 years.

Since 1945 to this year, there have been 247 individuals arrested in the United States for espionage or espionage related crimes. The Soviet Union and Russia have been involved in 49% of these cases (121) and as such the US Counterintelligence Community has learned CI tradecraft through the lens of studying KGB and GRU operations around the world.

In February 1992, the FBI changed its strategy approach to counterintelligence and began to investigate any country that was targeting the US with their intelligence

collection methodologies. The result was the FBI uncovered over 100 countries collecting against the US with 28 different countries publically identified as involved in running espionage operations against the USA. This list includes both political allies and adversaries. This is an average of four cases per year, with 10 cases in 2006 and 10 cases in 2005.

Since the end of the Cold War, there have been 78 individuals arrested for espionage or espionage-related crimes and since the 21st century began, there have been 37 individuals arrested in the US as agents of foreign powers. This is a clear indicator that espionage continues to be a very real threat to US National Security. Note the many different countries spying against America since the year 2000 in the following chart:

Agents of Foreign Powers Arrested in the United States in the 21st Century

NAME(S)	ORGANIZATION	SPYING FOR or ATTEMPTED or ALLEDGED SPYING FOR	YEAR OF ARREST
FAGET, Mariano	US Immigration & Naturalization Service (INS)	Cuba	2000
SMITH, Timothy S.	Navy civilian	Stole classified document	2000
TROFIMOFF, George	Retired US Army Colonel and GS-15 civilian	USSR/Russia	2000
HANSSEN, Robert	FBI	USSR/Russia	2001
MONTES, Ana	Defense Intelligence Agency	Cuba	2001
REGAN, Brian	US Air Force detailed to NRO; contractor for TRW	Iraq, China, Libya	2001
DUMEISI, Khaled Abdel	Civilian	Iraq	2003
LEUNG, Katrina	FBI Asset; Civilian	People's Republic of China	2003
SMITH, James J.	FBI	People's Republic of China	2003
YAI, John Joungwoong	Civilian	North Korea	2003
LATCHIN, Sami	Civilian; gate agent at Chicago O'Hare airport	Iraq	2004
ANDERSON, Ryan	US Army National Guard	Al Qaeda	2004
KEYSER, Donald	Department of State	Taiwan	2004
LINDAUER, Susan	Civilian/Journalist/Hill staffer	Iraq	2004
AQUINO, Michael	Former Philippine security official living in US	Philippines	2005
ARAGONCILLO, Leandro	US Marine on security detail to White House; FBI	Philippines	2005
FRANKLIN, Larry	Department of Defense	Israel	2005
ROSEN, Steven J.	Civilian, AIPAC	Israel	2005
WEISSMAN, Keith	Civilian, AIPAC	Israel	2005
GOWADIA, Noshir	Self; formerly Northrop	People's Republic of China, 7 other countries	2005
MAK, Chi	L-3/Paragon (DOD Contractor)	People's Republic of China	2005
MAK, Tai	Chinese TV Network	People's Republic of China	2005
MAK, Rebecca Laiwah Chiu	Civilian	People's Republic of China	2005
MAK, Flora	Civilian	People's Republic of China	2005
MAK, Fuk-Heung Li	Civilian	People's Republic of China	2006
MAK, Billy	Civilian	People's Republic of China	2006
ALVAREZ, Carlos	Civilian; University Professor	Cuba	2006
ALVAREZ, Elsa	Civilian; University Staff	Cuba	2006
MONTAPERTO, Ronald	DIA	People's Republic of China	2006
ALI, Amen Ahmed	Civilian	Yemen	2006
OMER, Ibrahim	Contractor	Yemen	2006
AL-RAHIMI, Mohamed	Civilian	Yemen	2006
BENJAMIN, William Shaoul	Civilian	Iraq	2006
WEINMANN, Ariel	US Navy	Russia	2006
HALL, Paul (Hassan Abujihaad)	US Navy	Al Qaeda/Islamic Jihadists	2007
SHEMAMI, Najib	Civilian	Iraq	2007
AL-AWADI, Ghazi	Civilian	Iraq	2007

The Federal Espionage Laws codified in Title 18 Section 793 and 794 US Code along with other related crimes date back to the terrorist attack of 1916 on Black Tom Island carried out by the German IIIb intelligence service. This event had such an impact on the nation that proposals were made to court martial civilians since there were no viable laws to deal with espionage at the time. The result was the 1917 Espionage Law of which codified a very restricted definition of the crime of Espionage. As you know espionage has four elements:

- Unauthorized transmittal
- of national defense information
- to a foreign power or agent
- with the intent to harm the US or aid that foreign power

As a result of a German espionage case in the early 1940s, that was appealed, and precedence was established that the national defense security information transmitted in an espionage case had to be protected information. Accordingly, it is essential to prove in an espionage prosecution that the information affected the military defense of the United States and was protected information not in the public domain at the time it was transmitted.

There was a period in America's history that we did not prosecute spies because we did not have the tools or the political will to do so. But as the evolution of espionage prosecutions evolved, the US began to develop the right tools and investigative expertise to successfully prosecute spies. To illustrate this, from 1967 to 1974 there were no federal prosecutions for espionage and only ten individuals convicted in military court for espionage-related activity. Training on how to conduct espionage cases was an essential tool which led to this new success. The FBI began to formally train its Special Agents in counterintelligence in November 1973 and how to conduct an espionage interview in early 1980s.

I'd like to focus on one of our courses which is applicable to today's hearing on espionage laws, entitled "Counterespionage Today: Complexities and Decisions." I'll describe what we teach attendees of the course and then I welcome your questions on the topics you would like more information on.

"Counterespionage Today" is an intensive five-day course which was designed because many US Intelligence Community personnel have no understanding of how difficult it is to fashion and build a successful prosecutable espionage case. Espionage cases are the "Super Bowl" of prosecutions. If you make a mistake during the process of investigating someone who turns out to be a real spy, it's going to be in the front page of the newspapers. This course introduces attendees to the complexities and the

decision making processes associated with investigating and prosecuting espionage cases in the United States in the 21st Century.

The course examines the basis for and establishment of viable predications for the initiation of espionage investigations. It also explores the inherent conflicts between the need for internal vigilance by US Counterintelligence and the civil rights of personnel within US sovereign territory.

The nation is in a time period where US Counterintelligence is required to address the US expanding war on terrorism and address the reality of post cold war espionage by US allies. During this period, the nation is debating and examining the tools, policies and laws that are and should be made available to the US Government to meet these challenges. This course identifies these issues and explains the evolution of key legal and policy decisions associated with prosecuting espionage cases today, emanating from both adversaries and allies.

"Counterespionage Today" provides all members of the US national security community a deeper understanding of the status of counterespionage today and their individual roles in the protection of our nation's most vital secrets, plans and programs.

We begin by ensuring the attendees know how a US person is targeted, recruited and handled by foreign intelligence services and collectors. We then provide a deep understanding of the various federal laws which aid the counterespionage investigator, including the Espionage Act of 1917, the CIPA Law which protects classified information and sources in prosecutions, and the Foreign Intelligence Surveillance Act (FISA). This includes a discussion of the North Vietnamese espionage case code named "Magic Dragon" which resulted in the passage of the FISA statute. Attendees see an espionage case from the legal prosecutions standpoint so they are able to conduct their investigations and security duties with the due process always in mind and therefore ensure the case is successfully prosecuted in court.

