House Committee on Science, Space and Technology

Subcommittee on Oversight

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

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

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

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

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

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

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

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

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

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

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

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

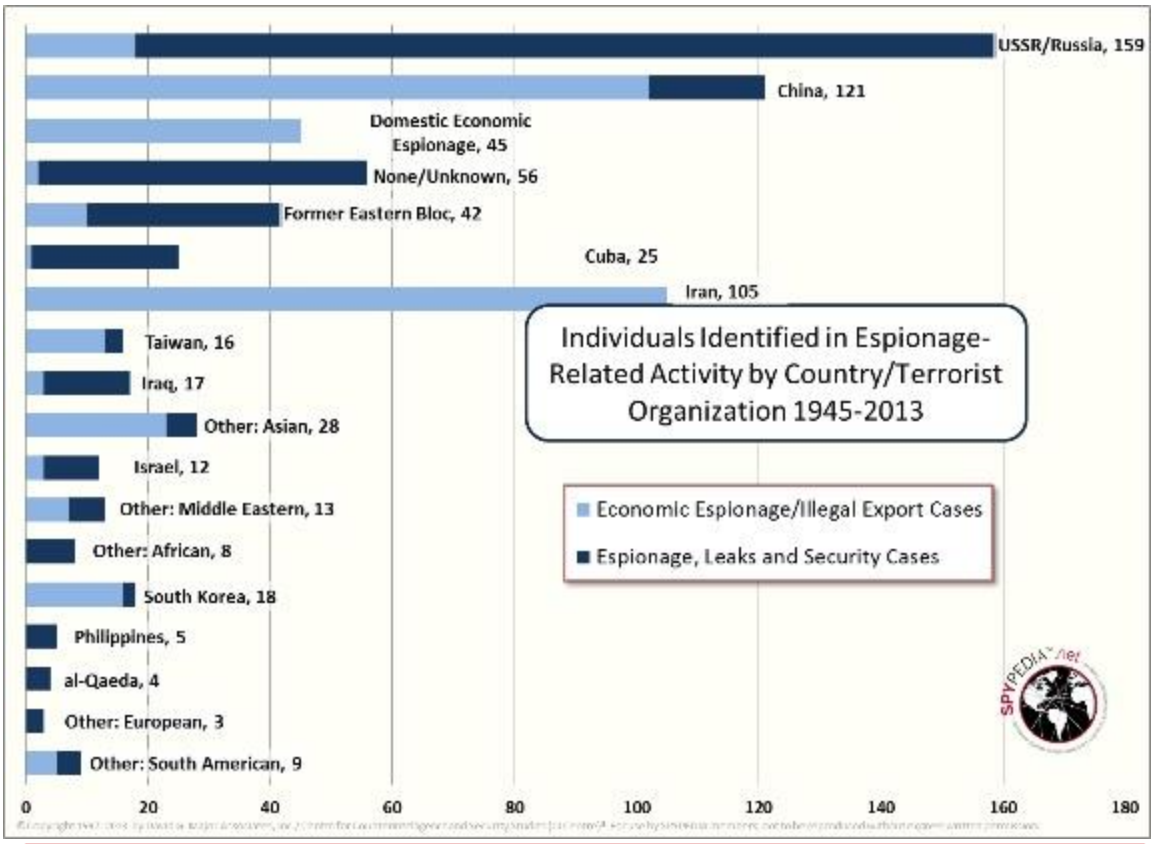
> "By creating the National Security Threat List (NSTL), which was approved by the attorney general in 1991, it changed its approach from defending against hostile intelligence agencies to protecting U.S. information and technologies. It thus identified all countries—not just hostile intelligence services—that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

