Cyber warfare operators assigned to 275th Cyber Operations Squadron of 175th Cyberspace Operations Group, Maryland Air National Guard, configure threat intelligence feed for daily watch in Hunter's Den at Warfield Air National Guard Base, Middle River, Maryland, December 2, 2017 (U.S. Air Force/J.M. Eddins, Jr.)

From DOPMA to Google

Cyber as a Case Study in Talent Management

By David Blair, Jason Hughes, and Thomas Mashuda

Talent management is the sine qua non of an effective organization and, therefore, a critical determinant of military success. Within the framework of this article, talent management is best understood as the thinking, policy, and strategy associated with hiring, training, and retaining great people. Due to the competitive nature of combat, military organizational structure and culture must be ruthlessly functional, designed to apply the abilities and skills of the populace in order to produce dominant combat capability. If the American military cannot attract, develop, and retain the right people, producing an environment in which these people flourish, the joint force cannot expect to find success in competition below the threshold of armed conflict, major combat operations, or credible deterrence. This is a moving target, as the proverbial "right people" change over time due to changes in society and technology. Stated simply, a nation's best military is the one that best leverages the deep strengths and best mitigates the weaknesses of that society. This is a function of both humans and hardware, requiring talent management reform and acquisitions reform, respectively, but as the special operations forces (SOF) axiom counsels, "humans are more important than hardware."[1] If the military is to retain its competitive edge, it must master talent management, especially in relatively new enterprises such as cyberspace.

Lieutenant Colonel David Blair, USAF, is a Senior Special Operations Aviation Advisor at the Office of the Secretary of Defense. Major (P) Jason Hughes, USA, is a Medical Service Corps Officer serving as the Joint Staff Surgeon's Strategic Plans, Exercises, and Logistics Action Officer. Lieutenant Commander Thomas Mashuda, USN, is an MH-60R Pilot currently serving in the Joint and Coalition Operational Analysis Branch of the Joint Lessons Learned Division of the Joint Staff J7.

Cyber as a Case Study

Surveying our present portfolio, this challenge is most acute and pressing in the cyber community. Since the full scope of the problem exceeds

the scope of any one article, talent management for cyber warriors is a manageable problem that implicates many of the larger talent management trends. A number of changes to the current industrial-era promotion and retention systems are necessary to maintain a competitive edge in cyber over the coming decades—specifically, tailored control over standards and advancement, a technical track for cyber operators, and the possibility of a cyber auxiliary force with an alternative means of accession.

To outline the challenges associated with talent management in the cyber force, this article begins by describing those challenges and continues by conducting strengths, weaknesses, opportunities, and threat (SWOT) analyses of the U.S. cyber status quo, the independent German "Gray Berets" cyber service model, and the Russian and Chinese levée en masse cyber models. From the SWOT analyses, the authors synthetically derive policy recommendations for improving cyber talent management. Ultimately, this cyber case study can provide a template for solving aspects of the larger talent management problem, especially in highly technical domains or branches.

The Current Cyber Baseline

This article assumes a general knowledge about the basic principles of the current military personnel system. As a quick review of the cyber status quo, cyber operators are subject to the same personnel system rules as the rest of the military. Of particular concern are the "up-or-out" system, the system of centralized promotion boards, and the centrally managed assignment system. These features fit well for an industrial-era assembly line bureaucracy.[2] They are ill-suited, however, to a tech company, as the case study below demonstrates, and cyber is more like a tech company than an assembly line.

Checking all the boxes to accommodate an industrial, centrally managed system is a particular problem for cyber, as the field runs at the speed of Moore's law, and operators out of the seat for more than 6 months have to relearn much of the new "state of the art" when they return. This is incompatible with the current staff and school-in-residence model required to advance under an up-or-out system. This remains a persistent problem that will take major changes to fix and which must be coordinated with multiple stakeholders.

Running parallel to this rigid promotion structure is a monetary incentive system that functions as a force management, rather than a talent management tool. The same bonus and incentive pay templates used to retain a sufficient number of pilots and Navy nuclear Sailors to meet billet quotas have been applied to cyber forces since 2010. Such Selective Reenlistment Bonuses and Assignment Incentive Pays, adopted by the Army Cyber Mission Force in 2015,[3] are shortsighted stop-gaps at best. They assume, possibly incorrectly, that throwing money at the talent management problem will fix it. These techniques are likely unsustainable in the shadow of an ever-growing private tech sector and workforce shifting toward millennials.

