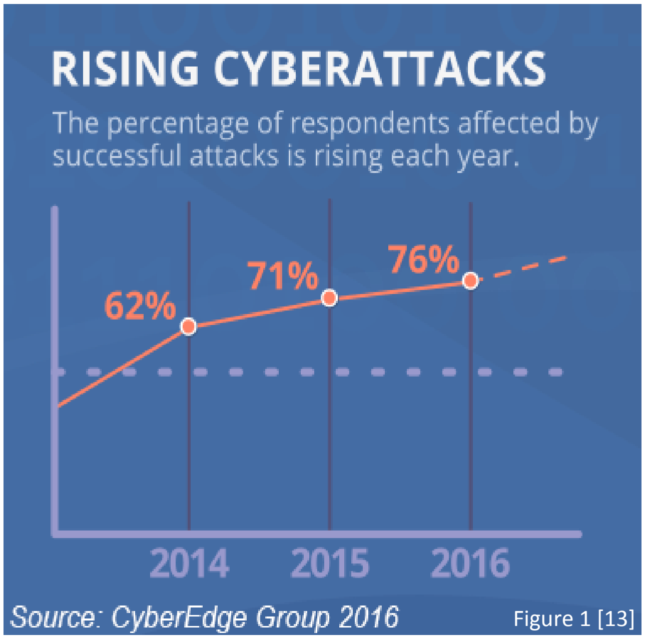
Published by Cyber Magazine, 04 September 2017,
http://magazine.milcyber.org/stories/buildingacadreofcyberintellectuals

Building a Cadre of Cyber Intellectuals

By Ray Mollison

Cyber-attacks are growing progressively and evolving rapidly each year which is making it harder to effectively combat cyber threats. One can best understand cyber-attacks through the applications of intelligence to learn "about the cyber adversaries and their methods combined with knowledge about an organization's security posture against those adversaries and their methods". [1] Cybersecurity has become a centralized topic of discussion in the government and business sectors where both sides are looking for solutions in a complex cyber world.



Source: CyberEdge Group 2016 Figure 1 [13]

Cyber Intelligence (CYBINT) is a marriage between the two disciplines of information technology and intelligence studies. Information technology is the study of creating, processing, storing, securing, and exchanging electronic data. [2] Intelligence is the study of credible and actionable information through collection, analysis and distribution. [3] Even though CYBINT is relatively infant as an intelligence discipline in academia and professional industries, Cyber Intelligence provides clarity to understand cybersecurity vulnerabilities, exploits, and threats. There is a good amount of analysis in information technology or "cyber" type roles using intelligence. [4]

Just like Clausewitz famously identified the three levels of war in his book "On War", the Cyber Intelligence Task Force from the Intelligence and National Security Alliance identified the same three parallel Levels of Cyber Intelligence: Strategic, Operational, and Tactical. [5] These Levels of Cyber Intelligence can help to acquire key information about U.S. adversaries' capabilities. The three levels are:

- Strategic Cyber Intelligence is to minimize risk to an organization's critical mission and assets of value by conducting assessments of threats and vulnerabilities. [6]
- Operational Cyber Intelligence facilitates analysis to determine the specific threat actors in order to reduce risks to critical information and intellectual property. [7]
- Tactical Cyber Intelligence contains the processes of examining priority requirements, collecting data, and developing actionable products. [8]

These Levels of Cyber Intelligence help to deter and neutralize threats through the process of analysis. It is important to note that *Joint Intelligence (JP 2-0)* publication is the baseline in providing fundamental principles and guidance to enhance the quality of tradecraft in intelligence to support joint operations. [9] This doctrine parallels the Levels of Cyber Intelligence which ensures all intelligence disciplines are crafted with the highest level expertise to minimize mistakes and maximize quality of results for the decision-maker.

The challenges of cyber are constant and it is vital to continuously gain knowledgeable insight to learn from past and present in order to improve future cyber operations. The Levels of Cyber Intelligence are to define and refine how information is collected through the lenses of data quantification in information technology. As shown in figure 2, the intelligence collection process in cyber must contain the "cycle of collection, analysis, dissemination, and feedback which must be *continuous*—not a periodic or intermittent—process." [10]

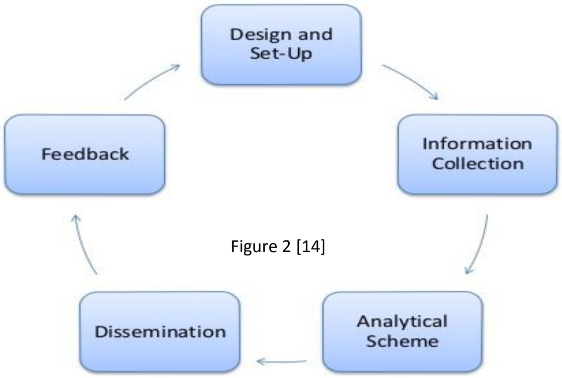


Figure 2 [14]

