Combat Readiness through Cyber Resilience

Asserting our presence

by Maj Jason R. Shockey

The Marine Corps is over-reliant on command and control (C^2) systems, not through a fault in judgment, but rather through the rapid technological evolution of the Internet and the requirement to become digital. The upside to technological evolution is efficient sharing of resources; the downside is an over-reliance on information technology (IT) and C^2 systems. Being critically dependent on IT systems creates vulnerabilities that must be acknowledged, understood, and mitigated to within acceptable risk tolerances. Cyber resilience is the ability of an organization to continue to operate in a degraded IT environment while maintaining operational capabilities and recover to an effective operational posture in a time frame consistent with mission needs.[1] Plainly stated, cyber resilience is the ability for Marines to fight and win battles in a degraded C^2 environment. The USMC can mitigate its over-reliance on C^2 systems vulnerability by increasing combat readiness through cyber resilience.

Units can measure cyber resilience by how long mission essential functions (MEFs) can continue when C^2 systems, computers, phones, and the Internet are degraded or unavailable. Some individuals and units can withstand impact to their IT systems for longer than others, but all units' mission productivity will be negatively impacted to some degree. High, moderate, and low operational impact indicates cyber resilience on the sliding scale from cyber rigidity to cyber resilience. Cyber rigidity is the inability to perform MEFs in a C^2-contested environment. So if a slight disruption to C^2 systems produces a high impact to MEFs, this indicates cyber rigidity. Severe disruption that produces low impact and continued MEFs indicates cyber resiliency. Cyber rigidity impacts

>Maj Shockey is an 0602 communications officer currently serving as the G-6 (Communications) Operations Officer, 3d MarDiv. He deployed in support of Operation Enduring Freedom to Combined Joint Task Force 76 from April to November 2004. He is a Certified Information Systems Security Professional (CISSP), has graduated from U.S. Strategic Command's Joint Network Attack Course (JNAC), the DOD Cyber Crimes Center (DC3) Cyber Analyst Course, and the DC3 Online Undercover Techniques course. Major Shockey is also a recipient of the 2014 Copernicus Award from AFCEA and the U.S. Naval Institute.

Mission essential functions are only available if they keep C^2 systems operating. *(Photo by Sgt Christopher O'Quin.)*

the mission, decreases overall combat readiness, and leads to increased risk to the Marine Corps' ability to contribute to the national security strategy. To be resilient to cyber disruption, efficiently fight in degraded C^2 environments, and return to a normal operational state in a timely manner to continue the fight, the Marine Corps must increase its cyber resilience. Currently, Marine Corps personnel and equipment are not as cyber resilient as they need to be and, therefore, cannot realize their full combat readiness potential. Combat readiness can be increased with cyber resilience through equipment hardening, personnel education, and developing a culture of innovation.

Equipment Hardening

C^2 systems and networked devices go through the stages of the system development life cycle that manage devices from initiation, assembly, shipping, and disposal. As Marines and United States citizens, we blindly trust that our C^2 systems and networked devices are secure and free of malware. Hackers, however, are constantly varying attack vectors to achieve maximum effects with minimal effort. An inexpensive and effective way to produce effects is to hack our systems before the devices are assembled, shipped, and used. Globalization has pushed the manufacturing of computer components to the outer edges of earth where the IT devices, when fully assembled and in the Marine Corps' hands, have gone through the global IT supply chain. In other words, hackers affect the Marine Corps mission when our systems are out of our positive control and in the highly vulnerable global IT supply chain.

The system development life cycle and global IT supply chain are intimately linked. At any stage in the global IT supply chain, hackers can implant malware on systems to allow unauthorized, undetected access to sensitive systems. The equivalent physical world vulnerability to hackers attacking the global IT supply chain to gain unauthorized, undetected access is having no security guards, unlocked doors, and open windows in Marine Corps buildings. With persistent access in place, the hackers can then access the affected systems through those back doors from anywhere in the world at any time they choose. Hackers are extremely good at hiding the presence of malware behind the systems and applications we routinely use. In the background, while we are using systems, the hacker's malware perform illegitimate operations that undermine security and send undetected, encrypted data to the hacker. This information could be common operational picture (COP) information, blue force tracker track data, and emails.

