Open Access License Notice

Cyber Threats to the Supply Chain: How Cyber Intelligence Informs Best Practices for Operational Security

Cherine S. Abdalla

Cyber threats to the supply chain of commercial Information, Communication and Technology (ICT) products, as well as, espionage activities targeting defense manufacturing facilities necessitates a multidisciplinary approach to be used. The integration of cyber intelligence can assist in building a framework for best practices to mitigate activities of Advanced Persistent Threat (APT) groups at the point of origin. Lower tier suppliers and vendors who provide raw materials and commercial off the shelf (COTS) component parts comprise the exposed soft underbelly most vulnerable to compromise. These lower tiers in the supply chain are the source of greatest disruption and vulnerability due to the opacity of security oversight upstream and are the key to building supply chain resilience.

Threat actors focused on both cyber and real world exploits have both the active support of cybercrime syndicates and the passive support of governments and legitimate corporations. Resources, skilled personnel, funding and even limited partnerships are forged where their interests may temporarily align, however different their core goals may be. Cyber intelligence can act as a critical component to supply chain security on strategic, operational and tactical levels.

Supply chain risk management is a formal process acting to ensure the integrity, safety and security of the supply chain as the interdependence on foreign technology, scarcity of resources and addressing the threat of malicious intent within US based or foreign products. It addresses implementing rigorous standards and security practices that ultimately would reduce risks that cyber threats and espionage pose to the supply chain.

Supply chain risk governance best practices demands that policies are in place to define the roles and responsibilities for implementing supply chain risk mitigation activities. International standard agencies can be called upon to develop and encourage a better strategy around complex environments, in order for leadership to make strategic level judgments the inclusion of actionable cyber intelligence in the calculus is necessary to more fully understand the threats that may deter them from fulfilling their objectives [1] through operational and tactical decisions.

A technically rigorous and analytic discipline, cyber intelligence gathers information collected from traditional intelligence sources to inform leadership on concerns affecting processes at all levels in the cyber domain.[2] It can be a powerful predictive and analytical tool that adds value at strategic, operational and tactical stages, as well as, helps to inform and guide the approach and response to real threats in both the physical and digital world. The cyber landscape is truly the new Wild West. The cyber world has few enforceable parameters, and internationally, there are few or outdated regulatory policies for international cyber security. Cyber intelligence is uniquely poised as an additional tool in the arsenal to aid risk management and cyber security measures within the international supply chain.

---

[1] "Operational Levels of Cyber Intelligence." Intelligence and National Security Alliance, Cyber Intelligence Taskforce. (2013, September).

[2] "Cyber Intelligence: Setting the Landscape for an Emerging Discipline." Intelligence and National Security Alliance, Cyber Intelligence Taskforce. (2011, September).

The threat is an asymmetric one. The imbalance of power, capital, assets, capabilities, strategy and tactics differs significantly between attacker and defender. Despite the battery of resources governments and corporations may have at their disposal slow response time due to lack of agility caused by the sheer breadth, scope and interconnectedness of the global supply chain severely hampers efforts on the defenders side. The supply chain is, by its very nature, highly fragmented. Defensive measures aim to provide and maintain successful and constant end to end security at a high cost, whereas threat actors have a much lower threshold to meet in order to achieve success. Highlighting the difficulties of mitigating asymmetric threats is the attackers anonymity, the ability to procure cyber black market exploit kits, the skills and coordination of like minded comrades from around the globe and the technical ability to create or purchase customized exploits targeted at specific persons, companies or government entities either individually or in combination. The challenges posed by these prolific multi-national cyber criminals is the talent to create innovative, cutting edge attacks and developing threat vectors beyond the technology of most security systems. The temporal, spatial and funding prerequisites from exploit generation to execution is minimal relative to the resultant damage caused.