The course examines several espionage cases from the legal and investigative perspective, including the Judy Coplon case, the Mariano Faget case, the Albert Sombolay case, the Ryan Anderson Case ,the Clyde Conrad case, an overview of spies in State Department, and for 1 ½ days, the Robert Hanssen case. Attendees learn from the mistakes and successes made during the counterespionage investigations of these cases and what happens if you do it wrong.

Challenges are reviewed such the predications of investigations, arrest or neutralizing of the subject, obtaining evidence legally, multi-agency involvement in a case including when foreign CI services must become involved, investigating in an overseas

environment, deciding when to brief the chain of command, the role of political leadership which gets involved in a case, and the result of lack of training in counterintelligence at all levels which can result in missteps allowing a subject to go free.

Attendee feedback on the course has been very positive and shows the impact the course had on them and their jobs:

- "This course has given me ideas for how to pursue current counterespionage cases and has reinvigorated my zeal for doing counterespionage work."
- "This course provided a solid foundation from which to conduct espionage/CI investigations. Understanding actual cases allows an investigator to recognize anomalies and patterns that may be exhibited by subjects in an ongoing investigation as well as reasons to initiate an investigation."
- "Really forced me to think of varied counterespionage issues that I had never thought of."
- "I can and will use all that I've learned as I do my job. I always leave here with a different/greater perspective of counterintelligence and counterespionage."
- "Wow! I am new to counterespionage/counterintelligence and the course is my first exposure to the intelligence world. I took an immense amount of information away from this course. I look forward to becoming a student of my new profession."
- "The course was very eye-opening in that I learned new ways to spot espionage and I got an internal look at how investigations can be glitched up and still be successful. I plan to keep my eyes wide open and to become a 'professional student' of counterintelligence."
- "The course clearly articulated a complex problem and the dynamic environment of counterintelligence. It demonstrated the decision making process when you have limited information and showed how *not* deciding can be harmful. It exposed the differences between CI investigations and criminal investigations. It had a great exercise of the conflict and balance between civil liberties and state sovereignty."

I welcome your questions.

Mr. SCOTT. Dr. Wortzel.

TESTIMONY OF LARRY M. WORTZEL, Ph.D., CHAIRMAN, UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, WASHINGTON, DC

Mr. WORTZEL. Chairman Scott, Mr. Forbes, Members of the Subcommittee, thank you for inviting me to address this hearing on Federal espionage laws.

I will address the issues raised about Chinese espionage in the convention of the U.S.-China Economic Security Review Commission's annual report to Congress. I also have some 25 years of personal experience as an intelligence officer, so I will add a few of my own views.

The Commission concluded that China's defense industry is producing new generations of weapon platforms with impressive speed and quality. We believe that some of these advancements are due to a very effective manner in which Chinese companies are integrating commercial technologies into military systems. However, we note that espionage provides Chinese companies an added source of new technology, and it leaps them ahead, while saving them time and money.

My own view is that it is often very difficult to distinguish between what we define as espionage related to the national security under the espionage act and economic espionage, or the theft of proprietary information and trade secrets. And even if we can make the distinction, we may not be able to prove it in court.

For American companies, however, for the defense of the United States, the impact of this espionage is the same. It robs companies of the cost of their research. It gives technology to China's armed forces. It undermines the security of American military personnel and our national security.

Mr. Rowan mentioned the Chi Mak case in California. I want to talk a little bit more about it, because I think it is a great example of the difficulties our intelligence and law enforcement agencies face in pursuing these cases.

You have five members of a California family who are charged with conspiring to export defense articles to China, which was a violation of the Arms Export Control Act. Yet they focused on corporate proprietary information and embargoed defense technology as related to propulsion weapons and electrical systems in U.S. warships.

Agents of the FBI and the Naval Criminal Investigative Service found direct tasking documents with Chi Mak, and it looks like the espionage effort was directed by a Chinese academic out at Zhongshan University in Guangzhou. The information that was going back to China was embedded in computer disks, CDs that seemed to be television broadcasts with pictures and sound.

It has a lot of the earmarks of traditional espionage tradecraft and state-directed espionage, but I will tell you that this practice is so widespread in China that it could have been an effort by some Chinese company, through a research institute at a university, to leap themselves ahead, or the university itself to market itself and get money from the government.

The Gowadia case out in Hawaii, where stealth missile technology was acquired by the Chinese, is another very important case.

Now we also noted in our report our concerns that computer or cyber penetrations of U.S. companies and government agencies represents another spectrum of the serious espionage threat from China that our Nation faces. Our Commission concluded that, as Chinese espionage against the U.S. military and American business continues to outpace the overwhelmed U.S. counterintelligence community, critical American secrets and proprietary technologies are being transferred to the People's Liberation Army and Chinese state-owned companies.

Now, among our recommendations were that Congress address the adequacy of funding for export control enforcement and counterintelligence efforts, that you also look at the adequacy of and the funding for specific military intelligence and homeland security programs that protect critical American computer networks. We felt that the Director of National Intelligence should run a capabilities assessment and identify specific strategies for addressing U.S. weaknesses.

In closing, Mr. Chairman, the law enforcement and the intelligence communities have been effective in meeting this challenge; and I think we all have to remember that there are a lot of other national security issues, like terrorism, that they face. So they have done a good job.

I should also note for you that our Commission prepared a classified report to the Congress. It is available to read in the Office of Senate Security.

I want to thank you again for the opportunity to appear before you and for holding this hearing, and I would be happy to respond to any questions you may have.

Mr. SCOTT. Thank you very much.

[The prepared statement of Mr. Wortzel follows:]

PREPARED STATEMENT OF LARRY M. WORTZEL

Chairman Conyers, Chairman Scott, Ranking Members Smith and Forbes, and Members of the Subcommittee, thank you for inviting me to address this hearing on the enforcement of federal espionage laws.

My name is Larry Wortzel and I presently serve as the chairman of the twelve member, bipartisan, bicameral United States-China Economic and Security Review Commission. As you know, the Commission members are appointed by the Congressional leadership. I have served on the Commission since 2001 and I also served as chairman for the 2006 reporting year. By mutual agreement, the twelve commissioners elect a chairman and a vice-chairman each year, rotating the positions between a Republican and a Democratic appointee. I was appointed to the Commission by Speaker Hastert.

I will address the issues raised about espionage by China by the Commission in its yearly report to the Congress, issued in November 2007. I also bring some personal experience on the matter to bear. During my 32 year military career, I spent 25 years in military intelligence with the United States Army. This experience involved gathering signals intelligence and human source foreign intelligence, primarily about China. For about five years I was a military attaché at the American Embassy in China. I was also trained as a counterintelligence officer and spent a number of years conducting counterintelligence investigations and developing programs to protect emerging defense technology from foreign espionage.

I should note that when I refer to the Report to Congress by the US-China Economic and Security Review Commission, I will summarize the views and consensus of the commissioners, as outlined in the report. You could have read that yourselves,

however; therefore, given my background and experience, I will also express my own views. When I do, I will identify them as such.

The Commission concluded in 2007 that China's defense industry is producing new generations of weapon platforms with impressive speed and quality. We believe that some of these advancements are due to the highly effective manner in which Chinese defense companies are integrating commercial technologies into military systems. However, we note that espionage provides Chinese companies an added source of new technology without the necessity of investing time or money to perform research. After a year of hearings, research, and classified briefings from agencies of the U.S. intelligence community, the Commission concluded that China's espionage activities are the single greatest threat to U.S. technology and strain the U.S. counterintelligence establishment. This illicit activity significantly contributes to China's military modernization and acquisition of new capabilities.