Our current defense procurement framework follows the globally accepted standard system development life cycle process and forces our C^2 systems through today's globally interconnected IT supply chain. This framework produces unquantified risk because the process forces the DOD to accept unknown, unmitigated risk with insecure systems that have gone through the global IT chain. A U.S. controlled supply chain would provide increased assurance of a secure device free from advanced persistent threats, but that supply chain is not sustainable in our current fiscally constrained environment. The global IT supply chain security challenge is tangible and of great concern. So much so that the National Institute of Standards and Technology (NIST) published an unclassified interagency report in October 2012 on information and communication technology supply chain risk management (ICT SCRM) to identify and mitigate the inherent risk residing in supply chains that support global IT products and services. Adoption of ICT SCRM into the Marine Corps acquisition and procurement cycle, its organizational culture, and combat readiness reporting will reveal previously unidentified risk to C^2 systems and provide a higher level of cyber resilience not previously realized in the Marine Corps.

The Office of the National Counterterrorism Executive (ONCIX) stated, "U.S. adversaries use the supply chain to simply and effectively insert counterfeit parts into products destined for the United States to gain access to sensitive systems and degrade the performance of U.S. systems."[2] In the current defense acquisition cycles following the "best-value continuum," there is a technique called lowest-price, technically acceptable, or LPTA. LPTA is a technique which, when acquiring equipment, "the best value is expected to result from selection of a technically acceptable proposal with the lowest evaluated price."[3] In other words, LPTA finds the lowest monetary price with the perceived best technical expectations to purchase and field to the Operating Forces but also fields unknown, unmitigated risk to the fleet. LPTA increases risk, decreases combat readiness, and should be immediately amended to reflect current secure acquisition practices.

A recommendation to increase the cyber resilience of the DOD's and Marine Corps' ICT SCRM and LPTA challenge is to participate in programs like the Defense Advanced Research Project's Agency (DARPA) Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program. DARPA announced SHIELD in February 2014 which currently "seeks a tool that authenticates electronic components at any step of the supply chain and will encrypt and transmit on-demand information about tampering of system components."[4] This DARPA-initiated tool would greatly increase cyber resilience and Marine Corps combat readiness.

Personnel Education

Today's cyber threat environment is complex and must be understood by all Marines in order to be combat ready. Therefore, cyber resilience must be acknowledged, instituted, and measured throughout the Marine Corps to ensure readiness. Education is the foundation for cyber resilience and leads to a more combat ready individual, unit, Marine Corps, and DOD. The Marine Corps can increase its combat readiness through cyber resilience by having an aware, educated, and incentivized workforce.

Cyber awareness for Marines occurs today through annual online cyber awareness training in MarineNet, an important tool attempting to explain today's complex, interdependent cyber environment. To fully understand these

complexities and interdependencies, an increased level of awareness is needed for combat arms and noncommunications combat service support Marines. A solution to enhance the present level of cyber awareness training in MarineNet is to provide real-world examples of cyberattacks. These new examples should be video-based, highlight recent attacks, and show the effects on DOD and civilian computer networks. Historical vignettes are effectively used in annual DOD antiterrorism training and their use in the cyber awareness would move the cyber awareness program forward from the present "this will never happen to me" type of training to "this recently happened to people just like you and these were the effects."

Improving the USMC 06XX cyber education from entry-level school through the end of a Marine's career would significantly increase cyber resilience. The Marine Corps needs to create an information security program for qualified personnel to further enhance and professionalize the Marine Corps cyber workforce and tie that information security program to pay and promotion. Such an information security program currently exists—the Naval Postgraduate School Center for Information Systems Security Studies and Research (NPS CISR). NPS CISR is the pipeline to create the USMC cybersecurity professionals desperately needed to lead, influence, and increase cyber resilience from the lowest levels to the Commandant of the Marine Corps. As compared to the Marine Corps, the U.S. Navy, Army, and Air Force send many more of their personnel to academic institutions to grow their cyber forces and systemically integrate cyber resilience into their Service cultures. The actions and commitment to excellence of the other Services have increased their cyber resilience and those Services are more combat ready than the Marine Corps to fight and win battles in the cyberspace domain—a domain in which all Services must fight. A recommended solution to increase the lack of a professionalized USMC information security workforce is to open attendance to NPS CISR to a wider audience and include the 0602, 0620, and 0650 occupational fields. Widening the pool to attend NPS CISR will increase the number of graduates, expand the Marine Corps body of knowledge, and align the Marine Corps with the DOD's overall cyber workforce growth and continuous cyber workforce improvement. Implementing these recommended solutions would move the USMC from rhetoric to action and align those actions to MARADMIN 362/14, released 24 July 2014, which stated, "the Marine Corps is investing heavily to increase cyberspace and electronic warfare expertise and capacity."[5]

