

Chinese Intelligence Webcast Q&A Section

Sponsored by American Military University

Answers provided by William Tucker, Counterintelligence Officer and AMU Graduate of Homeland Security

Is there an open source information repository online, where an individual interested in this subject matter can learn more about the "Chinese challenge?"

William Tucker: I will include a few links that you can start with. As you start reading the available material I strongly suggest that you do not take everything the authors say at face value. The listed materials are useful; however each author has their own agenda and facts can easily be lost. Focus on verifiable facts with accurate source information and go from there.

<http://www.fas.org/irp/threat/handbook/index.html>
<http://www.globalsecurity.org/intell/world/china/index.html>

You can read many exceptional articles in the *Journal of Intelligence and Counterintelligence* located in the AMU online library.

Books:

The China Threat, Enemies both by Bill Gertz

Unrestricted Warfare: China's Master Plan to Destroy America by Qiao Liang, Wang Xiangsui

In terms of the 2 million people working for Chinese Intel Services – are all of those engaged in Intelligence Collection or does it expand to ancillary roles? Here in the U.S. if you think about all the people working on government contracts for DIA, CIA, NSA and other areas it probably comes to many more than that. How does the 2 Million in China break down in terms of roles?

William: The "two million" figure is only suspected and the actual number is classified by the Chinese government. That being said the intelligence agencies of the Chinese government are structured similarly to most large intelligence agencies found worldwide meaning that actual collectors would only make up a fraction of the two million figure. Support personnel are necessary for any bureaucracy.

As far as US intelligence agencies go – DIA: 16,500; CIA: 20,000; NSA: 30,000. The actual numbers are classified, but these are fairly close. The Washington Post recently ran a series of articles entitled *Top Secret America* in which the authors claim that 854,000 Americans possess a top secret clearance. This number is unlikely as it only counts those that have a clearance rather than those that have access. We also need to consider that intelligence collection by private contractors is in many cases forbidden by US law (It still happens, however).

It seems that our U.S. operation in China is obsolete. Are we planning on countering any of the "thief issue" anytime soon?

William: First and foremost we have to separate US operations in China from the methods of countering threats domestically. Intelligence operations are conceived to fill a specific need and the US will have several operations targeting a large adversarial nation, such as China, depending on the needs of the Executive or Congress. Operations in China are focused on collection for several reasons, but the reason that stands out is the large security apparatus in China. Because of this security apparatus it is difficult to do much more.

US collection operations that are carried out in China are different than the counterintelligence operations that are run in the US. The US does carry out offensive CI operations in China, but because of the high risk nature of these operations they are used sparingly. Additionally, there is no one point of failure that could be targeted to disrupt Chinese collection operations run against the US. Rather it is imperative that government and industry work to better protect the intellectual property they consider sensitive. This is the most effective means at countering theft.

To put this differently, consider that in 2007 the US was targeted by 108 different nations for collection. It is impossible for any agency or company (unless it is an intelligence agency) to focus on 108 nations and discern their collection goals. Instead it is far easier to focus on our business conduct and protect those singular items that ensure success.

Where does open source intelligence fit in the overall scheme of intelligence?

William: In many ways open source intelligence doesn't fit in with the US national intelligence approach. That is not to say it shouldn't, but rather it has not been seen as a necessary aspect of intelligence collection and analysis which is a shame. Some agencies that have an intelligence apparatus have integrated open source intelligence units into their traditional intelligence groups, but the overall impact is still being assessed.

My personal view is that open source intelligence is vital to the nation. Simple things such as internet access and newspapers offer a substantial amount of information to those looking to protect their information.

How can we protect ourselves?

William:

1. Identify information and personnel that are vital to your organization and organize a plan to protect them. Know your limitations – not everything can be protected as well as we would like.
2. Educate your employees on the threat. You don't always have to know every threat, but just spreading the word that your information or people are being targeted is a great first step.
3. Outreach. If you are government you should reach out to private industry and vice versa. Local FBI field offices along with elements of DHS have local and international threat information that may impact your business. On the other hand the government cannot compile an accurate threat picture without your input. The same goes for reaching out to other companies security departments. Physical threats to one business can impact the operations of another.