There is a long record in China going back over two centuries of sending government directed missions overseas to buy or shamelessly steal the best civil and military technology available, reverse engineer it, and build an industrial complex that supports the growth of China as a commercial and military power. Indeed, my own view is that today it is often difficult to distinguish between what we define as espionage related to the national defense under the Espionage Act (18 USC 792–9), and economic espionage or the theft of proprietary information and trade secrets covered by the Economic Espionage Act (18 USC 1831–9). Indeed, for American companies and for the national defense of the United States, the impact of espionage can be the same, robbing U.S. companies of the costs of their research, giving technology with military application to China's armed forces, and undermining the security of American military personnel and our nation.

One reason that China's industries have been so effective at espionage is the centralized approach they have taken. In March 1986, the PRC launched a national high technology research and development program with the specific goal of benefiting China's long-term high technology development. This centralized program is known as the "863 Program" (or Torch Program). China's state council allocates money to acquire and develop biotechnology, space technology, information technology, laser technology, automation technology, energy technology and advanced materials.[1]

Our Commission recognizes that part of China's defense industrial base modernization strategy is to acquire advanced foreign equipment and technologies. While in some cases Chinese planners have chosen to purchase entire weapon systems directly, some Chinese and Western analysts do not see this as beneficial for the long-term modernization of China's defense industry.[2] Direct purchases are generally used as a temporary measure to fill critical gaps that China's indigenous defense companies are unable to fill. Some items purchased from foreign companies are dual-use components—those that can be used in military as well as civilian applications such as computers, semiconductors, software, telecommunications devices, and integrated circuits.[3]

The report also notes that partnerships forged between foreign companies and Chinese civilian companies also offer Chinese defense industries access to advanced foreign technologies. The nature of the regulatory and commercial environment in China places enormous pressure on foreign companies, including those of the United States, to transfer technology to Chinese companies as a part of doing business in China and to remain competitive globally.[4] Foreign companies are willing to provide not only technology but capital and manufacturing expertise in order to secure market access in China.[5] Indeed, many are, in fact, creating R&D facilities in China.

Still, we note in the report that access to restricted foreign technology is obtained by China through industrial espionage. We have heard from experts who advise us that China operates an aggressive clandestine effort to acquire additional tech-

---

[1] The 863 name comes from the month and the year that the program was proposed.

[2] U.S.-China Economic and Security Review Commission, *Hearing on China's Proliferation and the Impact of Trade Policy on Defense Industries in the United States and China,* testimony of James Mulvenon, July 13, 2007. Mulvenon sees this as a "scathing indictment of the failures of the PRC defense-industrial base to fulfill its long-standing promises to the PLA."

[3] U.S. Department of Defense, *Annual Report to Congress on the Military Power of the People's Republic of China,* (Washington, DC: July 2007), p. 29.

[4] Medeiros et al., *A New Direction for China's Defense Industry,* (RAND Corporation, Santa Monica, CA: 2005) p. 241.

[5] Medeiros et al., *A New Direction for China's Defense Industry,* (RAND Corporation, Santa Monica, CA: 2005) p. 241.

nologies.[6] In recent years, this has become such a problem in the United States that U.S. Immigration and Customs Enforcement officials have rated China's espionage and industrial theft activities as the leading threat to the security of U.S. technology.[7]

Our law enforcement agencies, our intelligence community, and our corporate security professionals must contend with seven or more Chinese state-controlled intelligence and security services that can gather information for the state-owned industrial sector inside China or overseas. These include

- the Ministry of State Security and its local or regional state security bureaus;
- the Public Security Bureau;
- the intelligence department of the People's Liberation Army (PLA), or Second Department;
- the PLA's Third, or Electronic Warfare Department;
- a PLA Fourth Department that focuses on information warfare;
- trained technical collectors from the General Armaments Department and the General Logistics Department of the PLA;
- the technical intelligence collectors of the military industrial sector and the Commission of Science Technology and Industry for National Defense;
- and the Communist Party Liaison Department r PLA General Political Department.

Frankly, I don't know if the Chinese government is funneling information or technology back into some of the now-privatized companies that engage in industrial or economic espionage in China. Also, I believe that the various science and research parks that operate under municipal control actively seek out new technology and so do the newer companies that operate outside government control in China.

The nature of the Chinese state also compounds the security problems. China is a totalitarian state, even if today there is far greater economic freedom there. The legal system in China still responds to the direction of the Chinese Communist Party. Thus the state has great power to compel citizens to cooperate and a far reach to retaliate if citizens in China refuse to do the state's bidding. I think that reach is decreasing as the economy offers more opportunity for Chinese citizens and there are more opportunities for private employment there. But it is still difficult to avoid the pressure that a one-party, Leninist-structured state can bring to bear on its citizens.

I would like to discuss one case brought to trial by the United States Attorney's office in the Central District of California as an example of how hard it is to know for certain whether our intelligence and law enforcement agencies face economic espionage or more traditional espionage designed to injure the national security of the United States. In the Chi Mak case, in California, five members of a southern California family were charged with acting as agents of the People's Republic of China in 2005 and in 2006 with conspiring with each other to export United States defense articles to the People's Republic of China (a violation of the Arms Export Control Act, 22 USC 2778). This technology theft ring focused on acquiring corporate proprietary information and embargoed defense technology related to the propulsion, weapons and electrical systems of U.S. warships. Going through Chi's residence, agents of the Federal Bureau of Investigation and the Naval Criminal Investigative Service found instructions tasking Chi to join "more professional associations and participate in more seminars with 'special subject matters' and to compile special conference materials on disk."[8]

Chi Mak was a support engineer at L-3 Communications working on navy quiet drive propulsion technology. In two documents instructing Chi, one hand printed in Chinese and the other machine printed, the military technologies Chi was to seek involved:

- Space-based electromagnetic intercept systems
- Space-launched magnetic levitation platforms
- Electromagnetic gun or artillery systems
- Submarine torpedoes

---

[6] U.S.-China Economic and Security Review Commission, *Hearing on China's Military Modernization and Its Impact on the United States and the Asia-Pacific,* testimony of William Schneider, Jr., March 29, 2007.

[7] U.S. Department of Defense, *Annual Report to Congress on the Military Power of the People's Republic of China,* (Washington, DC: July 2007), p. 29.

[8] CI Centre, http://www.cicentre.com/Documents/DOC__Chi__Mak.html

- Electromagnetic launch systems
- Aircraft carrier electronic systems
- Water jet propulsion
- Ship submarine propulsion
- Power system configuration technology
- Weapons system modularization
- Technologies to defend against nuclear attack
- Shipboard electromagnetic motor systems
- Shipboard internal and external communications systems
- Information on the next generation of US destroyers (DDX).

The espionage effort appears to have been directed by a Chinese academic at a research institute for Southeast Asian affairs at Zhongshan University in Guangzhou, China. The Chi family encrypted the information it was passing back to China into a computer disk that appeared to contain television and sound broadcasts. It was literally embedded in the other data in encrypted form.

This effort has all of the earmarks of professional espionage tradecraft and state-directed espionage, with sophisticated control and sophisticated clandestine communications means. The government university in Guangzhou could have been cover for a state-directed espionage effort. However, Chi Mak and his alleged co-conspirators could just as well have been part of a sophisticated economic espionage operation run out of a university research institute.