We have the equipment, now we need to develop an effective information security program. ***(Photo by Sgt Christopher O'Quin.)***

Marines are much more likely to stay Marine if properly incentivized. Incentives such as emotion and money vary with personal needs and motivation. The information security educational pipeline will give Marines highly marketable education, certified skills, and unparalleled experience that directly translates to the civilian sector and higher pay. That talent can be retained by the Marine Corps through proper incentives. The quickest and most efficient way to retain these cyber forces is by tying the information security education and certification to incentive pay, bonus, and promotion. Monetary incentives have a proven history in aviation, special operations, medical, and foreign language programs in the form of flight pay, jump pay, specialization pay, and foreign language proficiency bonuses. These same monetary incentive models should be instituted by the Marine Corps to retain the needed cyber talent and drive combat readiness through cyber resilience.

A very efficient way for the Marine Corps to properly acknowledge and understand cyber is for the Commandant to create a new professional category on the Commandant's Professional Reading List (CPRL), the Cyber Professional Reading Category. The CPRL currently has professional reading categories to further professionalize certain areas deemed important to the Marine Corps such as logistics, aviation, and maneuver warfare. All modern militaries must fight in the cyber domain; however, there is a glaring void of a USMC cyber reading category. This void sends a clear message to the Marine Corps, DOD, and the world that cyber is not a significant consideration for the Marine Corps. In order for the Marine Corps to retain its competitive advantage in future conflict, the Corps must increase its cyber understanding. It's time to create a cyber professional reading category on the CPRL. Suggested books for the CPRL's cyber professional cyber reading category that are aligned

with United States Strategic Command and United States Cyber Command include: the *Hacking Exposed* series by Stuart McClure, Joel Scambray, and George Kurtz; *Cyber War: The next threat to National Security and what to do about it* by Richard Clarke and Robert Knake; *Fatal System Error: The Hunt for the New Crime Lords Who are Bringing Down the Internet* by Joseph Menn; and *Geekonomics: The Real Cost of Insecure Software* by David Rice.

Culture of Innovation

History indicates that successful innovation during the interwar period depends on "long term decisions that affect the culture and values of the officer corps."[6] Furthermore, successful innovation in military organizations depends on "specificity and military culture" where specificity will find a specific solution to a military problem that "offers significant advantages to furthering the achievement of national strategy."[7] Military culture can "best be described as the sum of the intellectual, professional, and traditional values of the officer corps" where the culture "plays a crucial role in how military forces prepare themselves for combat."[8] Future combat will include cyber. The Marine Corps needs to acknowledge and accept that fact. Without a fully aware, more formally educated, and more certified information security workforce, the Marines Corps is currently postured to always be a customer of cyber. Therefore, the Marine Corps needs to incorporate cyber resilience into its officer corps appropriately through venues like NPS CISR, civilian certifications, cyber incentive pay, and the CPRL cyber professional reading category to ensure the Marine Corps stays relevant in the future fight and is not left sidelined by the more appropriately prepared and positioned Services.

The Marine Corps has a culture of innovation that has yet to include cyber into its exclusive, innovative gun club. The Marine Corps desperately needs to include cyber because history has trended that "innovation failed in military organizations that misused history to justify their current doctrine."[9] Existing doctrine blinds the Marine Corps from fully using cyber and cyber resilience to prepare for combat. History also indicates that military organizations failed to innovate when they were rigid, which led "organizations to shut off alternative paths that might ease the way for military operations."[10] Cyber resilience to achieve maximum combat readiness in the Marine Corps is that alternative path yet undiscovered. The Marine Corps needs to pursue the available paths of today to ensure the Marine Corps has a foothold in the battles of tomorrow.

The MAGTF provides a balanced team of ground, air, and logistics assets under a central command that is self-sustained and provides combined arms forces to conduct the full range of operations. MAGTFs recently added to their structure the cyberspace and electronic warfare coordination cell (CEWCC). "The CEWCC coordinates the integrated planning, execution and assessment of cyberspace and Electromagnetic Spectrum actions across the MAGTF's operational environment in order to increase operational tempo and achieve advantage."[11] The CEWCC is a good, innovative first step for the Marine Corps to conduct operations in the cyberspace domain. There is, however, residual risk in Marine Corps networks and systems where CEWCCs are not, and this is where hackers achieve effects. To properly secure the Marine Corps, CEWCC-like capabilities need to be placed in both the operational forces and in the remaining nondeployable Marine Corps areas, garrison, and the fifth element of the MAGTF. The partial implementation of the CEWCC capability in a very thin slice of the Marine Corps puts the MAGTF at a disadvantage when conducting operations because of the residual risk in the interconnected C^2 networks that reside in the non-CEWCC enabled areas which allow hackers to attack the gaps and avoid surfaces.

