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

Subcommittee on Oversight
Committee on Science, Space & Technology

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

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

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

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

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

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

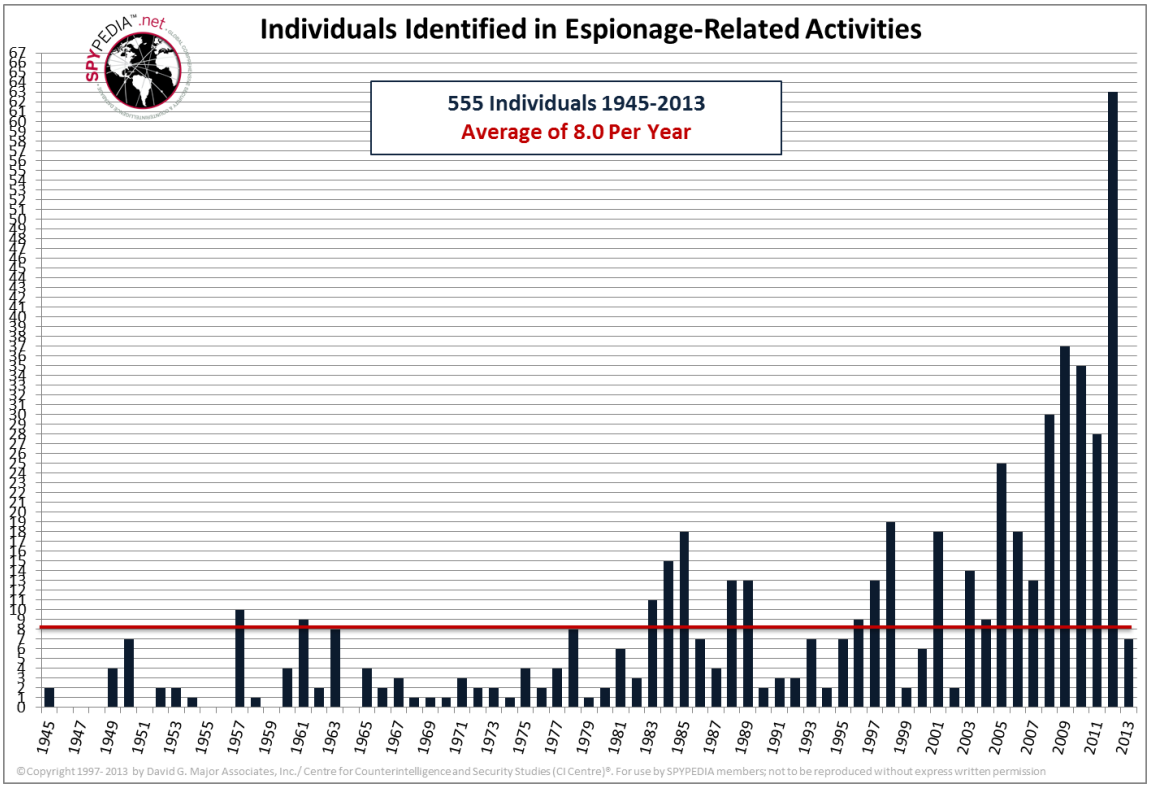
US Government agencies and personnel, corporations, universities and private citizens are members of SPYPEDIA® to meet a variety of their individual diverse needs and interests.

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

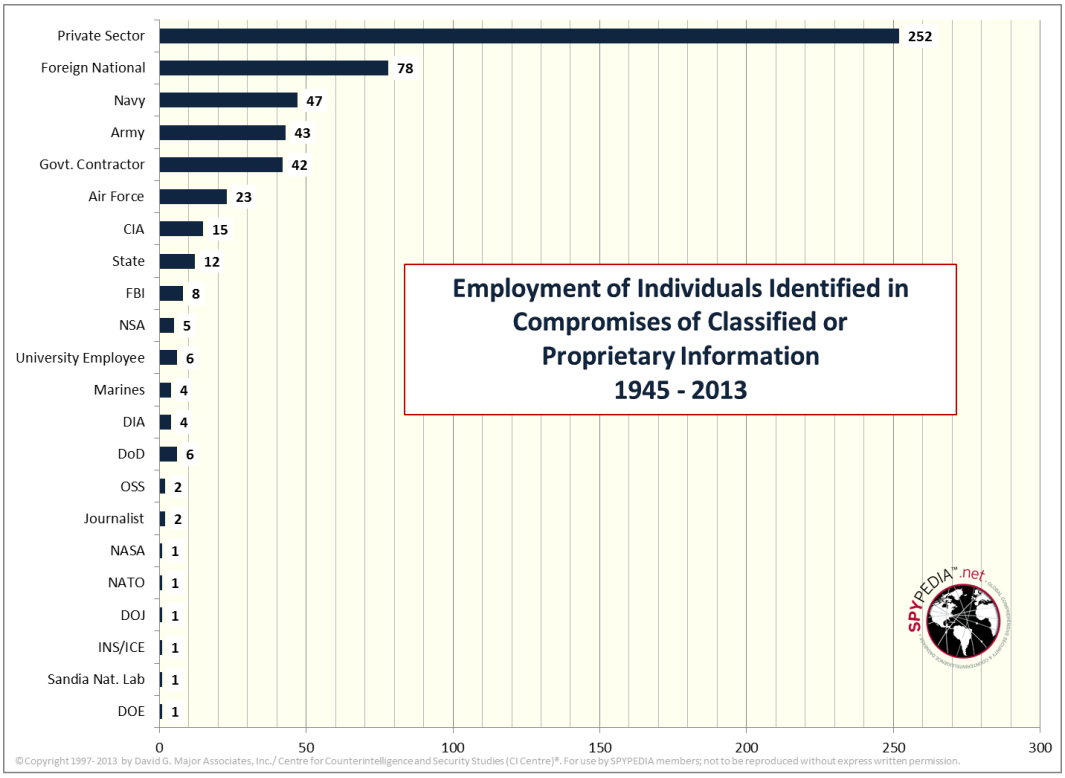
We collect espionage data for the period of 1945 to the present looking at the following individual charges to draw our conclusions.

