Talent Management for Cyber Warfare

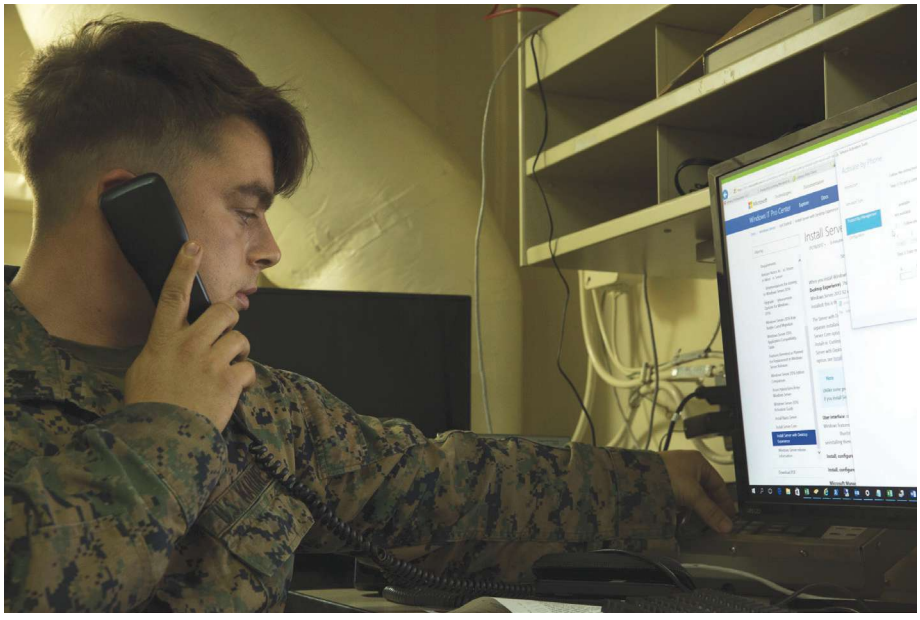
Maintaining the right workforce

by Capt Aric A. Ramsey

The means and methods the Marine Corps uses to fight its battles are rapidly changing. Each warfighting function is increasingly dependent on cyberspace for the speed and flexibility it generates through shortening the decision-making process and enabling more efficient prosecution of innumerable tasks. In its heavy reliance on digital data, the service is accepting highly targetable critical vulnerabilities in cyberspace, which are compounded by the Service's deep-rooted culture of making data available over keeping it secure. This system of systems, touted as a critical component of U.S. strength, has already become a fairly easy, low-cost, high-payoff target for our global competitors. Recent examples of U.S. government network vulnerabilities, such as the Office of Personnel Management breach of 21.5 million personal records or the penetration into the Joint Chiefs network, remind us that the threat of attack in and through cyberspace is real and underscores the inevitability of network compromise.[1] Thus our dependence on cyberspace, along with the struggle to keep up with potential adversaries in that domain, are subjects of much interest within the Department of Defense (DoD).[2] At the same time, the DoD faces problems maintaining a workforce of sufficient size and skill to support cyber operations, which fundamentally undermines efforts to operate effectively and securely in cyberspace. These manpower issues are well known and documented to some extent. Several years ago, the DOD published a cyberspace workforce strategy that identified the need for better recruiting, evaluation of skill maturity, and retention of qualified personnel—among other concerns.[3] The recommendations presented were generic and lacked realistic application, and the DOD still faces many of these same issues today. Unfortunately, the problem especially impacts the Marine Corps which lags behind its sister services in taking corrective action. The current Commandant is rightly interested in the Marine Corps' systemic talent retention problem, suggesting an incentives-based model that uses money like a focused weapon aimed exactly at the individuals we need.[4] The coming year will serve as a good indicator of whether his guidance will result in stemming the talent hemorrhage plaguing many specialized occupational fields. While not a panacea, making the cyber warfare community the first among such incentive-targets will close significant inequalities in pay and thereby remove one of the major considerations prompting young and qualified Marines to take the skills the Marine Corps has sacrificed to cultivate over to other uniformed services or the civilian workforce.

Cyber warfare is by nature a human-centric endeavor requiring highly trained and professional forces. The Marine Corps recognizes this and has made significant investment in the people it places in cyber warfare billets.

>Capt Ramsey is a Communications Officer serving as a Service cyber protection team leader attached to the Marine Corps Cyberspace Operations Group.