The DOD fiscal year 2015 budget request cited, in order to maintain readiness levels, the DOD "recognizes evolving critical demands like cyber, will guard against erosion of organic skills, and overreliance on contracted services."[12] To properly strengthen cyber skills, guard against erosion of critical cyber skills, and mitigate the existing systemic vulnerability of over-reliance on C^2 systems, the Marine Corps can make every Marine more cyber aware, certified, enhance educational opportunities, and retain top talent. These innovative programs will only serve to acquire, retain, and improve cyber talent and cyber resilience leading to combat readiness. Additionally, having this cyber capability would allow the Marine Corps to effectively compete fiscally for DOD cyber dollars and survive being sidelined by the other Services in future conflict. In order for the Marine Corps to observe historical lessons, successfully innovate "during the interwar period to affect the Marine Corps culture and values," to stay relevant in future warfare, and be able to contribute to the national strategy the Marine Corps must assert its presence in the cyberspace domain. The Marine Corps presence in cyberspace must be asserted, not assumed. The Marine Corps must never put itself in the position to be a customer of cyber because the Marine Corps is America's 9-1-1 middleweight force and must therefore be dominant as a MAGTF in all warfighting domains. This cyber presence must be an assertion from the Marine Corps that we are capable and talented to employ the MAGTF to fight tonight and win. Implementing these innovative ideas will round out the vital missing pieces of the MAGTF including bases, posts, and station to ensure the Marine Corps has a place on the battlefield in future wars.

Conclusion

Hardening equipment, educating Marines, and developing an innovative culture are the paths to cyber resilience that will maximize combat readiness in the Marine Corps. The Marine Corps of today, if called to perform its middleweight duties needs to have the requisite, sustained, in-house cyber capability needed for today's and tomorrow's battles. The Marine Corps needs to quickly fill its cyber gap by applying a formal, top down, aggressive approach to ensure the Marine Corps is not sidelined out of future battles

by the other Services or worse, fail to defend the United States. Marines do not fail; they adapt and overcome. It's time for the Marine Corps to adapt to cyber, increase combat readiness, and properly confront future battles. *Cyber resilience—not cyber reliance—will achieve the proper level of combat readiness to again prove that the Marine Corps is the vital, relevant force in future conflict as it has always been for the American people*. "The Marine Corps needs to be willing to adapt to new requirements and organize and train how we claim we will fight. As a Corps we need to commit ourselves to make this decision if we wish to remain relevant while other Services transform."[13]

Notes

1. National Institute of Standards and Technology, *Special Publication 34, Revision 1, Contingency Planning for Federal Information Systems*, (Washington, DC: 2010). National Institute of Standards and Technology, *Special Publication 800-53, Recommended Security Control for Federal Information Systems and Organizations*, (Washington, DC: 30 April 2013).

2. Office of the National Counterintelligence Executive (ONICX), *Supply Chain Threats*, (Washington, DC: 2012), accessed at http://www.ncix.gov.

3. Office of the Secretary of Defense Memorandum, *Department of Defense Source Selection Procedures*, (Washington, DC: 4 March 2011).

4. Defense Advanced Research Projects Agency (DARPA), "DARPA Targets Counterfeit Electronics," *Information Week Government*, (Washington, DC: 25 February 2014).

5. Marine Administrative Message 362/12 (MARADMIN 362/12), MAGTF Cyberspace and Electronic Warfare Coordination Cell (CEWCC) Concept, (Washington, DC: HQMC, 24 July 2014).

6. Williamson Murray and Allan R. Millet, *Military Innovation in the Interwar Period*, (New York: Cambridge University Press, 1998).

7. Ibid.

8. Ibid.

9. Ibid.

10. Ibid.

11. MARADMIN 362/12.

12. Department of Defense, *Department of Defense Fiscal Year 2015 Budget Request*, (Washington, DC: March 2014).

13. LtCols A.A. Khan, M.B. West, and Maj M.H. Brown, "Let's Organize and Train As We Would Fight," *Marine Corps Gazette*, (Quantico, VA: October 2002).