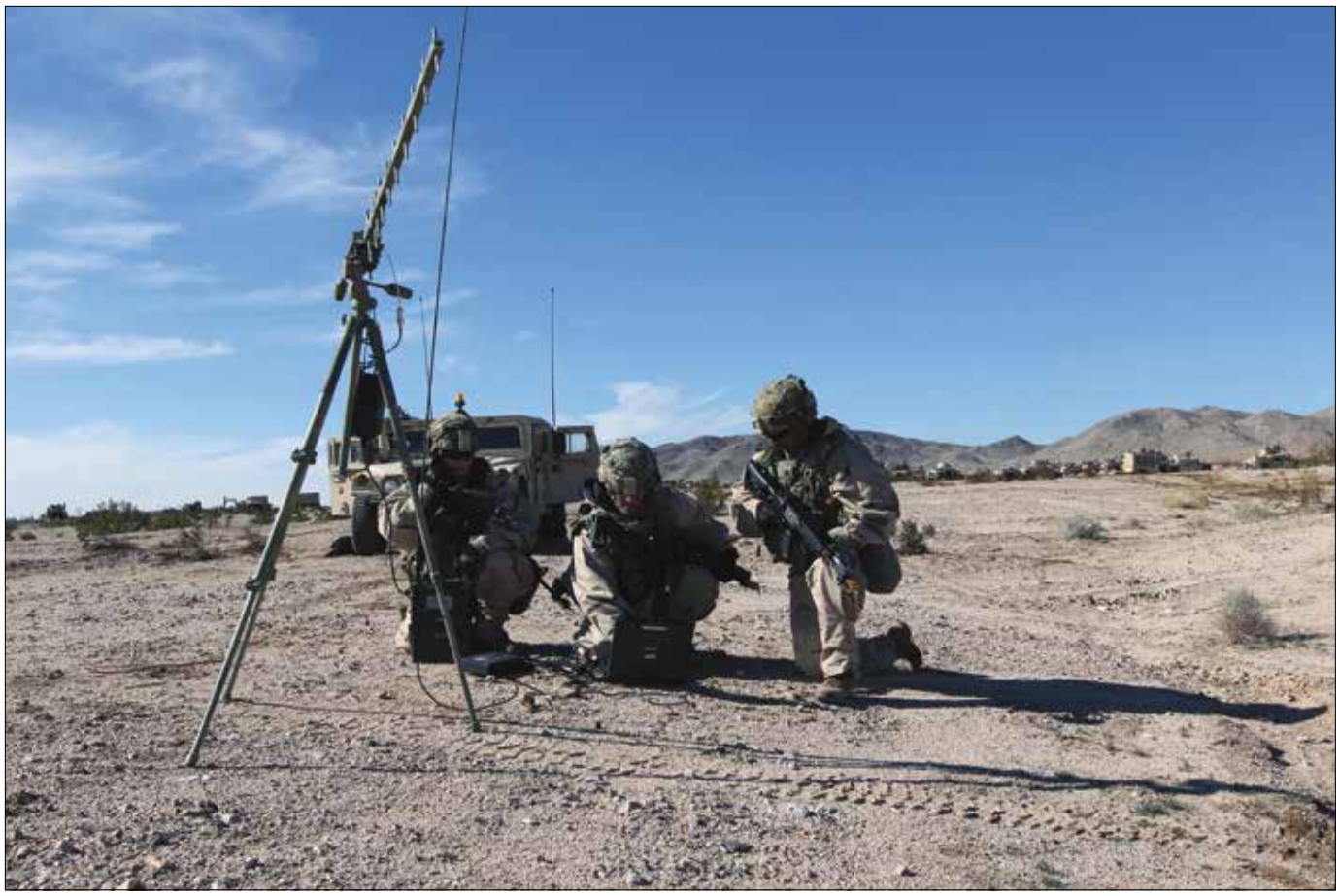
Structurally, cyber operators have achieved some degree of institutional autonomy within the Services—U.S. Army Cyber Command, the 24th Air Force and its cyber mission forces,[4] the U.S. Navy's Tenth Fleet, and the U.S. Marine Corps Forces Cyberspace Command.[5] Moreover, the establishment of U.S. Cyber Command (USCYBERCOM) provides a warfighting platform for these forces. USCYBERCOM is following a model similar to U.S. Special Operations Command (USSOCOM), with semi-independent funding and acquisition authorities and a direct operational link to the Secretary of Defense.[6] However, like USSOCOM, even with these changes, the command will not have much control over the personnel policies and processes of its people, which remain the province of the military departments. Unfortunately, as described above, it is in these policies and processes that the talent management problem lives, not in a lack of institutional independence.

