The Assumption of Employing Ethically Sound and Trusted Agents for the Future of Cyber Capabilities Must be Challenged

by Timothy Middleton

In a speech to the Association of the U.S. Army in October 2016, GEN Mark A. Milley, Chief of Staff of the Army, directs leaders to challenge every assumption[1]. An area that the U.S. Army needs focus on is the recruitment of candidates who are not security threats for the new Cyber Command. The assumption that those individuals recruited are worthy of trust with the U.S. Army's system should be challenged. In fact, the working assumption should be that these new recruits are the critical vulnerability of the system. If the newest members of the U.S. Army are the system's weakness, we should approach this challenge as an ethical problem instead of assuming those that show up have the nation's best interest at heart.

When Admiral William A. Owens was the Vice Chairman of the Joints Chief of Staff, he wrote a paper about a new revolution in military affairs.[2] He describes a "system of systems" that will help commanders lift the fog of war. In the pursuit of advanced technology, the modern U.S. Army is living this reality and it has come with inherent issues. The primary one is that technology usage has been the realm of a younger generation. The old guard, well versed in the technologies of a simpler time, appear to assume those who show up to serve are best suited to handle the security issues accompanying the latest advancements. ADM Owens mentions those doing the work and defines them as people working hard to realize the future who are "far from ignorant of the danger of inherent flaws."[3] He expounded on this idea for the private sector in a 2012 TED talk by outlining the number of folks trustworthy to use this technology as 10,000 individuals.[4] It is possible to arrive at the 10,000 individuals, but these Soldiers need to be recruited, selected, and trained. We should not assume that their presence in a recruiting station or merely holding a security clearance warrants trust.

Before giving an in-depth explanation of the ethical dilemma posed by the tech savvy recruits of today, it is worth offering examples that challenge the idea that individuals are "far from ignorant of the danger of inherent flaws" that handle the U.S. Army's system. The easiest example to highlight from a U.S. Army standpoint is Chelsea Manning's document dump to WikiLeaks.[5] The courts handed down a sentence that was commuted by an outgoing U.S. President.[6] Right, wrong, or indifferent; the Soldier was the weakness of the system. The process or system that investigated this Soldier's background, in a rush to employ a tech savvy individual, also cleared the way for access to potentially damaging items. This Soldier's military occupational specialty was 35F, intelligence analyst.[7] In eras gone by, someone with a lack of computer and technological awareness could be trained. Today, this specialty requires some level of specific knowledge or the products needed to build the intelligence preparation of the battlefield will be meager. This Soldier was tried in court and sentenced, but the damage was done. The result for the U.S. Army's system was upgrading security protocols and various other features, such as eliminating the use of portable memory or "thumb" drives. The information in U.S. diplomatic cables, video on air strikes, and disposition of detainees at Guantanamo has been published and the political fallout weathered, but was the system safe again? No, it was not safe. Manning handed WikiLeaks the data and it was released starting early in 2010.[8] By 2013 another "far from ignorant of the danger of inherent flaws" individual was busy downloading more damaging data.

Eric Snowden was not a U.S. Soldier when he violated the law, but his example is still important. Snowden did try to enter military service with the U.S. Army in the Special Forces as part of the 18x program.[9] He did not stay in the U.S. Army an entire year. What is important to note about Snowden is his skills as a recognized expert in computer security.[10] Snowden had access to significantly higher levels of data than a Soldier would need but he violated national trust and used WikiLeaks to disseminate classified information and programs. He lists no formal computer training, but held positions with the Central Intelligence Agency and Dell.[11] He has been formally charged and is currently somewhere in Russia on a temporary asylum visa. Snowden's impact has been so formidable to U.S. intelligence that companies were forced to upgrade software and operating systems based on revelations in the information he released.[12] Snowden was not the last person to release classified U.S. data.