- Foreign Nationals charged
- "Espionage" related arrests for violation of
    - US Code Title 18, Section 793 and Section 794
    - FARA US Code 18, Section 951
    - Economic Espionage, US Code 18, Section 1831 and Section 1832
    - Violation of US Code Title 18 Section1001
- Individuals who defected pending arrest
- Individuals who committed suicide pending arrest
- Individuals who diverted technology for foreign governments in violation of International Traffic in Arms Regulations (ITAR)

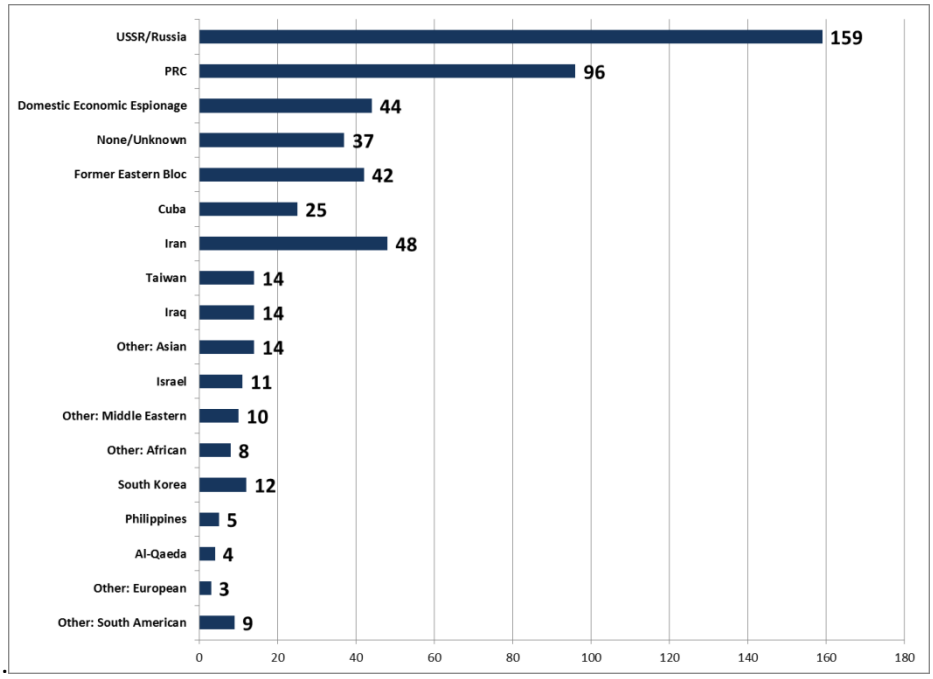
We have identified at least 555 individuals that meet these criteria.