The current structure leverages extant and stable Service processes, a strength that means that cyber does not need to fund and manage a separate personnel bureaucracy. However, the impediments of the industrial-age systems still used by the Services make it difficult to compete with the market to bring in talent and to retain any talent developed organically. The current structure can take advantage of the opportunity to follow the USSOCOM pattern that, under Section 922 of the 2016 National Defense Authorization Act, gained a responsibility similar to a Service Secretary for the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, which included new authorities for managing SOF personnel. A similar structure with similar authorities might be imagined for cyber policy elements under the Office of the Secretary of Defense. However, by continuing to rely on legacy industrial-age systems, the joint force may have to severely curtail the role of military cyber and rely on other options.[7] The better road is to recalibrate our concepts of professional military and citizen Soldiers around these new technologies.

Civilian Model: Flexible Tech Sector Careers

American businesses in the industrial and service sector follow a model similar to the military personnel system—the legislation that scripts the military personnel system was based on best practices from these industries in the late 1970s.[8] Gather thousands of applicants, select the best on paper, train them to execute the job required, and follow the company plan for promotion. Workers are placed in an assembly line talent management program, working their way up from the bottom. This works for industrial or service companies, whose product is stable and where optimization often trumps innovation. The tech sector, specifically Google and Microsoft, manages talent in a fundamentally different way because tech-sector requirements are fast-moving targets.

Google, for example, worked to build a system that allowed exceptional talent, outside of the normal metrics of degrees or certifications, to be identified and incorporated into their system. This allows



Cyberspace operations specialists with Expeditionary Cyber Support Detachment, 782nd Military Intelligence Battalion (Cyber), provide support to training rotation for 3rd Brigade Combat Team, 1st Cavalry Division, at National Training Center, Fort Irwin, California, January 13, 2019 (Steven Stover)