Vault 7 is the latest data dump of material classified by the U.S.[13] The information was also released to WikiLeaks and the impact of this new leak has yet to be felt. What is significant about the data dump is the Central Intelligence Agency and the U.S. President have made rare public comments about it.[14] This is not usually the case. Since the data dump appears to be authentic, a closer examination of the items is needed for a complete picture of this ethical dilemma. According to news agencies reporting on the data dump, the focus of the information is on the intelligence communities' offensive capabilities in the cyber realm.[15] Offense is the specific domain of the U.S. Army. Whether these tools are in the hands of Soldiers is not clear, but it would make sense that some type of cyber-attack would precede a high intensity conflict and this capability release authority does not currently reside with the combatant commanders. There has been speculation about the identity of the individual who released the data, and that person has been dubbed Snowden 2.0, by the world press.[16]

Chelsea Manning, Eric Snowden, and Vault 7; why are these important? The U.S. public has shown two points of view on the topic, one they are "whistleblowers" and heroes who deserve protection,[17] and two, traitors who should be punished.[18] Neither of these can be impacted by U.S. Army policy, and even in the case of Chelsea Manning the U.S. Army courts have had their say. The real take away from this should be twofold. One, the vetting process for U.S. Army cyber warriors needs to be wide-ranging and exhaustive. Two, the overall impact of one individual is enormously damaging. In the case of infantrymen, artillerymen, and armored forces, one individual does not impact national policy, but a single cyber warrior can expose the application of doctrine and tools needed to accomplish U.S. Army objectives. Here lies the critical vulnerability of the cyber community. Just these three data releases, ultimately these three individuals, have completely undermined the entire U.S. cyber operation. The monetary cost in damage has not even been calculated. Here is a thought about the money spent, if the Manning data dump spurred spending to secure systems it was undermined by the Snowden dump. The investment was completely wasted in a very short span of time. The release of the Vault 7 data alerted the nation's enemies on what to protect and forced U.S. planners back to the drawing board for new capabilities. The human cost and damage to U.S. international relations has taken an even higher hit.

When Manning released information, the cyber community responded by spending resources to institute new security rules that Snowden circumvented. Snowden's release of data required new resources to apply a new set of rules that the Vault 7 folks got around. In the past, security violators either benefitted monetarily from selling data or were helping a foreign government gain advantage over the U.S. No one individual or country seems helped by these three data breaches and anyone with an internet connection can access the information. These are no longer isolated incidents; it is a pattern.

Similar breaches have not occurred for the U.S. allies or enemies. There are no 24-hour news cycles dedicated to a Chinese or Russian defector who dumped all the intelligence gathering capabilities of these two countries, so this is uniquely an American issue. With this as the backdrop, it is now time to challenge ADM Owens' idea that individuals that are "far from ignorant of the danger of inherent flaws" and are

threats to running the U.S. Army "system of systems." ADM Owens provided the path to challenge his own assumption by outlining certain technologies that were open to "hacking."[19] This insider threat is more relevant than outsiders attempting to breach the system. ADM Owens also acknowledged that each system builds on others, in turn making the infrastructure harder to take down. In the case of the three data breaches, the entire Department of Defense relies upon these national security systems. Relying on the system to protect itself also needs to be challenged.

It is time to take a deeper look at considerations of why or what is driving this shift. Specific reasons may be hard to fathom but broad concepts have emerged and these can be examined for factors. The simplest concept may be embedded in the actual spread of technology itself, specifically for the youngest generation entering military service. For the newest cyber warriors, the ethical dilemma is based on community versus individual. As it applies to security technology, the world community is more important than the individual needs of the United States. Dr. Jack D. Kem's work on this subject provides a starting point for the discussion of the ethical dilemma of community versus the individual measured against the utilitarian base of what will produce the greatest good.[20] Since the community is more important than the individual, divulging the information will do the greater good. An argument can be made for the base being a principles approach as well, meaning if the information is released everyone else will change the rules and follow suit. However, the argument of the greater good is more important to the young recruits, rather than changing the system's rules. In the case of the new recruits, the greater good is not the United States, it's the larger worldwide community. They feel it is their personal responsibility to save the world.

If teachers ask these student (potential recruits) to make their lives more ecologically sustainable because the entire planet is counting on their actions, how can the intelligence community expect them to focus on just one country? The fact is that U.S. secrets are released with almost calendar like regularity by members of the same generation. The point of this is to juxtapose the current thinking that the U.S. Army is recruiting individuals who can be trusted with the "system of system" against the fact that most recruits today do not understand the need for international borders. For these newly recruited individuals it is an ethical dilemma, and the U.S. cyber warfare community is on the losing end of it. Ideally, students who show aptitude in the wide range of areas needed to be an effective cyber warrior will have acquired those attributes in multiple school activities. Many of the scholastic programs that afford deeper understanding in technology also require the student to participate in service projects that demonstrate long-term positive impact on the environment.[21] This global perspective diminishes a nationalist view required to maintain the U.S. Army's "system of systems".