The methods used to fight in the future will require cyber operator skills. *(Photo by Cpl Victoria Decker.)*

As we enter into the nineteenth year of the U.S. Cyber Command force building effort, a large amount of our most talented operators continue to exit the Marine Corps well before retirement. There are two primary reasons for this. First, Marines practicing cyberspace operations have few opportunities to be hard-living Marines, instead "engaging" with our nation's enemies through a laptop while seated in a cubicle and tucked in a secure building. This is not how recruits imagine Marine Corps life to be. Second, employment in the commercial cybersecurity industry requires certifications and experience, and our cyber-billeted Marines are equipped with both of these early in their careers. This makes them extremely competitive in the commercial industry at an average starting salary of $116,000.[5] On top of this extrinsic reward, the civilian world has no barracks inspections, no bailing coworkers out of jail at 0200, no mandatory change of station orders, no monthly 24-hour duties, and even allows its employees to use hotplates and rice cookers in their living quarters. Now the Corps is fielding its new 17XX occupational field of Marines, turning from the current paradigm of periodically rotating personnel back to communications or intelligence units to one where they will exclusively conduct cyber operations at the national or Marine Expeditionary Force level. This move was designed to stop pulling talented Marines from a highly specialized job just as they were achieving proficiency. It is likely to have an unexpected and profoundly negative effect on retention, as Marines are vertically assessed out of boot camp and immediately given at least 4 years of experience, a hundred thousand dollars in education, and a top-secret clearance. While nothing should be done about the inherently unpleasant aspects of being a Marine, something must be done to appropriately reward the high-demand, low-density skills of the Marines conducting cyber operations.

The current solution to cyber force staffing involves hiring contractors and federal service (GS and GG) employees to serve alongside Marines. This move not only enabled the Marine Corps to reach staffing goals faster than it could produce qualified uniformed operators, it also intends to provide continuity by building long-term expertise through years of service in the same job or command, whereas Marines transition frequently. Yet civilians often provide even less continuity than Marines. Because they receive the same training but have no contract to honor, civilians have the freedom to leave with merely two weeks' notice. In the new and rapidly developing field of cyber warfare, there is no shortage of attractive job offers within the Cyber Mission Force (CMF) that tempt employees to continuously transition jobs and rapidly climb the ladder to increased salaries. Additionally, a civilian is only allowed to work a 40-hour week. If they are asked to work more, they must receive additional time off or overtime. Finally, Federal employees in the GS-12 and 13 grade (step 5), who currently comprise a significant segment of the civilian cyber workforce, earn an annual salary of $94,520 and $112,393 respectively with access to competitive healthcare plans available for approximately $8,000 per year in premiums.[6] In comparison, a staff sergeant with 12 years of service, who comprise a significant segment of the uniformed cyber workforce, earn approximately $65,266 annually, including basic allowance for housing.[7] It is worth noting that this comparison between GS and military comparison is conservative. Marines who choose to enter the contracting force or private industry can reasonably expect to earn even more, although the tradeoff is often job security. In addition to an approximate $18,000 disparity in annual pay, Marines are regularly required to work longer hours, to include weekends, while civilians are required to leave after they reach their standard hours for the week, except in the extreme case where overtime is authorized. Collectively, these discrepancies naturally sow tension between the Marines and civilians working side by side, providing additional motivation and means for qualified Marines to leave the uniformed service. This is not intended as an indictment against our dedicated civilians. Rather, it is the unfortunate result of fundamentally different human resource models that cannot and should not be reconciled but are forced to co-exist. With whom is the uniformed cyber warfare community left? It is left with those few, highly qualified patriots for whom the intrinsic reward of service to the Corps is sufficient, those who have laterally moved into the community late in their career and are now a few years away from retirement, and those whose prospects in industry are less than promising.

The problem of retaining the most qualified and skilled Marines in cyber warfare billets is not new. In 2015, then Secretary of Defense Ash Carter proposed loosening standards on recruits who come with certain industry standard qualifications to boost the technical capability of the Service.[8] He posited that since cyber warfare is not conducted in the physical domain, recruits entering a cyber MOS should not be held to physical fitness standards and could potentially be exempted from attending boot camp. This concept, known as "lateral entry," was echoed by then MajGen Lori Reynolds, who compared the way the Marine Corps band is staffed with the potential future of the Marine cyber warfare workforce, though she later suggested that the Marine Corps will not change the culture of first being a Marine, then a rifleman, and finally a cyber warrior.[9] According to then MajGen Loretta Reynolds during the 2017 Navy League Sea, Air and Space Exposition:

> Maybe there is an opportunity for us to look at other ways [of recruiting cyber forces], kind of the Marine Corps Band model where you bring in gifted musicians and you make them Staff Sergeants and then they spend their years in the White House in a red uniform, but they are Marines. So we are going to look at everything, we are going to look at all those models. [10]