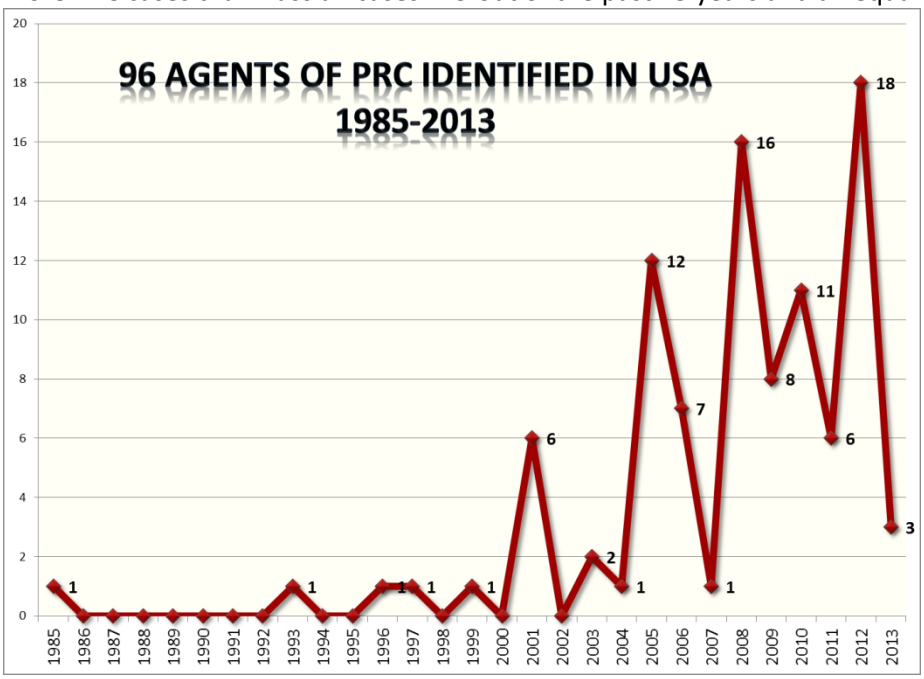
The vast majority these individuals are from the private sector with 252 cases and 78 foreign nationals.



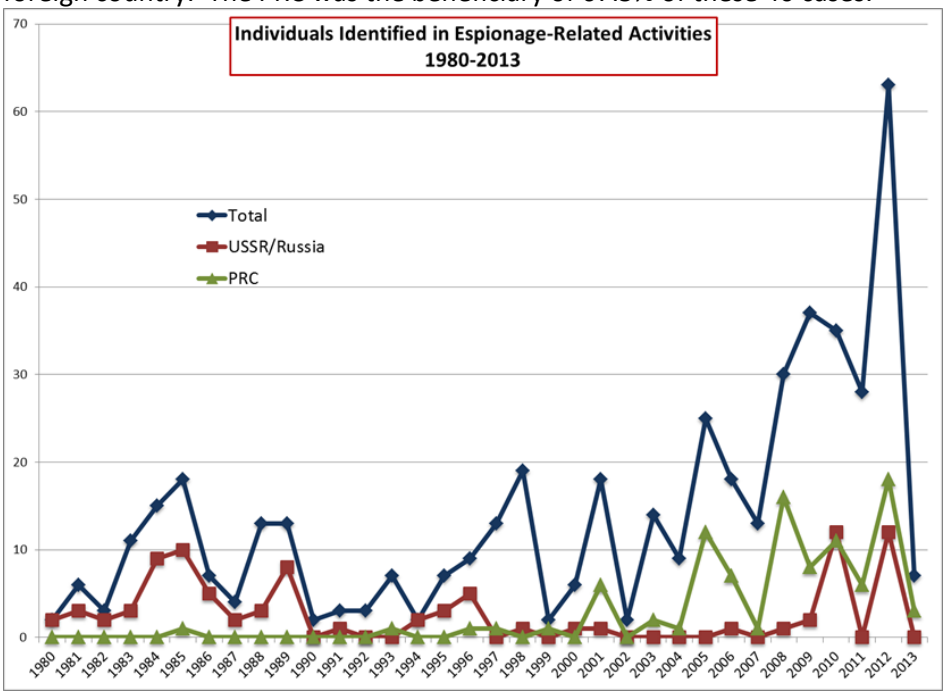
There are 31 countries identified in the public record as responsible for conducting the "espionage related cases" with the USSR/Russian and the People's Republic of China (PRC) having the largest number of cases.