Mr. Chairman, I could go on for a long time. The Computer and Intellectual Property Section of the Department of Justice web site lists 33 cases of alleged violations of the Economic Espionage Act between 2000 and 2005, many of which seem to have involved China. Immigration and Customs Enforcement has a large number of arrests and indictments, as does the FBI. In the US-China Economic and Security Review Commission's annual report, we note that "Mr. Joel Brenner, the top counterintelligence official in the Office of the Director of National Intelligence, has noted that of the 140 foreign intelligence agencies continuously attempting to penetrate U.S. agencies, China is the most aggressive.[9] The FBI stepped up counterintelligence efforts against Chinese intelligence operations in the United States in July 2007, because of what FBI Director Robert Mueller called a "substantial concern" about those operations."[10] An American engineer living in Hawaii was indicted for working with a Chinese government agent and supplying stealth missile technology over the course of six visits to China. A Defense Intelligence Agency employee was convicted on lesser charges but was indicted for leaking classified information to China's military intelligence service and hoarding classified U.S. documents in his home.

We also noted in our report concerns that computer, or "cyber" penetrations of United States companies and government agencies represent another spectrum of the espionage threat from China with which our law enforcement and intelligence community must contend. In England, the head of one of Britain's intelligence agencies warned of cyber-penetrations by China. The attacks allegedly targeted Royal Dutch Shell and Rolls Royce. So China's espionage activities target advanced technology, economic data and military secrets in many countries.

Our Commission unanimously concluded that "as Chinese espionage against the U.S. military and American businesses continues to outpace the overwhelmed U.S. counterintelligence community, critical American secrets and proprietary technologies are being transferred to the PLA and Chinese state-owned companies."[11] In response to this espionage, the Commission recommended the following steps:

- In order to slow or stop the outflow of protected U.S. technologies and manufacturing expertise to China, the Commission recommends that Congress as-

[9] Jeff Bliss, "China's Spying Overwhelms U.S. Counterintelligence," *Bloomberg,* April 2, 2007.
[10] Bill Gertz, "FBI calls Chinese espionage 'substantial,'" *The Washington Times,* July 27, 2007.
[11] U.S. Department of Justice Press Release, "Former Chinese National Convicted of Economic Espionage to Benefit China Navy Research Center," August 2, 2007; U.S. Department of Justice Press Release, "Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit China: First Conviction in the Country for Foreign Economic Espionage," December 14, 2006; Jeff Bliss, "China's Spying Overwhelms U.S. Counterintelligence," *Bloomberg,* April 2, 2007; Amy Argetsinger, "Spy Case Dismissed for Misconduct," *Washington Post,* January 7, 2005; Bill Gertz, "FBI calls Chinese espionage 'substantial,'" *The Washington Times,* July 27, 2007; U.S. Department of Justice Press Release, "Guilty Plea in Trade Secrets Case," February 15, 2007; U.S. Department of Justice Press Release, "Fifth Family Member Pleads Guilty in Scheme to Export U.S. Defense Articles to China," June 6, 2007.

sess the adequacy of and, if needed, provide additional funding for U.S. export control enforcement and counterintelligence efforts, specifically those tasked with detecting and preventing illicit technology transfers to China and Chinese state-sponsored industrial espionage operations.

- The Commission recommends that Congress assess the adequacy of and, if needed, provide additional funding for military, intelligence, and homeland security programs that monitor and protect critical American computer networks and sensitive information, specifically those tasked with protecting networks from damage caused by cyber attacks.
- The Commission recommends that Congress instruct the director of national intelligence to conduct a full assessment of U.S. intelligence capabilities vis-á-vis the military of the People's Republic of China, and identify strategies for addressing any U.S. weaknesses that may be discovered as part of the assessment
- The Commission recommends that Congress urge the Administration to engage China in a military dialogue on its actions and programs in cyber and space warfare to include threat reduction mechanisms, the laws of warfare, and specifically how the laws of warfare apply to the cyber and space domains.

In closing Mr. Chairman, I want to thank you and the Members of the subcommittee for holding this hearing. The law enforcement and intelligence communities have been effective in meeting this challenge, even if overwhelmed by other national security challenges. In my view, the Economic Espionage Act is a very helpful tool, especially since the elements of proof of the Espionage Acts are often more difficult to prove, as I tried to illustrate in my description of the Chi Mak case. In other indictments the law enforcement community has relied on the Arms Export Control Act and the Export Administration Act.

I should also note that the United States-China Economic and Security Review Commission also prepared a classified report to Congress. This report is available for Members and their appropriately cleared staff to read in the Office of Senate Security.

Thank you again for the opportunity to appear before you and I would be happy to respond to any questions you may have.

Mr. SCOTT. We will now ask you to respond to questions. I will first recognize myself for 5 minutes.

As I indicated in my opening statement, this is the Judiciary Committee. There are many other Committees that would have jurisdiction on some of the solutions to the problem.

But let me just begin by looking at the acquisition of technology. Mr. Rowan, you mentioned the dual-use technology that may be an issue and that that statute had lapsed. Did I understand that right?

Mr. ROWAN. That's right.

Mr. SCOTT. What problems occur by virtue of the fact that that statute has lapsed?

Mr. ROWAN. Well, some of the penalties that would otherwise be available under the Export Administration Act are not available.

What has occurred is that the regulations that were imposed and support the Export Administration Act have been adopted through IEEPA. So we are able to reach a lot of the conduct, but we have to reach it through IEEPA, and so the sort of statutory regimen that exists under the Export Administration Act is not available to us. And that means that penalties and everything else that sort of was thought up to directly target dual-use technologies is not available to us.

We, you know, obviously prosecuted cases using that statutory or regulatory fix, but it is a statute that we would—we could certainly use more effectively if it was in effect.

Mr. SCOTT. In terms of commercial activities and export controls, do we need to do anything from the Judiciary Committee point of view with universities or businesses in terms of protecting the information?

Mr. ROWAN. Well, Mr. Chairman, we certainly would be pleased to work with you on any proposals in that area, but I don't come to you today with any proposals for how this Committee might be able to target that specific problem.

Mr. SCOTT. Mr. Major or Dr. Wortzel, do you have any recommendations as to what this Committee could do to protect our military and commercial secrets?

Mr. WORTZEL. Mr. Chairman, dual-use technologies are a real problem; and it has been very difficult to get the Export Administration Act passed through Congress. I would encourage you to work on that.

I think that the problem of universities and contracts and research laboratories is a huge one; and it is very difficult to know, when a contract is given to a university or corporation, who some of the subresearchers are, who is actually working on it. That is an area I think that would be useful to address.

A second area that we have explored with the Commission is the problem that many corporations are beginning to move both manufacturing and research overseas into other countries, specifically into China. In order to get in there, they increasingly have to provide access to manufacturing techniques and proprietary information; and they lose that.

So those are areas I believe that we could tighten up and that with the help of the Justice Department there might be improved legislation.

Mr. MAJOR. A couple general comments.

In front of you we have provided you a chart, if you have a chance to look at it, that will illustrate the extent of this problem. Because when you open it up you realize what we try to make is a list of every single espionage case publicly identified in the last hundred years, starting from 1900 to 2006. And if you look at that and you realize how long this problem has been with us and how we deal with it.