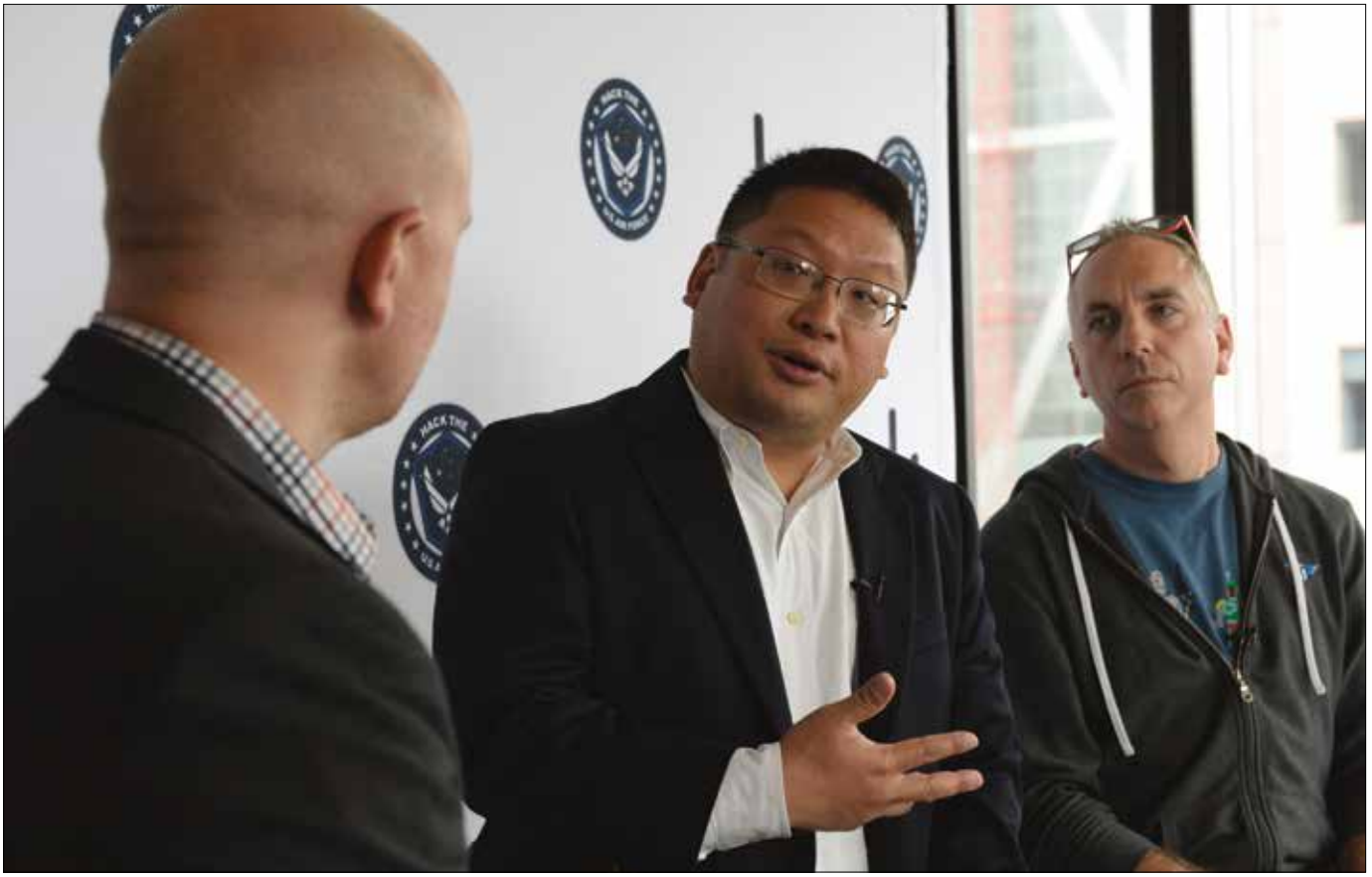
recruiters to attract young, ambitious self-starters and original thinkers to keep up with the ferocious pace of change in the tech sector. Competing for those people means understanding how to attract them.[9] One of the key aspects of the Google system is an organizational culture that encourages collaboration and individual projects—the company aspires to the concept of "20 percent time," or the principle that employees are empowered to spend one-fifth of their working time on projects of their own initiative. Google demonstrates that in an information-age talent management system, there is a blurring of lines between recruiting, retention, and employment of talent, and quality of service works alongside quality of life both to attract the right people and to use them well.

Microsoft realized that outdated techniques of recruiting hurt its ability to attract the talent needed to succeed in today's environment. The millennial generation and other prospective employees use technology and social networks far more than previous generations. Attracting talent requires a social recruiting strategy that leverages social networks in more fluid and interactive ways.[10] The Department of Defense (DOD) could similarly shift toward a more fluid recruiting and assignment system that leverages social networks rather than financial incentives.

Recruiting exceptional talent is the first step. Keeping the talent is next. Younger workers want to make an impact by changing the way the world lives one algorithm at a time.[11] They value this "quality of service" more than job security, which was a recruiting factor for earlier generations. Organizations had to design their culture and structure to accommodate this desire. Technical companies eschew hierarchical management structures to emphasize the individual. Google highlights that they are an organization built by engineers for engineers; this yields a structure that allows freedom on the technical side but manages their career.[12]

Google established Project Oxygen, which uses analytics to develop leaders who allow technical workers to thrive in their culture. Technical experts want to be managed by those who understand their skills. Project Oxygen found that leaders who empowered the team, eschewed micromanagement, communicated with a clear vision and strategy for the team, and wielded key technical skills to advise are those best equipped to manage in a technical environment.[13]

The civilian model enjoys the strength of a flexible organizational structure, not beholden to dated personnel systems, to take advantage of talent or the market. The civilian sector can provide attractive