In a 2016 Deloitte report about those born after 1982, 64% of people surveyed demonstrated no loyalty to the company where they were currently working.[22] Even those in senior positions were more likely to leave. Since only 17% of initial entry Soldiers remain on active duty past the primary commitment, this tracks with expectations. The problem with this for cyber security is that the more educated population tends to be mobile. Why is this important? It takes a long time to make an effective cyber warrior and investing in someone who does not think U.S. interest should needs protecting is dangerous.

How much time does it take to make a cyber warrior? In "Outliers: the story of success," Malcom Gladwell builds on earlier work and postulates the deeper meaning of the 10,000-hour rule.[23] For those unfamiliar, 10,000 hours of activity is needed to be considered an expert in a given task. Author Gladwell highlights Bill Gates of Microsoft as logging in the required 10,000 hours, building the needed technical background for his company's financial successes long before its founding. The individual who puts in the time has a chance at making a fortune. Balance money making with security and there does not seem to be a clear need for national borders. Computing is global. If a company uses a portal to sell goods or services, anyone in the world with an internet connection can view the products. The young student who logs the requisite number of hours learning new programing skills can write their own ticket at larger commercial companies.

This problem is so pervasive that companies are spending large sums of money to keep the visa application process free flowing.[24] Paying to hire a computer genius from India is cheaper than hiring an American with the same skills. Does the U.S. Army risk spending 10,000 hours on training someone that might leave to start the next internet company? This question must be asked for every innovation but the internet's commercial usage is not new, the military application of interconnectivity is still evolving. For the Army, the cart is in front of the horse and attracting a Bill Gates is highly improbable.

What is at the heart of this ethical dilemma is a cultural change. One the cyber community has fully embraced, but not the cyber security community. This cultural change has made the planet flat, according to New York Times author Thomas L. Friedman. In his book "The World is Flat: A Brief History of the Twenty-First Century," he describes the technologies that created the commercial use of the internet, which was used by up to a third of the world's population in a short span of time.[25] The author's point is clear, people can effortlessly communicate across great distances. This communication has changed the face of business, how people choose to be governed, and how people view the planet itself. In addition to monitoring the status of the planet's health, these potential cyber warriors get to converse with other inhabitants of the earth, without a real understanding of the true separation. Whether the future cyber warrior is playing a first-person video game, on-line chatting about the environment, or updating social media it is likely the other members of the online forum are in other countries ranging from India to China. To add another layer, the future cyber warrior does not have to learn the respective languages, either software will automatically translate the conversation or the other members of the forum will speak English. It becomes clear that the U.S. Army cyber warrior may actually be at odds with the commander's intent on a personal level and view the guidance as illegal.

This all adds up to clearly show that Soldiers recruited today will not view the U.S. as needing security in the way the U.S. Army needs its "system of systems" protected. Whether the view stems from a global perspective of community or one derived from commerce, the theme is the same. There is no need for borders. Manning and Snowden still view themselves as winning the war against secrecy. Time will tell what the motives are behind the Vault 7 breach, but the investigation is narrowed to contractors, the same title Eric Snowden had when he was discovered. This perspective is cultural, not isolated. According to the 2016 Deloitte report, the need to ensure the entire world is aware of all activities only exists in the generation born after 1982.[26] This generation came of age when the internet had already reached critical mass. They did not have to wait for it to mature in order to benefit. There is an inherent understanding that this generation comprehends all things computer but does not see the need to keep it private or secure. A "hacker" who posts a video on how to "undo" the security protocols, with little or no repercussion, follows almost every single technological advance by a corporation.

A watershed event for file sharing and what could be the groundwork of a community ethos occurred with the music industry. The destruction of the music industry's ability to control their product highlights this shared community value. Since file sharing has taken hold, no artist has seen profits from music on the level that were once possible. Today the industry subsists on licensing and live performances, not music sales, because of the cultural change of community sharing.[27] This cultural shift is bad for securing systems with technology and it creates windows for exploitation.

