TITLE: Lessons Learned from Chinese Intelligence Officer Arrest
Date: Oct. 17, 2018

Disclaimer: this briefing note contains summaries of open sources and does not represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

The following key events are discussed in this briefing note with specific application to cybersecurity practices which enables early detection and investigation of potential threats. The following events are: 1) A press release (Oct 10, 2018) announcing Chinese Ministry of State Security (MSS) operative, Yanjun Xu, aka Qu Hui, aka Zhang Hui, has been arrested and charged with conspiring and attempting to commit economic espionage and steal trade secrets from multiple U.S. aviation and aerospace companies[1]. 2) A press release (Sept 25, 2018) announcing that the FBI arrested a Chinese national named Ji Chaoqun in Chicago working as a unregistered agent of China's civilian intelligence agency targeting American defence contractors.

NATURE OF DISCUSSION

These two incidents share the following common details:

1. Both press releases make reference to a Chinese intelligence officer, specifically a Deputy Division director with the Jiangsu Province MSS (ref: fn1 and fn2).
2. MSS Deputy Director XU's activity is dated to December 2013.[2]
3. MSS Deputy Director's activity for CHAOQUN is dated to June 2003[3].
4. CHAOQUN's enlistment as U.S. Army Reserve program (Military Accession Vital to the National Interest program, known as MAVNI)(ref: fn3)
5. Both involved access to sensitive information, and
6. The use of human connections for intelligence gathering.

[1] Department of Justice, 2018, Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation companies. Retrieved from https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading

[2] US District Court for the Southern District of Ohio (Cincinnati), 2018, United States of America v. Xu YANJUN

[3] Gertz, 2018, FBI Arrests Chinese National Charged as Beijing Spy, Retrieved from https://freebeacon.com/national-security/fbi-arrests-chinese-national-charged-beijing-spy/print/

BACKGROUND

Reports about the Chinese spy arrest, from authors such as Schoenberg and Strohm[4] and Stewart from Stratfor[5], rightly point out the Chinese will continue to use technology and human intelligence sources to conduct espionage. This is consistent with China's military doctrine book "Unrestricted Warfare"[6] which identifies "financial warfare" "trade warfare" "economic aid warfare" "regulatory warfare" "sanction warfare" (p. 146). The authors (Liang and Xiangsui, 1999) also provide insight into the ideal combinations of political, ideological and diplomacy rules which support these types of warfare. Central to their insight, the notion of taking time and focusing on specific targets which improve China's ability to be a world economic power.

However, it is critical to point out the U.S. indictment for XU contains references which confirm that physical security combined with information technology security does provide opportunities to intercept and disrupt these espionage efforts by China.

For example, the US District Court of Southern District of Ohio (Western Division) Indictment Case 1:18CR-43[7] provides evidence which indicates Victim Company A and the targeted Employee 1 were able to coordinate a response to the enticements by XU with Employee 1. Mr. Xu's enticements included paid trips to China, during which Employee 1 would present Victim Company A's specific aviation technologies associated with jet engine fan blades and fan containment structures. There was also direct instructions from Mr. XU to Employee 1 to reveal commercial secrets, which would occur on a trip to European Union sometime Feb/Mar 2018. The indictment appears to be a coordinated effort by US officials and Victim Company A to meet with Mr. XU and subsequently arrest and deport Mr. Xu from Belgium to the United States on April 1, 2018.[8]

The indictment also provides information about the physical and intellectual security measures of Victim Company A. The security measures included limiting physical access to restricted portions of campus, use of manned, gated entrances and requiring identification and access badges. Victim Company A also had employee non-disclosure and other confidentiality agreements that extend beyond the length of employment at Victim Company A; recurrent training and instruction for employees regarding the processes in place to safeguard restricted and confidential business information; notifying all employees that publication and/or disclosure of restricted or confidential company information is prohibited without express company authorization. Victim Company A also had various data security policies; and enforced limited access to company proprietary information to employees or contractors on a need-to-know basis. All of these security features appear to inform the merits of the case and helped inform Employee 1 of his/her responsibility.

---

[4] Schoenberg & Strohm, 2018, Chinese Intelligence Official charged with Stealing U.S. Aviation Secrets. Retrieved from http://time.com/5421088/chinese-u-s-spy-extradited/

[5] Stewart,. (2018). A Sting Operation Lifts the Lid on Chinese Espionage. Retrieved from https://worldview.stratfor.com/article/sting-operation-lifts-lid-chinese-espionage?utm_so

[6] Liang & Xiangsui, 1999, Unrestricted Warfare.

