Command and General Staff Officer College

2017 Ethics Symposium

The assumption of employing ethically sound and trusted agents for the future of cyber capabilities must be challenged

By

MAJ Timothy Middleton
Staff Group 17B

29 March 2017

October 2016, in a speech to the Association of the US Army, GEN Mark A. Milley, Chief of Staff of the Army, directs leaders to challenge every assumption[1]. One of the sacred cows that the US Army now struggles with is the recruitment of candidates, that are not security threats, for the new Cyber Command. The assumption that those individuals recruited are worthy of trust with the US 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 US Army are also the most tech savvy, and 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.

Admiral William A. Owens, while Vice Chairman of the Joints Chief of Staff 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 US Army is living this reality. This has come with inherent issues. The primary one being that technology usage has been the realm of a younger generation. The old guard well versed in the technologies of a simpler time have assumed those that show up to serve are best suited to handle the security issues accompanying the latest advancements. ADM Owens mentions those doing the work as well, he defines the group that is working hard to realize the future as individuals who are "far from ignorant of the danger of inherent flaws"[3]. He has expounded on this idea further in a TED talk in 2012, outlining the number of these "far from ignorant of the danger of inherent flaws" 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 and not assumed that their presence in a recruiting station and 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 US Army's system. The easiest example to highlight from a US Army standpoint is Chelsea Manning's document dump to WikiLeaks[5]. The courts handed down a sentence that was commuted by an outgoing US President[6]. Right, wrong, or indifferent the Soldier was the weakness of the system. The process or system that investigated this Soldier's background also cleared the way for access to potentially damaging items in a rush to employ a tech savvy individual. This Soldier's MOS 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 discovered, tried in court, and sentenced, but the damage had already been done. The result on the US Army's system has been upgrading security protocols and various other features, such as eliminating the use of portable memory or "thumb" drives. The information in US Diplomatic cables, video on air strikes and disposition of detainees at Guantanamo has been published and the political fallout has been weathered, but is the system safe again? No, 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 US Soldier when he violated the law, but his example is still important. Snowden did try to enter military service with the US Army in the Special Forces, as part of the 18x program[9]. He did not stay in the US 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 also 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 US 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 US data.

Vault 7 is the latest data dump of data classified by the US[13]. The information was also released on WikiLeaks and the impact of this new leak has yet to be felt. What is significant about the data dump so far, is the Central Intelligence Agency and the US 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 US Army. Whether these tools are in the hands of Soldiers is not clear, but it would stand to reason that a high intensity conflict would be preceded by some type of cyber-attack 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, 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 US 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 US Army policy, and even in the case of Chelsea Manning the US Army courts

have had their say. The real take away from this should be twofold. One the vetting process for US Army cyber warriors needs to be wide-ranging and exhaustive and 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 US Army objectives. In this lies the critical vulnerability of the cyber community. Just these three data releases, ultimately these three individuals, have completely undermined the entire US 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 and in a very short span of time. The release of the Vault 7 data has alerted the nation's enemies on what to protect and forced US planners back to the drawing board for new capabilities. The human cost and damage to US international relations has taken an even higher hit.

So, to be clear, Manning released information, the cyber community responds by spending resources to institute new security rules that Snowden circumvented. Snowden's release of data requires new resources to apply a new set 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 US. No one individual or country seems to be 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 by the US 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 back drop, 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 US 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, these are national security systems that the entire Department of Defense relies upon. So, 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, those that are just reaching military age and entering the US Army, 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. Kem's work on this subject can also be explored by 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 then 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 potential recruits, while they are still students, 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 answer is clear with the fact that US secrets are released, with almost calendar like regularity, by members of the same generation. This is not a formal accusation of the current education system or the desire to clarify anyone's understanding of environmental factors. The point of this is to juxtapose current thinking, that the US 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 that the US cyber warfare community is on the losing end of. 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, ideal studies for the future cyber warrior, 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 US Army's "system of systems".

In a 2016 Deloitte report about those born after 1982, 64% 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, 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 US interest should needs protecting is dangerous.

How much time does it take to make a cyber warrior? In "Outliers", 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, playing music, programming computers, etc. 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 10,000-hour rule has been widely accepted and demonstrates an even more difficult obstacle to overcome. The individual who puts the time in, has a shot at making a fortune. Balance money making with security, and again 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, to keep the visa application process free flowing[24]. Paying to settle a computer genius from India is cheaper than hiring an American with the same skills. Does the US 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 new innovation, but the internet's commercial usage is not new, the military application of interconnectivity is still evolving. So, 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 titled "The World is Flat: A Brief History of the Twenty-First Century", he describes the technologies that created the commercial use of the internet, by up to a third of the world's population in a short span a time[25]. While the author's point was not of a physical nature, the impact 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 being asked to monitor 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. Couple these facts together and it becomes clear that the US 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 US as needing security in the way the US 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 inherent in understanding that this generation comprehends all things computer, but does not see the need to keep it private or secure. Almost every single technological advance by a corporation is followed by a "hacker" who posts a video on how to "undo" the security protocols, with little or no repercussion. It is bad for the corporate's image to be seen coming down on a single individual. Even if the individual downloads thousands of songs and movies with illegal file sharing technology.

A watershed event for the widespread use of file sharing and what could be the groundwork of a community ethos occurred with the music industry. The distribution and 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 actually train in protecting a cyber system and its safeguards? 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 plus. 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, so that more data does not find its way to willing distributors, 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 so far 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 being used, it should work more on creating community for the Soldiers not accustomed to it. The day to day social programing of isolation with individuals who have shared experiences will go a long way to close the gap. It must be more intense than current initial entry training. If there is no groundwork in the US Army, then the training circumstances used by the US 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 smaller ideas as well. ADM Owens set down the idea that individuals that understood the inherent dangers of a system breach were working on solutions. 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.