With these ethical dilemmas in mind, what is the answer? Is there a solution to ensuring the generation born after 1982 can be counted on to protect a cyber system? The Deloitte report also had a glimmer of hope. The key to this generation is "liking" their efforts.[28] On line activity that receives recognition elevates the author. In the case of cyber warriors, this will mean being reintroduced to actual Soldiering techniques that have lay dormant for the past decade or more. The recent attempts to create mentors is the fundamental way to stem the tide and prevent further loss of sensitive data. Current security protocols prevent one data area from bleeding over into another one, but it also separates personnel. This may be an effective method to

prevent spillage, but at this point the genie is out of the bottle. There is a sincere need for community among these individuals. This is not a call to put Soldiers in open bay barracks, however, the core training elements of that could build a positive view of their country. The net effect of instructing cyber protocols has been similar to teaching Ranger students to conduct a linear danger area crossing without posting security. The patrol leader would be receiving a "no-go" at the end of phase counseling.

With Ranger school as an idea, there is merit to isolating the potential trainees and conducting an assessment and selection process. The selection process should not mirror those currently in use, but should work more on creating community for the Soldiers not accustomed to it. It must be more intense than current initial entry training. If there is no groundwork in the U.S. Army, then the training circumstances used by the U.S. Navy to train sailors in submarine warfare is a good starting point. Before the detractors become entrenched in the "old ways" it may be worth pointing out that nuclear subs and cyber weapons have the same release authority, but one of them gets to run rampant and post sensitive information to WikiLeaks.

Nassim Taleb, noted Black Swan theorist, wrote "…science evolves from funeral to funeral."[28] If this is true of scientists, it is probably true of other ideas as well. ADM Owens set the idea that individuals that understood the inherent dangers of a system breach were working on solutions. The time will come that those Soldiers tasked with monitoring the system and attending to its upkeep will decide it is not worth the effort, or it is unethical. Once that vulnerability exists in the technological advantage it will cease to provide protection or benefit. This is not a call to abandon the pursuit of more advances; this is call to ensure those that present the greatest threat to the system receive the most encouragement to protect it.

Endnotes

1. Samuel Ezerzer, "U.S. Army's chief of staff; Warning to Enemies "'Russia', will defeat any foe in ground combat"." *YouTube* (October 05, 2016), https://www.youtube.com/watch?v=_6oNMlmmMuU (accessed May 29, 2017).

2. William A. Owens, "The emerging U.S. system-of-systems" Washington, D.C.: National Defense University, Institute for National Strategic Studies, 1996.

3. Owens, "The emerging U.S. system-of-systems". 3.

4. TEDxTalks. "The Future of Innovation: Admiral William A. Owens: TEDxMonroe.mp4." YouTube. August 30, 2012. Accessed May 29, 2017. https://www.youtube.com/watch?v=DmUvUYqs_FA.

5. Tate, Julie. "Bradley Manning sentenced to 35 years in WikiLeaks case." The Washington Post. August 21, 2013. Accessed May 29, 2017. https://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html?utm_term=.93cc0d41c952.

6. Savage, Charlie. "Chelsea Manning to Be Released Early as Obama Commutes Sentence." The New York Times. January 17, 2017. Accessed May 29, 2017. https://www.nytimes.com/2017/01/17/us/politics/obama-commutes-bulk-of-chelsea-mannings-sentence.html?_r=0.

7. O'Brien, Alexa. "Bradley Manning's full statement." Salon. March 1, 2013. Accessed May 29, 2017. http://www.salon.com/2013/03/01/bradley_mannings_full_statement/.

8. Barnes, Julian E. "What Bradley Manning Leaked." The Wall Street Journal. August 21, 2013. Accessed May 29, 2017. https://blogs.wsj.com/washwire/2013/08/21/what-bradley-manning-leaked/.

9. Ackerman, Spencer. "Edward Snowden did enlist for special forces, US army confirms." The Guardian. June 10, 2013. Accessed May 29, 2017. https://www.theguardian.com/world/2013/jun/10/edward-snowden-army-special-forces.

