LESSONS LEARNED FROM CHINESE INTELLIGENCE OFFICER ARREST

Date: October 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 (Department of Justice, 2018). 2) A press release (Sept 25, 2018) announcing that the FBI arrested a Chinese national named Ji Chaoqun in Chicago working as an 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 refer to a Chinese intelligence officer, specifically a Deputy Division director with the Jiangsu Province MSS (Department of Justice, 2018; US District Court for the Southern District of Ohio (Cincinnati), 2018).
2. MSS Deputy Director Xu's activity is dated to December 2013 (US District Court for the Southern District of Ohio (Cincinnati) 2018).
3. MSS Deputy Director's activity for CHAOQUN is dated to June 2003 (Gertz, 2018).
4. CHAOQUN's enlistment as U.S. Army Reserve program (Military Accession Vital to the National Interest program, known as MAVNI) (Gertz, 2018).
5. Both involved have access to sensitive information.
6. The use of human connections for intelligence gathering.

BACKGROUND

Reports about the Chinese spy arrest, from authors such as Schoenberg and Strohm (2018) and Stewart from Stratfor (2018), 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," which identifies "financial warfare," "trade warfare," "economic aid warfare," "regulatory warfare," and "sanction warfare" (Liang and Xiangsui, 1999, 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 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 (U.S.A. v Yanjun Xu, 2018). 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 are 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 (Delaney, 2018).

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.

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 the power of collaboration and knowing whom to collaborate with. PSC Canada (2016) provides ten critical infrastructure sector and specific federal department contacts. 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:

> "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" (p.42).

Some participants indicated that actions to improve cybersecurity 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 (Nielson, 2017 p. 42).

How can Canada move to be a leader in proactive offensive cybersecurity to protect critical infrastructure?

Key Point 2 - Public Safety Canada *Fundamental of Cybersecurity for Canada's Critical Infrastructure Community (2016)* outlines 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 'cybersecurity 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?

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/chi nese-spy-charged-stealing-us-aviation-secrets-and-extradited?MCAccountID=3775521f5f542047246d9c827&MCCam paignID=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-chinesenational-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-lidchinese-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-intelligenceofficer-charged-economic-espionage-involving-theft-trade-secretsleading.

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

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/