Now, to respond to this problem, it is interesting that it is not—first of all, the most difficult thing in an espionage case is finding out who might be the betrayer, who might be the agent; and you either have to target who the collector is and the methodologies they use or you have to try to find other mechanisms to say who that person is. That is the first, very important step.

If you notice when you look at that chart, you can see that by year we have listed both congressional actions over the years, FBI reorganizations, CIA reorganizations, world events, and then the number of individual cases by year. And the one thing it does indicate, this problem is not going to go away, no matter how much we want it not to be the case.

China represents a very unique problem because China doesn't spy the way God intended people to spy. You do not have an intelligence officer filling a dead drop. China's location for espionage is a couch in Beijing. It is very difficult to fashion or put a case together like this.

And one of the other issues you have is exactly as you just heard, that when Americans are trying to expand their business, as they go to China, since they do not have copyright laws to the same degree in Asia that you do in the United States, is you say to many corporations color it gone, and soon you will be talking about your competitor that is there. So the real issue is it is an education one to make sure people know what they are walking into and how they are doing it.

One of the things that has worked in an espionage case is that you find out who the agent is, but then what do you do about it? And a good example is on the list I gave you. Of the 37 people arrested for espionage this year, one was a North Korean espionage agent by the name of John Yai, who they investigated for some time, but they couldn't prove he had passed national defense information. So it turned out to be that 951 was the only way that you could go after him, which is the agent of a foreign power.

And if someone examined beefing that law up, expanding the amount of penalties you would have for that particular crime—because it is the one thing that you can prove. I can prove that you are an agent, but I can't prove that you have actually passed national defense information, which really limits the kind of response you can have to deal with it.

Mr. SCOTT. If you are an agent of a foreign government, is that a crime?

Mr. MAJOR. If you are an unregistered agent of a foreign power. Whether you are a lobbyist or a spy, if you come to the United States, you have a requirement to go down to the Department of Justice and say I am a trained spy. And if you don't do that, you are in violation of the law.

Well, most spies don't do that. Lobbyists do it, lawyers do, but spies don't. And it is like spitting on the sidewalk for espionage. There is the 1-year sentence and then you can get a bigger one. And it is the one that has been used against the Iraqis recently. We went through a period of time that we didn't want to use that, but now in the last—this century we have been using it more. But, still, the penalty for it is significantly lower than it is for what you and I would define as big espionage.

Mr. SCOTT. Mr. Forbes.

Mr. FORBES. Thank you, Mr. Chairman; and thank you, witnesses, for being here.

This is both impressive and frightening as we look at this. But there is one major sea change that has taken place throughout all of this that isn't totally reflected on here. And that is, based on testimony that we have received in this Committee before, would any of you disagree that today the number one espionage threat in the United States is China?

Mr. MAJOR. I am not sure it is the largest. I would expand on that that the size of the Soviet intelligence service, which has always been large, one of the ways to look at it is it is coming back, the size of their intelligence service—the Soviet Union in 1991, when it collapsed, had about 296 million people, and the size of their intelligence service was 496,000 people. Now we roll the camera forward to 2007, there are about 141 million people in Russia today, which is half the population, and their intelligence service

is down to about 400,000 people. Which means they have 400,000 people as members of their intelligence service, which means the population is half the size, but the size of the intelligence service is 20 percent less, which means there are more intelligence officers per capita than during the Cold War. And there are as many Russian intelligence officers in the United States as there were Soviet intelligence officers during the Cold War, and we have had a tougher problem coming to deal with that.

If you read policy papers today, it is interesting that we seem to have an awakening to China. You can look at it, a number of strategic papers that are made, some of the cases made, I think there is a slow awakening, starting with the Cox report, which is a very significant one, to wake up to China.

For a long time, we did not recognize China, because China is a very difficult country to penetrate their intelligence collection. Because they don't do it the way you are supposed to do it. They don't use intelligence services to do it. So it was for a very long time we were not very successful against China. And I would suggest in the last 7 to 8 years we are getting better at dealing with China.

During the same time, the Soviet Union is coming back, and we now find that there are as many intelligence officers here. And, as you well know, FSB has the authority, that is the counterintelligence service, to go around the world and conduct assassinations. It is like Stalinism is back.

The one other thing you do see happening, which is a real transition in espionage, is the marriage between Islamic terrorism and espionage, like the case with Yemen and other cases that we are seeing that you didn't used to see any connection between terrorism and espionage. You do like the China case, Paul Hall, who in fact was providing classified information from the Navy, but he was doing it to support terrorism. And I think that is a new trend that we are seeing in just the last few years here in the United States.

Mr. FORBES. Mr. Wortzel?

Mr. WORTZEL. Mr. Forbes, one of the unique things about China obviously is the population, 1.3 or 1.4 billion people. But the nature of the state and its ability as a totalitarian Leninist state allows seven or eight intelligence services and technology collection organizations to literally target and train people or compel people during their routine activities of travel and work to gather information.

I doubt that everybody complies that is told by the Chinese Government to do something. There are more opportunities in China today to avoid that repressive state and get another job. But it really does, as a state, have the capability to say you are not traveling unless you go here and you do such and such.

Mr. FORBES. Your Commission concluded or at least indicated that China's espionage and industrial theft activities were a leading threat to the security of U.S. technology. Is that an accurate statement?

Mr. WORTZEL. Yes, sir. That is the unanimous consensus of a bipartisan Commission of 12 people.

Mr. FORBES. And do any of you have any information that we have had any cyber penetrations, as you talk about, or invasions of elected officials in the United States or government officers or American corporate executives by Chinese espionage?

Mr. WORTZEL. Mr. Chairman or Mr. Ranking Member, we would have to address that—it is addressed in our classified report. I can't address that here.

Mr. FORBES. Okay. The other thing I would ask is, we had testimony, I think that there are a number of companies here that are front companies in China or Chinese companies that are doing espionage activities. The question I would ask you is what is the extent of that? If you have any information on that that you can share with us.

And, also, Mr. Rowan, how do we identify those companies? Or do we have a capacity to do it so that we can stop them from those activities? Or is there just no opportunity to do it?

So either of the three of you.

Mr. MAJOR. Well, the first thing you have is to even identify which companies, because the numbers are breathtakingly large, to even look at which companies to be looked at.

As you well know from talking to the counterintelligence community in China, the numbers are so large, how many of the companies there are. And then the point is, what are their activities and how do I investigate them? Are they in fact doing it is the biggest problem.

Because there is no magic bullet to say, well, these five companies are involved in doing it. You make a very good point when you say you don't have to be a front company to do it if the company finds itself, its methodology of collecting, and you are going to have a company that will use that area. It is a problem. It is probably a resource problem more than a law problem.

Mr. FORBES. And my time has expired, so I ask you if you all could submit those for the record for us.

[The information referred to can be found in the Appendix.]

Mr. FORBES. And also, Mr. Wortzel, I would like for you to comment in your written statement, just because my time is out, about the Commission's recommendation that Congress instruct the Director of National Intelligence to conduct a full assessment of this and give us a report back. If you could comment on that.

[The information referred to can be found in the Appendix.]

Mr. FORBES. And I want to stop so we can have the other Members ask their questions before we go to vote.

Mr. SCOTT. Thank you.

Ms. Sutton?

Ms. SUTTON. Thank you, Mr. Chairman. Thank you for having this hearing today. It is an extraordinarily important subject, and I appreciate the distinguished witnesses who have testified.