10. Drew, Christopher, and Scott Shane. "Résumé Shows Snowden Honed Hacking Skills." The New York Times. July 04, 2013. Accessed May 29, 2017. http://www.nytimes.com/2013/07/05/us/resume-shows-snowden-honed-hacking-skills.html.

11. Drew, Christopher, and Scott Shane. "Résumé Shows Snowden Honed Hacking Skills."

12. Casino, Khier. "5 ways Edward Snowden has changed the world since NSA leaks." NY Daily News. October 01, 2015. Accessed May 29, 2017. http://www.nydailynews.com/news/world/5-ways-edward-snowden-impacted-world-nsa-leaks-article-1.2381980.

13. Burgess, Matt. "WikiLeaks drops 'Grasshopper' documents, part four of its CIA Vault 7 files." WIRED UK. April 07, 2017. Accessed May 29, 2017. http://www.wired.co.uk/article/cia-files-wikileaks-vault-7.

14. Borger, Julian. "To security establishment, WikiLeaks' CIA dump is part of US-Russia battle." The Guardian. March 07, 2017. Accessed May 29, 2017. https://www.theguardian.com/media/2017/mar/07/wikileaks-cia-documents-us-russia-conflict

15. Domonoske, Camila. "WikiLeaks Releases What It Calls CIA Trove Of Cyber-Espionage Documents." NPR. March 07, 2017. Accessed May 29, 2017. http://www.npr.org/sections/thetwo-way/2017/03/07/519010317/wikileaks-releases-what-it-calls-cia-trove-of-cyberespionage-documents.

16. Cuthbertson, Anthony. "Who was behind WikiLeaks Vault 7 Leak-an insider, a hacker or Russia?"

Newsweek. March 14, 2017. Accessed May 29, 2017. http://www.newsweek.com/who-cia-vault-7-wikileaks-dump-russia-insider-contractor-565296.

17. Žižek, Slavoj. "Edward Snowden, Chelsea Manning and Julian Assange: our new heroes | Slavoj Žižek." The Guardian. September 03, 2013. Accessed May 29, 2017. https://www.theguardian.com/commentisfree/2013/sep/03/snowden-manning-assange-new-heroes.

18. Geraghty, Jim. "Manning, Assange, Snowden: These Are Not the Good Guys." National Review. January 18, 2017. Accessed May 29, 2017. http://www.nationalreview.com/corner/443953/manning-assange-snowden-these-are-not-good-guys.

19. Owens, "The emerging U.S. system-of-systems"., 3.

20. United States. Combined Arms Center. Command and General Staff Officer Course. Ethical Decision Making: Using the "Ethical Triangle". By Dr. Jack D. Kem. Fort Leavenworth, KANSAS: CAC. 1-12.

21. "Community Service Idea Starters | NHS." National Honor Society & National Junior Honor Society. Accessed May 29, 2017. https://www.nhs.us/hyfn/honor-your-future-now/community-service-idea-starters.

22. "Millennial Survey 2017 | Deloitte | Social impact, Innovation." Deloitte. April 27, 2017. Accessed May 29, 2017. https://www2.deloitte.com/global/en/pages/about-deloitte/articles/millennialsurvey.html.

23. Gladwell, Malcolm. Outliers: the story of success. New York: Back Bay Books, Little, Brown and Company, 2008.

24. Schouten, Fredreka, and Alan Gomez. "Tech companies driving the lobbying on immigration." USA Today. April 29, 2013. Accessed May 29, 2017. https://www.usatoday.com/story/news/nation/2013/04/29/tech-companies-lobbying-immigration-facebook-family-visas/2121179/.

25. Friedman, Thomas L. The world is flat: a brief history of the twenty-first century. Bridgewater, NJ: Distributed by Paw Prints/Baker & Taylor, 2009.

26. Deloitte., "Millennial Survey 2017 | Deloitte | Social impact, Innovation."

27. "Music Industry Revenue In 2016." Careers In Music | Music Schools & Colleges. January 03, 2017. Accessed May 29, 2017. https://www.careersinmusic.com/music-industry-revenue.

28. Taleb, Nassim Nicholas. Fooled by randomness: the hidden role of chance in life and in the markets. London: Penguin, 2013.