The globalization of technology, its development and manufacture has led to an increased demand and has created a high level of competition throughout the supply chain. The drive to maintain competitive by keeping costs low fuels dynamic innovation, however, the great need for raw materials and the limited oversight and visibility of

procurement at third and fourth tier supplier levels can make determining the complete security of an end product speculative. The degradation of confidentiality, integrity and availability is the resulting byproduct of an expansive global supply chain offering a multitude of possible access sites vulnerable to exploits at any point in product lifecycle. These points of access, whether due to technological based vulnerabilities or purposeful malware or spyware insertion are caused primarily by the following three variables. Inherent upstream vulnerabilities include being based 3 and 4 degrees of separation from main suppliers, also vendors providing key mined resources and component parts are typically geographically far removed. Lastly, suppliers and vendors neither contractually nor culturally carry the obligation to guarantee such overarching security measures for quality assurance. Further, the advancement and intensity of cyber threat activity has increased exponentially caused by the general belief that these threats are primarily technical and tactical in nature not accounting for other threat vectors. Vendor threat information culled from strategic cyber intelligence sources would help to create informed risk based decisions driven by a focused effort on operational security further down the supply chain.

The increasing dependence on commercial off the shelf (COTS) products, particularly by Department of Defense (DOD), in order to increase speed, efficiency and as a cost saving measure for a global multi-tiered supply chain has had the singular undesired consequence of being inadequately secured due to global outsourcing. Because of their many component parts there is a great risk of taint and counterfeit that may fail at significantly and possibly dangerously higher rates as well as poor quality as they are

being sourced from lower tier suppliers and vendors. An inferior quality product may not have been produced by malicious intent but rather the desire to make or save money through a lower cost substitution. However, that material substitution may create vulnerabilities that can be later exploited for malicious insertion further down the supply chain or allow unauthorized users access to sensitive systems.

The Asian market, specifically China, has been the prime location for global outsourcing of ICT commercial off the shelf (COTS) products and their components from lower tier supplier and vendors. China is an interesting case study in its near virtual government dominance of its telecommunications manufacturing industry. The Chinese have built this monopoly by nearly eliminating every other foreign mining operation with their ability to more cheaply extract rare earth metals and materials found in limited quantities around the globe and necessary for modern electronic and metallurgical applications. The Chinese control in this supply chain sector of ICT and COTS products has produced a lengthy history of sizeable amounts counterfeit and tainted components in U.S. products. A United States Senate special investigation in 2012 revealed that 70% of counterfeit parts found during the course of a single year originated from China. Since 2007 numerous high profile espionage activities have been exposed dealing with critical U.S. infrastructure and military weapons systems . This has highlighted the adversarial stance China is using to not only severely compromise and hamper U.S. private sector infrastructure and national defenses but to advance and secure their own weapons system foregoing the output of funding for research and development enabled by the very supply chain business the U.S. is providing. These incidents illustrate the vulnerability not only

of U.S. supply chain security with lower tier Asian suppliers but of United States national security, global strategic relations and the possibility of an entirely new kind of warfare on the horizon. In order to understand the aspects of this new dimension to the U.S. ICT supply chain cyber intelligence should be leveraged as part of an interdisciplinary methodology necessary to develop a holistic approach to meet this challenge.

Intelligence is a product that meets a specialized objective. By merging cyber intelligence as part of the supply chain security apparatus the collection and analysis of intelligence informs capabilities at an operational level. Gathered information given context and direction has strategic relevance and provides support by creating a window of time for building capabilities as well as assessing the technical direction, vector approaches, focus and vulnerabilities of adversaries. As neither supply chain nor cyber security professionals are trained in the requisite skill set for cyber intelligence that is not fully in line with their scope of responsibilities a new corps of experts needs to be developed as intelligence support for them. By provisioning a distinct appointment dedicated to cyber intelligence it maintains secure, effective and efficient operations and prevents the erosion of performance and capability of supply chain risk managers and cyber security personnel. By focusing the spotlight on lower tier suppliers providing ICT COT's component parts and raw materials cyber intelligence is uniquely qualified to help close the security gap on cyber threats to the supply chain.