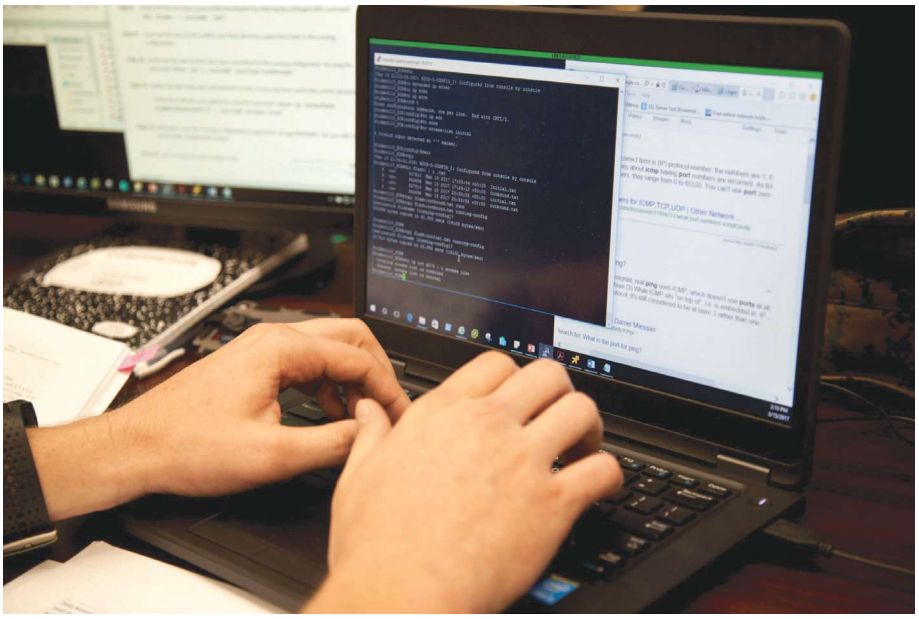
The idea of allowing civilians to assume the title "Marine" based on their skill in the cybersecurity industry violates the foundation of what it means to be a Marine. From the very beginning Marines are indoctrinated with our institutional core values and dedication to the concept of mission and team

over self. This invaluable and intangible quality distinguishes military service from many other professional models and is why qualified Marines are a valuable commodity in any workforce. Thankfully, the Marine Corps has not yet entertained this concept beyond casual conversation.

An alternative approach, mentioned by the former Commandant, Gen Robert B. Neller, is the adoption of the Assess and Select (A&S) model used by Marine Forces Special Operations Command (MARSOC).[11] This system allows Marines from any MOS to go through the assess and select process for potential entry into that elite group. Once a Marine enters the special operations community, they take on the MOS 037X and never return to the Fleet Marine Forces. Where this comparison breaks down is that MARSOC offers Marines the opportunity to be elite warriors who complete missions and gain combat experience they would not receive anywhere else. Should they leave that community, it is unlikely their special skills will seamlessly apply to another high-paying industry. In contrast, the eighteen-year-old Marine who takes on the 17XX MOS and gains advanced training and technical experience will quickly realize that he or she is not doing the kinds of work pictured in recruiting commercials. Further, they can do essentially the same job from a different cubicle in private industry or Federal service for significantly more money and with less encroachment on personal liberty. However, one useful comparison between the fields is that MARSOC operators earn over $10,000 per year in incentive, special duty, and hazard pay, which is based on compensation for low-density skills and not inclusive of retention bonuses. Similar compensation should be considered for the kinds of skills the force requires of Marines conducting cyber operations.

Marines from any MOS could go through an assessment process and become a member of the cyber community. *(Photo by Cpl Victoria Decker.)*

Because training a cyber warfare specialist requires years of costly training and experience, the Marine Corps should consider a human resource model similar to its aviation community. In exchange for incentive pay and valuable training, Marines would be required to sign extended commitments and demonstrate performance under pressure, allowing the service to build a highly-trained yet sustainable cyber workforce primarily comprised of uniformed members. Marines operating in the cyber domain would slowly gain both the certificates and experience necessary for employment in the industry as benefits of their service, while providing critical skills at great savings to the government compared to hiring Federal employees for the same job. To enter the 17XX cyber warfare field, Marines would agree to a six-year enlistment, starting after completion of approximately two years of rigorous cyber training. It is important to remember that the CMF's mission is to counter state-sponsored adversaries, or the foreign equivalent of NSA, which it cannot do with people who fail to meet requirements in a training setting. Should Marines fail to pass cyber training, they would transition to the communications or intelligence communities with a standard enlistment term. Under the plan outlined above, a Marine who has received the training and experience needed to be successful outside the military would first be eligible for exit from service eight years into his career. At this point, the roughly 26-year-old Marine should be offered another six-year enlistment that sends them to another round of advanced training, the start of a significant "cyber pay" annual incentive to close the wage gap with GS employees, and an additional retention bonus commensurate with the Corps' needs that year. Upon the completion of this enlistment they would be at 14 years of service and now practicing at the level of a master of their craft. At this point, having gained significant training and experience, many Marines are likely to exit service for much higher paying jobs elsewhere. Those who stay are the dedicated few who want to shepherd