You know, it is fascinating to hear you talk about sort of the unique nature of the challenge we are dealing with with China. And I think it is crucial that this body, that Congress and our government as a whole get a good grasp of what exactly we are facing. Because, as you say, it is not traditional.

Now, I have more of a bent toward the commercial, you know, the stealing of trade secrets. One of my colleagues recently told me

about a situation in his district where an employee working for a company in his district, an employee who came in, worked for this company, stole trade secrets, fled to England. When it was discovered, the Chinese government brought him out of England, took him back to China and is shielding him from prosecution by the U.S. Now, how common is that?

Mr. WORTZEL. It is pretty common, Ms. Sutton. One of the points I make in my written testimony is that, in 1986, the central leadership of the People's Republic of China and the Communist Party made a decision to create a nationwide program to target about 16 technologies across the world that specifically had dual-use in military applications and send people out to gather these technologies and ensure that as they began to put them into industrial production for state-controlled defense industries that they would at the same time be able to spin them off into civil production. Almost the opposite of what we have done.

They have been very successful at it, and it is not like the program ended. In July of last year, the Second Artillery Corps, the strategic missile forces of the People's Republic of China, ran a national strategy commission, and they brought in the intelligence departments, they brought in the operations departments of the People's Liberation Army, they brought in the Navy and the Air Force and the defense industry, and central at the table was the 863 Program Office of the Division of Science and Technology for National Defense.

So this hasn't gone away. It is centrally orchestrated. I don't think that every person that comes out has a specific task, but I think that they are able to draw on their own ability to monitor people and know who has access and to touch them and get what they can.

Ms. SUTTON. And I guess the question and one of the purposes of this hearing is, what do we do about that? What do we do about dealing with the country that is now shielding this person from prosecution? How do we fight back on this?

Mr. WORTZEL. Well, first of all, I wouldn't look at every Chinese student or worker and think you are dealing with a spy.

Ms. SUTTON. Right.

Mr. WORTZEL. I would be very careful about that. I don't think everybody necessarily complies, and I doubt that everybody is touched. But I think that in these cases it is very important to have a strong counterintelligence and industrial security education program. The Defense Criminal Investigative Service runs one.

At the time I dealt with Mr. Major, the FBI had a very good defensive program out in industry. I have been away from it. I don't know what they are doing today.

But, out in industry, industrial security and corporate security have to be enhanced; and there has to be a partnership between corporations and the government.

Mr. MAJOR. You can't ride in from Washington to solve the problem to say these are the five companies you have to worry about.

Probably one of the greatest assets you have, if you can make a commitment to educate your employees and to educate these corporations, one of the things that the CI Centre does is we are in the education business, and so we do a lot of these kinds of

trainings today. We go into large corporations, and we try to give them a feel exactly of the problem that you are talking about.

One of the things we do also is to try to say how big is this problem? Which was what the Chairman's question was, also. That is in our Web site that we update every single day. We list all of these cases about China on a daily basis. And if you actually study that, you can spend all day just reading them.

Because it is not just an American problem. It is a European problem, also. Because, remember, as I said, China has a copy culture. It is honorable. They don't have copyright laws. It is perfectly acceptable to do that.

So my point is that if you are going to stop the problem, the people being victimized sometimes are the best ones to come forward and say I have a problem with you doing this.

But is it a serious problem? Yes, it is. Is it growing? I would suggest more so than I have seen in a long time for China.

Ms. SUTTON. Yeah. And I would just say it is not really—my concern is perhaps even less in dealing with the individuals than dealing with the country. Okay. And so what kind of leverage do we have to deal with a country who is acting in concert to get every advantage they can gaining this technology? That is just—I know my time is up.

Mr. MAJOR. The one comment that often happens is you find a case like this, you bring it up in the political sense to the leadership of the government, and China's leadership says we don't do that, and then it moves away.

And we have multiple examples, of "we don't do that," "we are not involved with that," and "we never do that." And there is a flat denial, and there is no political price to pay for that.

And that is a much bigger issue to talk about, because there are economic connections with it. But China does not pay any kind of price for finding it to have an open door ability to collect intelligence against us. And their big attitude is, so what? In essence, you can take the next line, so what are you going to do about it? Because we really do not do much about it. So down at the prosecutable individual level we try to deal with it.

Ms. SUTTON. Well, I have a problem with that. Thank you.

Mr. SCOTT. Thank you.

I think we have about 5 minutes for the gentleman from Texas.

Mr. GOHMERT. Okay. Well, I realize our time is very limited, and I need the witnesses to really contemplate this more than 4 or 5 minutes. So what I am going to do is lay my predicate very briefly and then give you the questions and, if it is all right with the Chairman, ask them to submit thoughtful responses in writing back to this Committee.

Because you pointed out—first of all, let me say it has been mentioned they don't have copyright laws like ours. I met with some of their officials who were supposed to enforce their copyright laws. They do have copyright laws. They just don't enforce them. And therein lies a huge problem. And it is actually against their pecuniary interest at this point to enforce them, because they make so doggone much money off of them. And so one of the things is we have got to make it—I think, as Ms. Sutton alluded to, we have

got to get their attention by making it worth their interests to enforce them.

But it was mentioned earlier we need to beef up 951 to allow more penalties, if I understood it. Is 951, that is the section that is applicable?

So here is my question to you. What penalties should we have? As a former judge, it is nice to say we should have different penalties, but there is only one way to get those, and that is if you have different levels of the offense. And if you have different levels of the offense, then you are creating additional burdens of proof for a prosecutor to have to jump over.

So, question one, what penalties should we have?

And then the next question, number two, is what different categories or levels of the crime can we have so that we don't make it unprovable?

And then, number three, since China doesn't do espionage like they are supposed to, how do you prove they are trained intelligence officers and not just a regular person that has been asked to pick up some piece of information?

Because it seems to me that is a real problem for the Chinese espionage, whether it is a student, whether it is a corporate officer or somebody saying we are not training you, but we do need this piece of information, just get it however you can. So that is my third question. How do we get to those people who maybe really aren't trained intelligence officers? Maybe we can't get them through the means you are suggesting. How do we get to them?

And, really, I see that as just follow-up to what Ms. Sutton is saying. How do we get the leverage we need to enforce this stuff?

And I appreciate the chart. That is terribly helpful. As an old history major, I think we can't do very well in the future if we don't know where we have been in the past. But just because espionage has always been and will always be doesn't mean that we throw up our hands and say, well, just get what you want. We have got to make an effort to defend this country.

Mr. SCOTT. Thank you, and I would like to thank the witnesses for their testimony today. As the gentleman from Texas indicated, we have additional questions for our witnesses which we will forward to you and ask that you answer as promptly as you can so the answers can be made part of the record. Without objection, the hearing record will remain open for 1 week for submission of additional materials.

And, again, I would like to thank my colleague from Virginia for his leadership on this issue.

Without objection, the Committee stands adjourned.

[Whereupon, at 2:59 p.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

PREPARED STATEMENT OF THE HONORABLE BETTY SUTTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO, AND MEMBER, SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

REMARKS BY REPRESENTATIVE BETTY SUTTON

JUDICIARY CRIME SUBCOMMITTEE HEARING ON "ENFORCEMENT OF FEDERAL ESPIONAGE LAWS"

TUESDAY, JANUARY, 29TH, 2008
2:00 P.M. RAYBURN 2237

I would like to thank Chairman Scott for calling this hearing today. I would also like to thank my colleagues and our distinguished witnesses who will offer their testimony and recommendations.