Filtering information on networks will strengthen the cybersecurity posture to be more proactive rather than reactive. Unfiltered information on networks will weaken the U.S. cybersecurity posture by making it more reactive versus proactive. Cyber Warfare conflicts range from political conflicts, espionage, and propaganda and the types of actors are nation-states, terrorists, and sociopolitical groups. [11] In Cyber Warfare, our adversaries' intentions are to attack our vulnerabilities which could degrade, disrupt and deny users' access, or destroy data, servers and networks, or steal personal identification information. The application of Cyber Intelligence is to gain knowledge of our adversaries by learning and studying their virtual footprint in cyber practices and methodologies.

Therefore, the levels of Cyber Intelligence play a role in filtering information to determine the reason of the attack, the intent of the conflict, and the type of malicious actors. Cyber Intelligence relies on fusing Human Intelligence (HUMINT) with timely and accurate Signal Intelligence (SIGINT) to respond to emerging and reemerging threats. [12] HUMINT, SIGINT, and CYBINT are inseparable disciplines and rely on each other together to collect information to achieve actionable and reliable intelligence in Cyber Warfare.

In conclusion, the cyber world will continue to be unstable; however, it can be stabilized by learning about adversaries' tactics, techniques, and procedures to maintain a superior cybersecurity posture at all three levels of Cyber Warfare – strategic, operational, and tactical. Cyber Intelligence can help build a stronger cybersecurity position by offering insightful knowledge to better defend against an adversarial cyber-attack.

About the Author

Ray Mollison is a field-grade officer in the Military Intelligence Readiness Command (MIRC) as an Army Reservist. He is pursuing his Master's degree in Cybersecurity at the University of South Florida. Ray enjoys working out and spending time with family.

[1] RSA. *Getting Ahead of Advanced Threats*. Jan. 2012. Web. <http://www.emc.com/collateral/industryoverview/ciso- rpt-2.pdf>
[2] Rouse, Margaret. *Information Technology*. TechTarget. Apr 2015. Web. <http://searchdatacenter.techtarget.com/definition/IT>
[3] Duverge, Gabe. *Intelligence Studies vs Criminal Justice*. POINT PARK University. Mar 2015. Web. <http://online.pointpark.edu/intelligence/intelligence-studies-vs-criminal-justice/>
[4] TRIPWIRE. *An Introduction to Cyber Intelligence.* Jan. 2014. Web. <https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/>
[5] Bamford, George, John Felker, and Troy Mattern. *Operational Levels of Cyber Intelligence*. Cyber Intelligence Task Force, Intelligence and National Security Alliance (INSA) White Paper, 2013
[6] Dennesen, Kristen, Felker, John, Feyes, Tonya, and Kern, Sean. *Strategic Cyber Intelligence.* Cyber Intelligence Task Force, Intelligence and National Security Alliance (INSA) White Paper, 2014.
[7] Hengel, Steven, Kern, Sean, Limbago, Andrea. *Operational Cyber Intelligence*. Cyber Intelligence Task Force, Intelligence and National Security Alliance (INSA) White Papers. 2014
[8] Hancock, Geoff, Anthony, Christian, and Kaffenberger, Lincoln. *Tactical Cyber Intelligence*. Cyber Intelligence Task Force, Intelligence and National Security Alliance (INSA) White Papers. 2015
[9] Joint Publication JP 2-0. *Joint Intelligence*. Oct. 2013. Web. <http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf>
[10] Randy Borum, John Felker and Sean Kern. "Cyber Intelligence Operations: More than Just 1s &amp; 0s" *Proceedings of the Marine Safety and Security Council: The U.S. Coast Guard Journal of Safety and Security at Sea* Vol. 71 Iss. 4 (2014)
[11] Sanjay Goel. Communications of the ACM. *Cyberwarfare: Connecting the Dots in Cyber Intelligence*. VOL 54. No. 8. Aug. 2011. Pg 132.
[12] "What is Cyber Threat Intelligence and why do I need it?". *iSIGHTPARTNERS*. 2014.
[13] "62% OF INFORMATION SECURITY PROS EXPECT BREACH IN 2016 – AND THEY MAY BE TOO OPTIMISTIC". *Ikanow Editorial*. Feb. 23, 2016. <http://www.ikanow.com/62-percent-information-security-pros-expect-breach-2016/>
[14] Ezendu, Elijah. "Competitive Intelligence". *Slideshare*. Jan. 2, 2010. <https://www.slideshare.net/ezendu/competitive-intelligence-2814940>