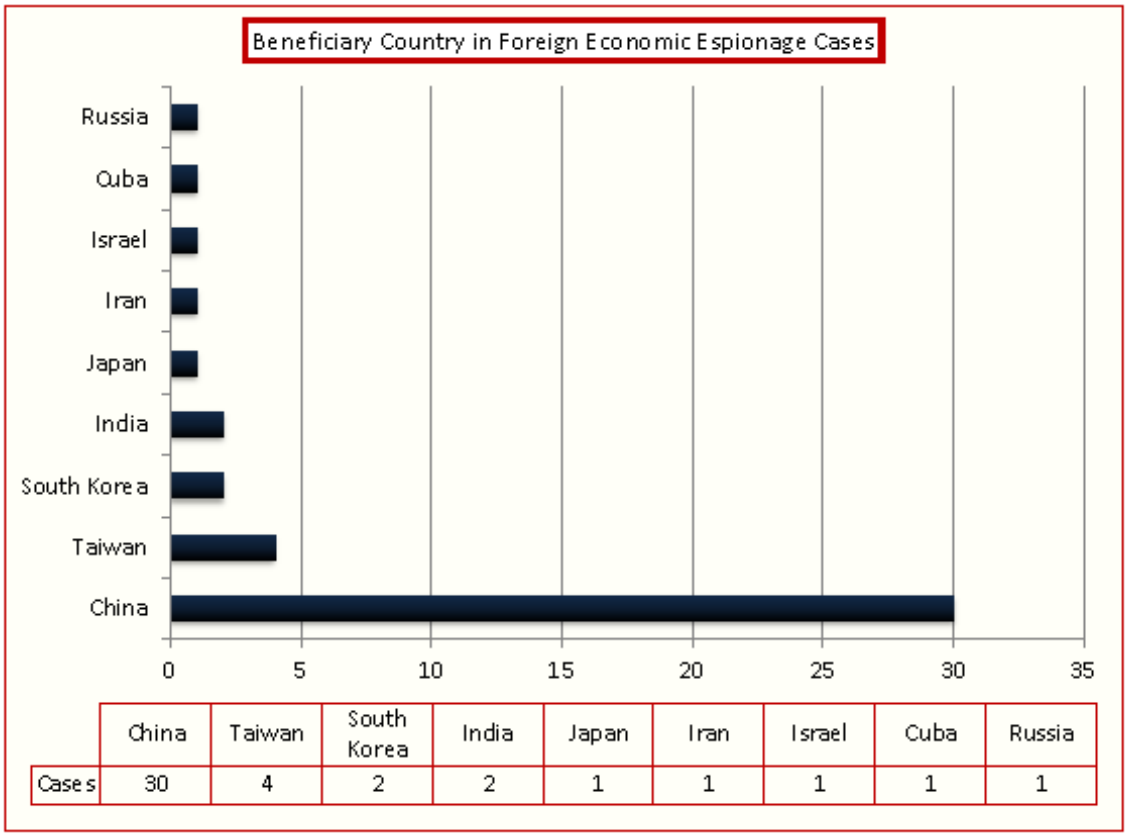
The FBI's foreign counterintelligence mission is set out in a strategy known as the National Security Threat List (NSTL). The NSTL combines two elements:

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

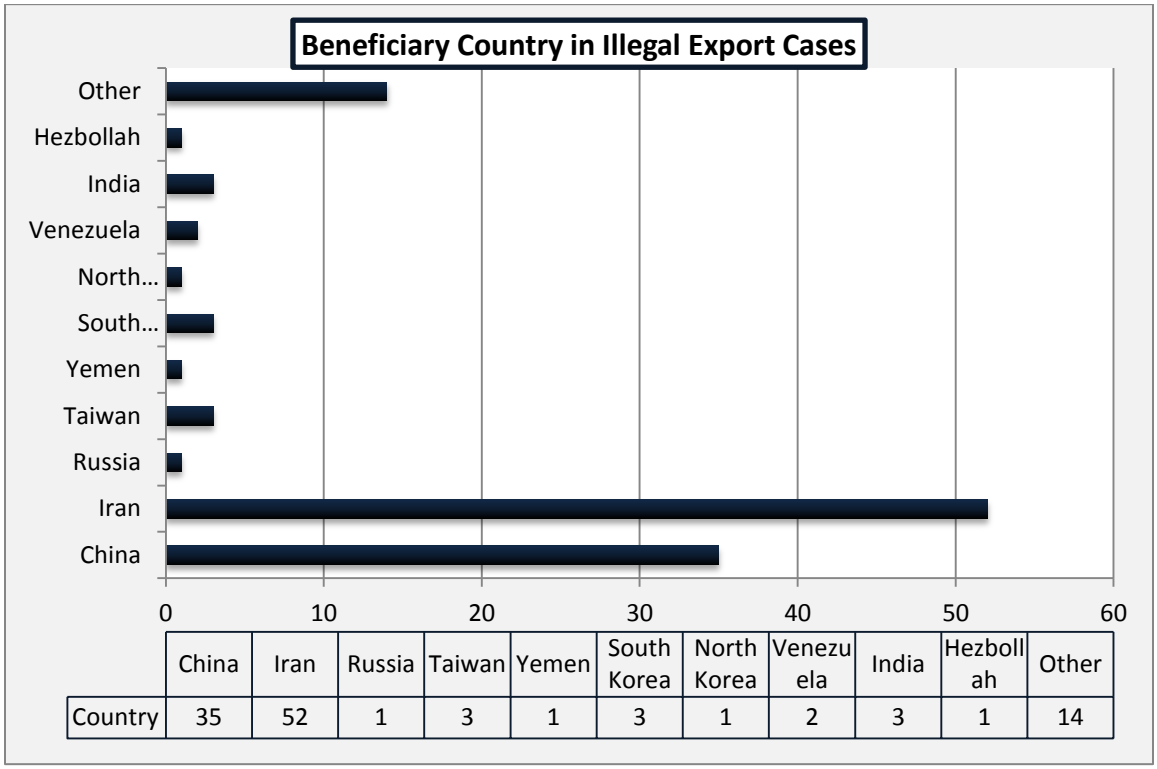
Accordingly, the national counterintelligence strategy has already addressed the essence of this question. The DOJ and FBI require evidence of aggressive intelligence collection against the USA before a country can be placed on the NSTL Country Threat List. Responding to this collection threat is not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