The Judiciary Committee has held several hearings this year on the Foreign Intelligence Surveillance Act and addressed how we can best harness our nation's intelligence capabilities to keep us safe while also protecting our citizens' precious civil liberties. I am glad that today we are turning to an equally challenging question—how to protect our nation's government and

businesses from espionage that puts our security and economic prosperity in danger.

We must ensure that our nation's espionage laws and prosecutorial efforts match the seriousness of this issue. It is greatly disturbing to me that in 2007 hackers from the Chinese People's Liberation Army were able to penetrate computer systems in the Pentagon. We have the finest military in the world and must do everything to retain our strategic advantage in protecting our homeland and our allies against those who would seek to do us harm.

I am also concerned that China's record of stealing technology is just one of the many underhanded tactics it has used to support its rapid growth as a commercial and military power. My colleague, Congressman Donnelly from Indiana, knows firsthand the damage these tactics

inflict on American workers. An employee of a company in his district stole trade secrets, skipped town to England, and then was shielded by China when the U.S. sought to prosecute him.

Additionally a manufacturing facility of Avery Dennison Corporation that is located in my home state of Ohio was betrayed by an employee who passed trade secrets to a Taiwanese company. Federal prosecutors estimate that the research and development costs expended to develop the information obtained by the defendants in that case exceeded $50 million.

I look forward to working with my fellow members on this challenging issue, and I look forward to hearing the panel's recommendations.

I look forward to hearing the panel's recommendations and working with my fellow members on this challenging issue that affects our national security and economic prosperity. Thank you.

COMMITTEES:
ARMED SERVICES
SUBCOMMITTEE ON READINESS
SUBCOMMITTEE ON SEAPOWER AND EXPEDITIONARY FORCES

JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY – RANKING MEMBER
SUBCOMMITTEE ON IMMIGRATION, CITIZENSHIP, REFUGEES, BORDER SECURITY, AND INTERNATIONAL LAW

J. Randy Forbes
United States Congress
4th District, Virginia

307 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-6365

425-B SOUTH MAIN STREET
EMPORIA, VA 23847
(434) 634-5575

2903 BOULEVARD, SUITE E
COLONIAL HEIGHTS, VA 23834
(804) 526-4869

505 INDEPENDENCE PARKWAY
LAKE CENTER II – SUITE 104
CHESAPEAKE, VA 23320
(757) 382-0080

October 2, 2007

The Honorable Robert C. Scott
Chairman, Subcommittee on Crime,
Terrorism and Homeland Security
B-370 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Scott:

As we have previously discussed, the issue of espionage and cyber-crime as it relates to China's influence and operations in the United States is of great concern to me. I am requesting that you schedule an oversight hearing of the Subcommittee on Crime, Terrorism and Homeland Security to investigate the extent to which Chinese espionage and cyber-attacks threaten the security of the United States and what legislation may be useful to aid law enforcement activities in this area.

Chinese military doctrine considers computer network operations as a force multiplier in the event of a confrontation with the United States or any other potential adversary. We know that Chinese cyber-warfare units are attacking computer systems in the United States today. In 2006, there were several attacks on U.S. government sites traced back to the People's Republic of China. Most recently, the Department of Defense confirmed a cyber-attack on the offices of Defense Secretary Robert Gates in June of this year.

The Attorney General has testified before this Committee that China represents the number one espionage threat to the United States. It is estimated that there are between 2,000-3,000 Chinese front companies operating in the U.S. to gather secret or proprietary information. Foreign intelligence operations gather sensitive information through legal and illegal means, such as; business solicitations; circumvention of export controls; and university research and product development; attendance at seminars and conventions; and acquisition of American companies.

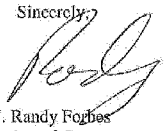
Furthermore, in testimony before the House Judiciary Committee on September 18, 2007, Mike McConnell, the Director of National Intelligence, stated that "China and Russia's foreign intelligence services are among the most aggressive in collecting against sensitive and protected U.S. systems, facilities and development projects, and their efforts are approaching Cold War levels."

The recent recalls and safety concerns with products imported from China, including pet food, toothpaste, and toys, should remind us that the United States is ultimately responsible for protecting its citizens from any and all threats. In light of China's expansive military modernization and its tremendous economic growth, we cannot afford to ignore the threat that espionage and cyber-attacks directed by China towards the United States poses to our national security.

I hope that you will consider this matter and act upon it as quickly as possible.

With kind personal regards, I am

Sincerely,



J. Randy Forbes
Member of Congress

ESPIONAGE: THE ENEMY WITHIN AND THE THREAT TO NATIONAL SECURITY

AMERICA IS AT RISK

- The United States is the Number 1 target of virtually every significant espionage service on the face of the Earth. Just over 100 countries have been identified as a threat to United States interests.

- China, Cuba, Russia and Iran are the most aggressive countries spying on the United States.

- Foreign intelligence operations gather sensitive information through legal and illegal means, such as: business solicitations; circumvention of export controls; and university research and product development; attendance at seminars and conventions; acquisition of American companies.

- Foreign born faculty make up 30 percent of science and engineering departments in United States universities and colleges.

- Foreign intelligence operatives exploit relationships with United States firms which transfer sensitive data to foreign subcontractors

- Foreign intelligence services use widely-available technology, such as cell phone cameras, digital assistants, computers, encryption software to steal classified information, and prey on businessmen traveling overseas to steal or bug communications

Chinese Intelligence Operations

- The FBI has stated that China is -- and will continue to be -- America's greatest counterintelligence problem during the next ten to fifteen years. China does not rely on a "professional" spy operation stationed overseas to the extent other major intelligence services use

such techniques. Instead, China uses low-profile civilians to collect information. They often co-opt Chinese travelers, especially businesspeople, scientists and academics, to gather intelligence or purchase technology while staying in the United States.

- The PRC especially prizes overseas Chinese students, hi-tech workers and researchers living in the United States because of their access to sensitive technology and research/development that Beijing can use for civilian and military purposes.

- The PRC also recruits in the Chinese-American community, including sleeper agents. Developing personal relationships, invoking a common Chinese heritage, threatening cultural alienation or offering access to powerful people are persuasive in a culture where "guanxi" (connections) are important.

- The manpower available to the Chinese government and its corporations to devote to gathering information in the United States is nearly limitless. There are some 300,000 visitors to the United States from China each year. It is impossible to know if these people are here for study and research or if there are here to steal our secrets.

- In 2003, for example, the State Department granted about 27,000 visas to Chinese "specialty workers," the H1-B visa. Some of these were intra-company transfers coming to the United States from US firms operating in China. Indeed, between 1993 and 2003 there were about 40,000 immigrant visas from China a year. The US government has handled about 2,410 asylum cases from China a year. In 2003, there were about 55,000 student visas granted to Chinese students. The sheer magnitude if these numbers presents a great challenge to the Federal Bureau of Investigation, particularly when the US is also concerned about terrorism.

- It is estimated that there are between 2,000 and 3,000 Chinese front companies operating in the United States to gather secret or proprietary information, much of which is national security technology or information.

- The PRC is methodical in its programs to gather information from abroad. In March 1986, the PRC launched a national high technology research and development program with the specific goal of benefiting China's medium and long-term high technology development. This centralized program, known as the "863 Program" for the date when it was announced, allocates money to experts in China to acquire and develop bio-technology, space technology, information technology, laser technology, automation technology, energy technology and advanced materials.