[7] U.S.A. v Yanjun XU (2018). Case No. 1:18CR-43. U.S. District Court Southern District of Ohio (Western Division).

[8] Delaney, 2018, Chinese spy caught in rare sting after 'plot to steal US trade secrets'. Retrieved from https://www.scmp.com/print/news/china/politics/article/2167973/chinese-spy-charged-stealing-us-aviation-secrets-and-extradited?MCAccountID=3775521f5f542047246d9c827&MCCampaignID=a96bf9761c&MCUID=7871f94cce&tc=1

KEY POINTS OF DISCUSSION AND WEST COAST PERSPECTIVES

Key Point 1 - Strong Interagency and Infrastructure Information Sharing and Cooperation. As noted in the discussion points, Victim Company A and a U.S. agency were able to coordinate their responses with Mr Xu which resulted in him being extradited from EU. This speaks to power of collaboration and knowing who to collaborate with. **PSC Canada (2016)** provides 10 critical infrastructure sector and specific federal department contacts (ref: fn10). However, Neilson (2017) suggests there is a need for more public education, funding of cybersecurity, and the development and promotion of established standards, best practices, certification and legislation. Neilson's closing comment is the most intriguing

- Being proactive "There appears to be an overemphasis on resilience, emergency management and disaster recovery, thus presenting a policy of failure as the starting point of a strategy for cyber and critical infrastructure protection. Proactive cyber defence should be added." Some participants indicated that actions to improve cyber security in Canada should be proactive in nature, instead of reactive. In fact, it was expressly stated by a few participants that the action areas given to them as examples in the workbook were too defensive, and should instead be more offensive in nature. (p. 42)[9].

HOW CAN CANADA move to be a leader in proactive offensive cyber security to protect critical infrastructure?

Key Point 2 - Public Safety Canada *Fundamental of Cyber Security for Canada's Critical Infrastructure Community (2016)* [10] outline threats to Canada's digital economy (industrial espionage, state-sponsored cyber espionage, criminals, hacktivists/recreational hackers, and insider threats). The PSC document also clearly notes 'cyber security is everyone's responsibility', and also notes what those responsibilities. **SHOULD Canada** specifically educate national infrastructure companies on the details of the Chinese threat and evaluate Chinese hosted conferences as potential espionage activities?

[9] Nielson, 2017, Cyber Review Consultations Report, Public Safety Canada. Ottawa, ON.
[10] Public Safety Canada, 2016, Fundamentals of Cyber Security for Canada's Critical Infrastructure Community.

References

Delaney, 2018, Chinese spy caught in rare sting after 'plot to steal US trade secrets'. *South China Morning Post* (Oct 11, 2018). Retrieved from https://www.scmp.com/print/news/china/politics/article/2167973/chinese-spy-charged-stealing-us-aviation-secrets-and-extradited?MCAccountID=3775521f5f542047246d9c827&MCCampaignID=a96bf9761c&MCUID=7871f94cce&tc=1

Gertz, B. (2018). FBI arrests Chinese national charged as Beijing spy. *Washington Free Beacon* (Sept 25, 2018). Retrieved from https://freebeacon.com/national-security/fbi-arrests-chinese-national-charged-beijing-spy/print/

Liang, Q., & Xiangsui, W. (1999). *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House.

Nielson. (2017). *Cyber Review Consultations Report.* Public Safety Canada. Ottawa, ON.

Public Safety Canada. (2016). *Fundamental of Cyber Security for Canada's Critical Infrastructure Community.* Ottawa, ON.

Schoenberg, T. & Strohm,C. (2018). Chinese intelligence official charged with stealing U.S. aviation secrets. *Time: China* (Oct 10, 2018). Retrieved from http://time.com/5421088/chinese-u-s-spy-extradited/

Stewart, S. (2018). A sting operation lifts the lid on Chinese espionage. *Stratfor (Worldview)* (Oct 16, 2018). Austin, TX. Retrieved from https://worldview.stratfor.com/article/sting-operation-lifts-lid-chinese-espionage?utm_so

US District Court for the Southern District of Ohio (Cincinnati). (2018). *United States of America v. Xu YANJUN. Case No. 1:18MJ-190*. Cincinnati:OH.

U.S. Department of Justice. (2018). *Chinese intelligence officer charged with economic espionage involving theft of trade secrets from leading U.S. aviation companies.* U.S. Department of Justice (Office of Public Affairs (Oct 10, 2018). Washington, DC. Retrieved from https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading.

U.S.A. v Yanjun XU (2018). *Case No. 1:18CR-43.* U.S. District Court Southern District of Ohio (Western Division).