References

Austin, E. (2013, June 6). US Weapons Systems Compromised by Chinese Spies. Retrieved February 26, 2014, from http://oneworldlabs.com/2013/06/us-weapons-systems-compromised-by-chinese-spies/

Chinese Counterfeit Goods in US Military Supply Chain – Part II | Top Secret Writers. (2012, July 3). Retrieved February 19, 2014, from http://www.topsecretwriters.com/2012/07/chinese-counterfeit-goods-in-us-military-supply-chain-part-ii/

The company that spooked the world. (2012, August 04). Retrieved January 15, 2014, from http://www.economist.com/node/21559929

CrossTalk -The Journal of Defense Software Engineering. (2014). *Mitigating Risks of Counterfeit and Tainted Components, 27*(2). Retrieved January 20, 2014, from http://www.crosstalkonline.org/storage/issue-archives/2014/201403/201403-0-Issue.pdf

Cyber Intelligence: Setting the landscape for an emerging discipline. (2011, September). Retrieved January 12, 2014, from https://www.insaonline.org/i/d/a/Resources/Cyber_Intelligence.aspx

Dealing with Today's Asymmetric Threat: Cyber Threats to National Security, Countering Challenges to the Global Supply Chain. (2010, June). Retrieved February 12, 2014, from http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf

DeAngelis, S. (2013, October 1). Cyber Security: A Growing Risk to Supply Chains. Retrieved January 15, 2014, from http://www.enterrasolutions.com/2013/10/cyber-security-a-growing-risk-to-supply-chains-2.html

Dugun, G. (2013, October 1). Businesses warned over cyber threats to supply chains. Retrieved January 18, 2014, from http://www.supplymanagement.com/news/2013/businesses-warned-over-cyber-threats-to-supply-chains

Dunnigan, J. (2014, January 29). China Again Deploys The Rare Earth Weaponby James DunniganJanuary 29, 2014. Retrieved February 24, 2014, from http://www.strategypage.com/dls/articles/China-Again-Deploys-The-Rare-Earth-Weapon-1-29-2014.asp

Feakin, T. (2013, June). *Enter the Dragon: Understanding Chinese Intelligence Agencies Cyber Capabilities* (Issue brief). Retrieved February 5, 2014, from Australian Strategic Policy Institute website: http://msisac.cisecurity.org/webcast/2013-06/index.cfm

Filsinger, J., Fast, B., Wolf, D. G., Payne, J. X., & Anderson, M. (n.d.). *Supply Chain Risk Management Awareness* (United States of America, Armed Forces Communication & Electronics Association, Cyber Committee). Retrieved March 10, 2014, from http://www.afcea.org/committees/cyber/documents/Supplychain.pdf

Garcia, T. (2013, November 18). Supply Chain Cyber Security: What Are The Risks And How Can Companies Address Them? Retrieved January 20, 2014, from http://www.manufacturing.net/articles/2013/11/supply-chain-cyber-security-what-are-the-risks-and-how-can-companies-address-them

Gore, L. (2013, May 28). Report: Multiple weapons systems with Huntsville ties compromised by Chinese hackers. Retrieved January 20, 2014, from http://blog.al.com/breaking/2013/05/report_multiple_weapons_system.html

Green, W. (2014, January 14). New institute to study the cyber attack threat to supply chains. Retrieved January 15, 2014, from http://www.supplymanagement.com/news/2014/new-institute-to-study-the-cyber-attack-threat-to-supply-chains

Higgins, K. J. (2013, May 29). Chinese Cyberspies Access U.S. Military Weapons System Designs. Retrieved January 20, 2014, from http://www.darkreading.com/attacks-breaches/chinese-cyberspies-access-us-military-we/240155699

Inserra, D., & Bucci, S. P., Ph.D. (2014, March 6). Cybersecurity Challenges and Cyber Supply Chain Security. Retrieved March 15, 2014, from http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace

Jackson, W. (2012, November 15). Supply chain threats 'hard to detect, expensive to fix' -- GCN. Retrieved January 13, 2014, from http://gcn.com/articles/2012/11/15/supply-chain-threats-hard-to-detect-expensive-to-fix.aspx

Kapersky Security Bulletin 2013. (n.d.). Retrieved http://media.kaspersky.com/pdf/KSB_2013_EN.pdf

Laird, R. (2013, September 9). Breaking Defense. Retrieved February 26, 2014, from http://breakingdefense.com/2013/09/us-needs-21st-century-arms-export-system-embrace-allies/