- The 863 program was proposed by China's strategic weapons scientists to emphasize strategic civil and military technology development. Thousands of students and scientists were sent abroad by China over the years to pursue critical civil and military, dual-use technologies. This practice still continues.

- Rep. Wolf has been an outspoken critic of the PRC's espionage activities and the need for a more credible criminal deterrent. "In the Cold War people went to jail for a long time" for spying, he says, but today's "negligible penalties" are more appropriate to low-level embezzlement than military spying

- China's intelligence activities have been "very aggressive" at acquiring U.S. advanced technology, often before it is fully developed here. "The technology bleed to China, among others, is a very serious problem," he said, noting that the FBI is improving its efforts to identify and protect sensitive technology.

- In 1995, China allegedly obtained secrets of nuclear technology in the United States. In 1999, China gained knowledge of the newest warhead that the U.S. was developing- the W-88. A defected Colonel from the Chinese army described the PRC army spy operations -- noting that the Clinton administration partnered with the People's Liberation Army on military training, computers, encrypted communications equipment, satellites, and exclusive access to U.S. military facilities inside America. According to this official, Chinese army intelligence officers abused civilian programs to mask their

military and economic espionage.

- Chinese officials have toured U.S. aviation facilities under the Federal Aviation Administration civil exchange program, using civilian titles and names. One delegation consisted of several high ranking military officials, including the Chinese Army Deputy Chief of the general staff who planned the brutal 1989 army attack on unarmed student demonstrations in Tiananmen Square.

- Under the same FAA program, Chinese officials visited Edwards Air Force Base, which is a test center for American military and NASA research aircraft including the F-22, Joint Strike Fighter and space shuttles. The officers were given detailed information on military operations, including information on "special airspace" areas used for military training, research, and national security zones; the latest information on advanced mobile radars; command and control systems; GPS navigation and "surveillance avionics" such as "air to air," "air to ground," " surface area movement" surveillance radars; combat missions; combat readiness; and received simulated F-16 training.

- PRC Spy Chi Mak, a foreign born electronics engineer who worked for a U.S. defense contractor was caught on an FBI wiretap discussing how to smuggle an encrypted computer disk to China. The disk contained intelligence on "electronic-drive" submarine propulsion systems. Access to this technology could help China achieve a strategic goal: making US Navy operations in the Taiwan Strait so perilous that it would jeopardize Washington being able to aid Taiwan in the event of a cross-strait conflict.

- Katrina Leung operated as a double agent for China and the United States for 20 years, passing on valuable intelligence including information about nuclear weapons to the PRC. She obtained the intelligence through sexual entrapment of the FBI's most senior agents.

SUPPLEMENTAL PREPARED STATEMENT OF LARRY M. WORTZEL, PH.D., CHAIRMAN, UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, WASHINGTON, DC

Chairman Conyers, Chairman Scott, Ranking Members Smith, Gohmert and Forbes, this supplemental testimony addresses questions posed in the January 29th, 2008 hearing on "Enforcement of Federal Espionage Laws." With respect to Chinese front companies, several years ago, officials of the Federal Bureau of Investigation gave rough estimates of the number of Chinese front companies operating in the United States. My discussions with FBI officials more recently suggest that the Bureau is not confident that it can provide such an estimate. I believe that the reticence of FBI officials to provide a number for Chinese government front companies in the U.S. is reasonable. Beginning in 1998, the Chinese military began to divest from its front companies, spinning some off to other government agencies, privatizing some, and creating conglomerates from others. That process has continued to date. My opinion is that absent a concerted effort by the intelligence community to penetrate the network of state, provincial, and locally owned businesses of the People's Republic of China, we will not be able to identify front companies.

I suggest, instead, that the law enforcement and intelligence communities would be more productive and effective if they focused on any illegal activities conducted on behalf of the Chinese government or PRC companies, public or private.

2) With respect to the US-China Economic and Security Review Commission's recommendations about a Director of National Intelligence assessment of U.S. intelligence capabilities vis-à-vis China, the Commissioners generally believe that there are some weaknesses in our intelligence on the PRC. We note in our annual report that the speed with which China is fielding new or improved weapons systems is increasing. In the case of new submarines and new missiles, our impression is that the U.S. government was surprised by the numbers and timing of the fielding of new systems in China. We note that the U.S. national security advisor opined that in the case of China's January 11th, 2007 satellite shoot-down, the President and Communist Party Chairman of China, Hu Jintao, may have been taken by surprise. Yet officials of the PRC Foreign Ministry and People's Liberation Army were firm when we questioned them on this point in April 2007, that as Chairman of the Communist Party Central Military Commission, China's President was aware that the test would take place. This suggests that at the highest levels of the U.S. government, our understanding of decision-making processes in China could be improved. Commissioners also think that better language capabilities in the intelligence community may lead to improved intelligence collection and analysis as well as better counterintelligence. We therefore recommended a broad assessment of all U.S. intelligence capabilities vis-à-vis China and that the DNI identify strategies to address any weaknesses such as assessment may discover.

3) With respect to espionage cases and the burden of proof, I noted in my testimony that prosecution often relies on lesser charges or on violations of the Arms Export Control Act, the Export Administration Act (and related Executive Orders) or on 18 USC 951, or acting as an agent of a foreign government. My own experience in counterintelligence investigations and my observations of other prosecutions tells me that in many cases we are able to establish that an individual illegally obtained, removed, or collected and hoarded classified information or information respecting the national defense, but we can't prove espionage. In some cases investigations have lead to charges that an individual acted as an agent of a foreign power, and in at least one case a polygraph examination led to an individual admitting that he communicated classified information to a foreign power. Hoarding or removing classified documents illegally, however, does not prove intent or espionage. Some individuals do this because they want to write memoirs, while some have such egos that they think they are smarter than classification authorities and can ignore security classifications. I investigated one case where a U.S. Army officer was hoarding classified U.S. documents and probably giving them to Chinese military officers in trade for research materials for his own academic efforts; however, we could not prove espionage. That officer was punished for improper handing of classified documents. I am convinced he was guilty of espionage. Therefore, I suggest that the Committee examine 18 U.S.C. 793 (e) and (f) with a view toward strengthening the language, specifying a large fine, and increasing the maximum penalty beyond 10 years. With respect to 18 U.S.C. 798, I recommend that the Committee increase the penalties for violations concerning communications intelligence and cryptographic activities. Finally, I note that there is no specific mention of imagery intelligence or other electronically gathered forms of intelligence. I recommend that the Committee consult with the DNI and other relevant agencies of the intelligence commu-

nity to examine whether other mediums of U.S. intelligence should be addressed in the law.

4) With respect to identifying trained intelligence officers or the recruited assets of trained intelligence officers, success really depends on good counterintelligence, careful investigation, and good surveillance on the part of U.S. intelligence and law enforcement personnel. Our intelligence professionals need the tools of electronic surveillance and must be able to conduct offensive counterintelligence operations to penetrate a foreign intelligence service and learn its methods of operation. Investigations may take some time however; there is always the danger of allowing damaging vital information to be conveyed to a foreign power while trying to gather more information on espionage methods or to broaden a case. There is no formula here, but good cooperation among the law enforcement community, the intelligence community and the Department of Justice is key to success.