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



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



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

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

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

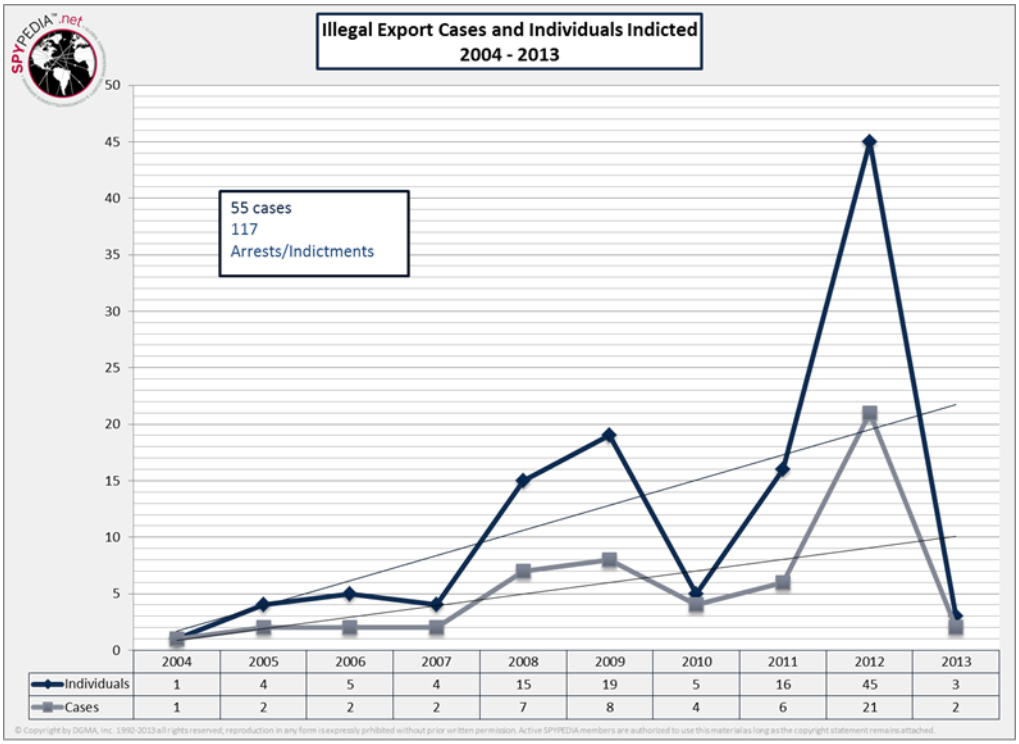
As for how this information is stolen, the majority of the subjects' simply downloaded protected files onto an external hard drive and other personal devices, or forwarded it via email. There are a few interesting cases where individuals traveled to foreign locations and gave lectures at universities/business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

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

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

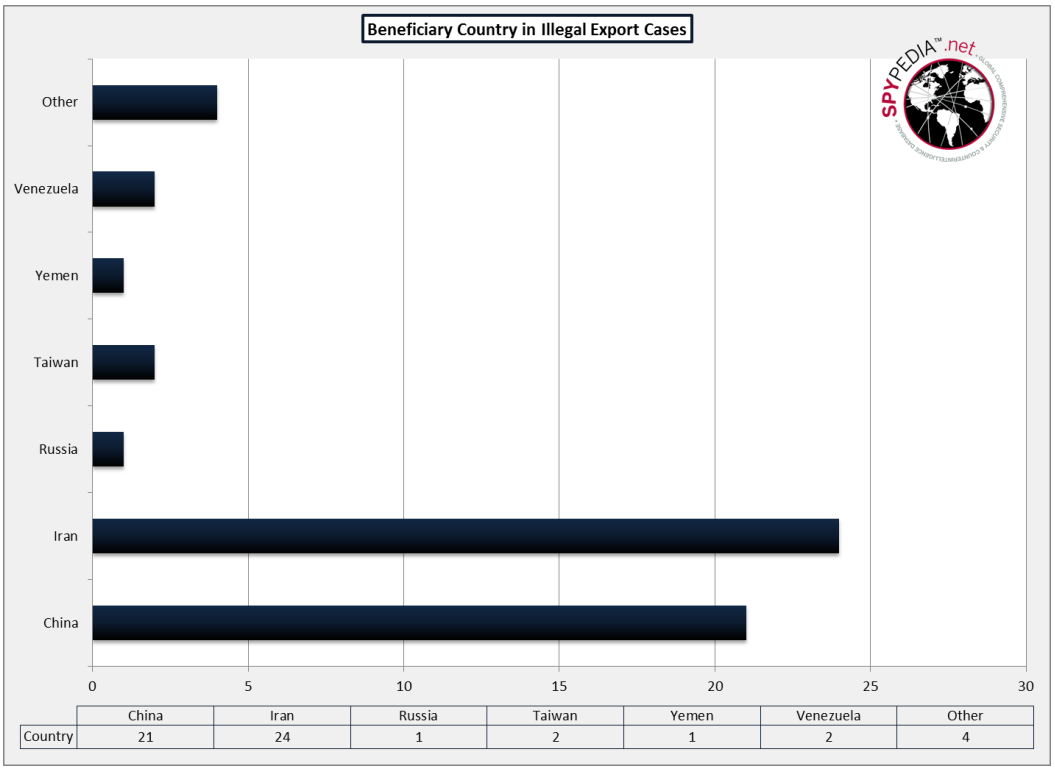
- Foreign nationals in labs -- they need extremely robust real-time 100% computer monitoring
- Foreign nationals need to be sealed off from physical access to sensitive areas.
- The labs need vigorous and realistic training of cleared personnel regarding loose chatter to un-cleared personnel.

There have been 55 technology diversion cases involving 117 individuals



	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Individuals	1	4	5	4	15	19	5	16	45	3
Cases	1	2	2	2	7	8	4	6	21	2

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



	China	Iran	Russia	Taiwan	Yemen	Venezuela	Other
Country	21	24	1	2	1	2	4