Los, R. (2012, August 22). False Flags, Geopolitics and Cyber Spies. Retrieved January 20, 2014, from http://www.infosecisland.com/blogview/22248-False-Flags-Geopolitics-and-Cyber-Spies.html

McGroarty, D. (2013, June 4). China: From Cyberwar to Supply Chain Sabotage? Retrieved January 20, 2014, from http://www.realclearworld.com/articles/2013/06/04/china_from_cyberwar_to_supply_chain_sabotage_105211.html

Metzger, R. S. (2014, February 17). Convergence of Counterfeit and Cyber Threats: Understanding New Rules on Supply Chain Risk. Retrieved March 5, 2014, from http://counterfeitparts.wordpress.com/2014/02/17/convergence-of-counterfeit-and-cyber-threats-understanding-new-rules-on-supply-chain-risk-robert-s-metzger/

Nakashima, E. (2013, May 28). Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies. Retrieved January 20, 2014, from http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html

Operational Levels of Cyber Intelligence. (2013, September). Retrieved January 20, 2014, from http://issuu.com/insalliance/docs/insa_wp_cyberintelligence_pages_hir/1?e=6126110/4715911

Paganini, P. (2013, March 1). Cyber-espionage: The Greatest Transfer of Wealth in History. Retrieved January 20, 2014, from http://hplusmagazine.com/2013/03/01/cyber-espionage-the-greatest-transfer-of-wealth-in-history/

Popick, P. R., & Reed, M. (n.d.). Requirements Challenges in Addressing Malicious Supply Chain Threats. Retrieved March 18, 2014, from http://www.acq.osd.mil/se/docs/ReqChallengesSCThreats-Reed-INCOSE-Vol16-Is2.pdf

Ragan, S. (2013, September 25). Espionage campaign targeting Asian supply chains uncovered. Retrieved January 21, 2014, from http://www.csoonline.com/article/740393/espionage-campaign-targeting-asian-supply-chains-uncovered

Rawnsley, A. (2011, June 22). Fishy Chips: Spies Want to Hack-Proof Circuits. Retrieved January 15, 2014, from http://www.wired.com/dangerroom/2011/06/chips-oy-spies-want-to-hack-proof-circuits/

Reed, J. (2012, May 30). Proof That Military Chips From China Are Infected? Retrieved February 26, 2014, from http://defensetech.org/2012/05/30/smoking-gun-proof-that-military-chips-from-china-are-infected/

Reporter, D. M. (2013, May 28). Plans for more than two dozen U.S. weapons systems - including an F35 fighter - have been stolen by Chinese hackers, claims Pentagon. Retrieved February 26, 2014, from http://www.dailymail.co.uk/news/article-2331949/More-dozen-U-S-weapons-systems-compromised-Chinese-hackers.html

Scissors, D. (2011, May 5). China and Cyber Security: Trojan Chips and US-Chinese Relations. Retrieved January 23, 2014, from http://www.heritage.org/research/reports/2011/05/china-and-cyber-security-trojan-chips-and-us-chinese-relations

SEI Emerging Technology Center: Cyber Intelligence Tradecraft Project (Rep.). (2013, January). Retrieved January 15, 2014, from Carnegie Mellon Software Engineering Institute website: http://www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key-findings.pdf

SEI Emerging Technology Center: Cyber Intelligence Tradecraft Project (Rep.). (2013, January). Retrieved January 15, 2014, from Carnegie Mellon Software Engineering Institute website: http://www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key-findings.pdf

Shalal, A. (2014, March 10). Exclusive: Chinese raw materials also found on U.S. B-1 bomber, F-16 jets. Retrieved March 15, 2014, from http://www.reuters.com/article/2014/03/10/us-usa-china-weapons-idUSBREA291UK20140310

Slate, R. (2009, January). Competing with Intelligence: New Directions in China's Quest for Intangible Property and Implications for Homeland Security. Retrieved January 20, 2014, from https://www.hsaj.org/?article=5.1.7

Toensmeier, P. (2013, November 13). Defense Department Installs Cyber Threat Reporting for its Supply Chain. Retrieved March 15, 2014, from http://www.thomasnet.com/journals/procurement/defense-department-installs-cyber-threat-reporting-for-its-supply-chain/