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

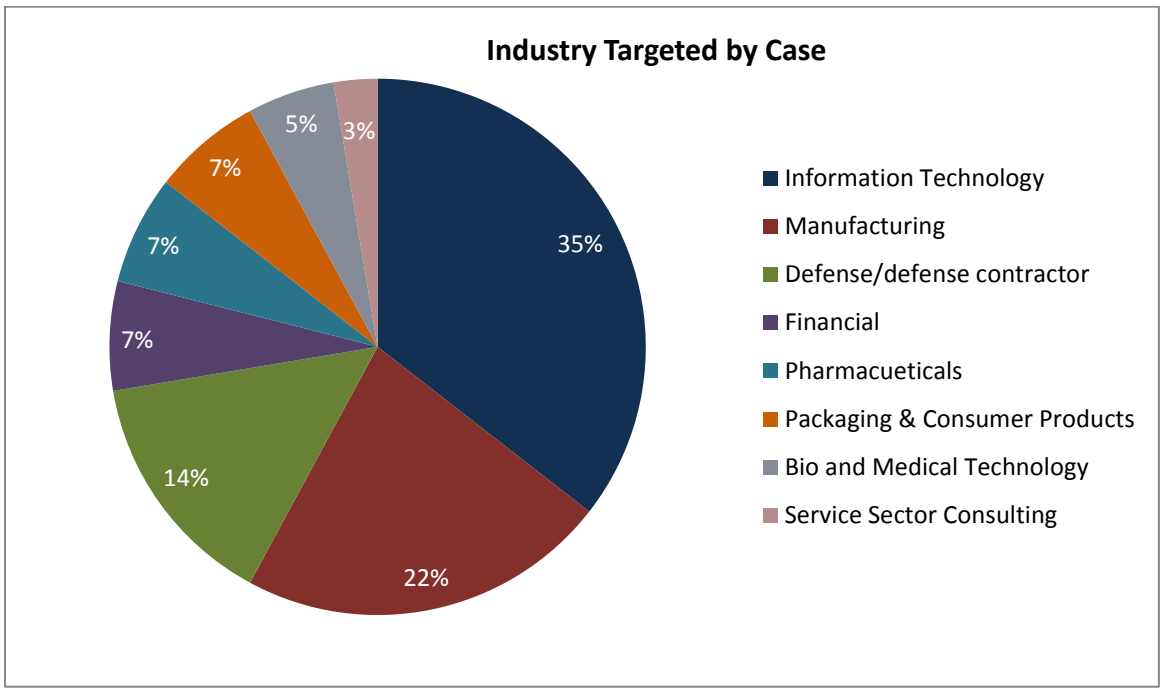




	China	Taiwan	South Korea	India	Japan	Iran	Israel	Cuba	Russia
Cases	30	4	2	2	1	1	1	1	1



	China	Iran	Russia	Taiwan	Yemen	South Korea	North Korea	Venezuela	India	Hezbollah	Other
Country	35	52	1	3	1	3	1	2	3	1	14



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

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

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

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

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