Creating a cyber warfare MOS was the first step toward building a credible cyber force. *(Photo by LCpl Jose VillalobosRocha.)*

the next generation or continue in a niche field like offensive cyber operations, neither of whom find greater income potential compelling enough to leave. A more effective incentive for these Marines may be the opportunity to remain in a geographic location, so long as there is an open billet, until they desire to move or choose to retire. Similarly, 17XX manpower models should consider allowing an E-7 to turn down promotion in favor of continuing to practice as a technician, thereby avoiding a promotion that would force them into an administrative role for the rest of their career. While the details and numbers of this plan are flexible, the tenets of extended time commitments and roughly equal compensation with the civilians who do the same job are critical to fielding a credible uniformed force in the cyber domain. Even after the significant annual "cyber pay" starting after year six, the government will have saved approximately $108,000 over the course of the Marine's career compared to hiring a federal civilian, with the added benefit of more predictable staffing across the force. To be sure, there is more to being a Marine than pay, but it is not an insignificant consideration as members venture into life events like home ownership and children. Until action is taken, the Service is accepting a natural limit to the expertise it is likely to achieve in uniform.

The Marine Corps cannot hope to outpace nation-state threats without the expertise of the field's best and most capable operators. The creation of a cyber warfare MOS was a necessary first step in the effort to build a capable cyber force and is helping to properly train, billet, and focus retention efforts. On its own, however, the specialized MOS only makes retention more difficult by ensuring that Marines are highly trained and provided advanced experience over a short period of time, especially early in their careers. The calling of a Marine is far more demanding than a typical job and should never be compromised. However, just as the service rewards special operators and aviators according to the demand of their skills, Marines practicing cyber operations should receive extrinsic benefits equitable to their civilian counterparts. If there is no change, Marines have few incentives, apart from a love of the Corps, to remain in cyber warfare billets, and it is unlikely that those who stay will be numerous enough to field a uniformly capable cyber force. The cyberspace domain offers many opportunities for advantage in future conflict, many of which the Marine Corps will be forced to neglect without taking aggressive measures to retain its well-qualified Marines.

Notes

1. Jim Sciutto, "OPM Government Data Breach Impacted 21.5 Million," *CNN*, (2015), available at https://www.cnn.com; Reuters in Washington, "US Military's Joint Staff Hacked as Officials Point the Finger at Russia," *The Guardian*, (August 2015), available at https://www.theguardian.com; and Hayley Richardson, "Companies Must See Cyber Attacks as Inevitable," *Newsweek*, (February 2015), https://www.newsweek.com.

2. U.S. Cyber Command Combined Action Group, "Beyond the Build," *Joint Force Quarterly*, (Washington, DC: National Defense University Press, 1st Qtr 2016).

3. Department of Defense, *Department of Defense Cyberspace Workforce Strategy*, (Washington, DC: December 2013); and Department of Defense, *2018 DoD Cyber Strategy and Cyber Posture Review,* (Washington, DC: 2018).

4. Gen David H. Berger, *38th Commandants Planning Guidance*, (Washington, DC: HQMC, 2019).

5. Kenneth Corbin, "Cybersecurity Pros in High Demand, Highly Paid and Highly Selective," *CSO*, (August 2013), available at https://www.cso.com.au.

6. Office of Personnel Management, "Salary Tables," (2019), available at https://www.opm.gov; further information available at https://www.opm.gov.

7. Information available at https://www.dfas.mil.

8. Evan Vucci, "Ashton Carter Considers Easing of Enlistment Standards," *NBC News*, (March 2015), https://www.nbcnews.com.

9. Jeff Schogol, "Every Marine A Rifleman No More?," *Marine Corps Times*, (May 2017), available at https://www.marinecorpstimes.com; and "Cyber Operations; Sea Services Panel," (panel, Navy League Sea, Air, and Space Exposition Day, National Harbor, MD, April 2017).

10. "Cyber Operations; Sea Services Panel."

11. "Every Marine A Rifleman No More?"