(From left) Alex Rice, chief technology officer and co-founder of HackerOne, Peter Kim, Air Force chief information security officer, and Chris Lynch, director of Defense Digital Service, announce "Hack the Air Force" event at HackerOne headquarters, San Francisco, April 26, 2017 (U.S. Air Force/Dan DeCook)

employment packages oriented toward creative incentives rather than solely compensation. For instance, Google's commitment to 20 percent time consistently receives high reviews and results in profitable results, most notably Gmail and Google Earth.[14] Furthermore, access to worldwide talent provides ample access to sources of talent not available to the military. However, the pace and volatility of the industry is a liability that causes constant churn in the workforce.[15]

Visionary leaders such as Elon Musk[16] provide what Simon Sinek calls the "why,"[17] attracting funding and talent to tackle seemingly unachievable goals. As described above, changing the world is a key attraction for tech talent. The private sector is able to leverage "lore," openly discuss big ideas, and trumpet past accomplishments, thereby creating room for collaboration with other like-minded companies or pull "free agents" from other sectors. (Lore as an attractor is hardly foreign to the military—every high-level headquarters has a hall of honor that retells the stories of the exemplars of the command. Doing the same for cyber would require a careful navigation of security issues.) Survival in an entrepreneurial environment is only possible by maintaining an innovative spirit and the drive to solve problems.

A talented 12-year-old with access to limitless information can change the world,[18] and can threaten a company's business model or bottom line. Google, Microsoft, and similar tech companies face threats from continuing digital transformation, advanced analytics, artificial intelligence, machine learning, and other innovations that could fundamentally change the talent landscape. Companies that guess wrong today will find it difficult to attract a workforce needed to win in an unpredictable future.[19]

This analysis reveals several key principles from the civilian sector, namely, that technical cyber operators desire to be led by those who understand their craft. Additionally, creativity is a hiring draw as well as a value producer, and the flexibility to pursue creative craft is a necessity. Finally, freedom in job placement is a stronger draw than compensation. Gaining and maintaining skill in the cyber domain for the long term require concessions from the traditional military model, especially in the form of a "technical track" option and relief from the pressures of an up-or-out system.

Independent Service: Germany's "Gray Berets"

Germany's Cyber and Information Space Command, colloquially known as the Gray Berets,[20] was established as the sixth German military service in April 2017. This three-star command joined the German army, navy, air force, joint support service, and joint medical service.[21] It was borne out of a real and growing concern that Germany was ill-equipped to fight future wars (and conflicts short of war) in the cyber domain.

This concern was borne out as hackers targeted the Bundeswehr's information technology (IT) infrastructure 284,000 times in the first 3 months of 2017.[22] This new cyber service is slated to garner 13,500 personnel from various IT and intelligence specialties in the existing German force.[23]

The independent service model has been advocated by many military leaders, most notably Admiral James Stavridis, USN (Ret.), as a means of ensuring the operational effectiveness of U.S. cyber capabilities.[24] Since the German Cyber and Information Space Command is still in its infancy, it is difficult to say exactly how successful a separate cyber force will be at recruiting and retaining talent. However, one can still hypothesize on the strengths, weaknesses, opportunities, and threats that such a force presents. Given the recency of cyber military operations, the ambitious nature of this project commends it as a model worth considering, and one whose advantages are apparent, although in the abstract, especially given the popularity of propagating services and corps in this particular historical moment.

The strengths and opportunities for talent management inherent in the German model of a separate cyber force are numerous. First, that force would be able to set its own standards for entry that could greatly increase eligibility rates within the existing talent pool. Among these are standards for age, physical fitness, and level of education. The German cyber force has already recognized this opportunity and discussed waiving certain education qualification entry requirements.[25]

Second, an independent cyber force could standardize training for its members. Whereas U.S. Cyber Servicemembers receive a disparate breadth and depth of training among the Services, an autonomous cyber service could ensure its members have a common baseline. Germany has signaled its intent to do just this by instituting a cyber security master's degree at its Bunderswehr University to train up to 70 future cyber force soldiers per year, and subsequently create an educational incentive for enlistment.[26] It will take time to determine the effectiveness of the Gray Berets' retention practices, but increased flexibility in cyber career options should yield positive results.

Next, free from the archetypes of other services, a separate cyber force would also be able to shape its own rank structure and establish the incentives and opportunities for advancement within it. The leadership of such a force would be notionally free to establish the criteria it values among its members and then reinforce those criteria in its advancement and retention systems. This would open possibilities for a flattened rank structure similar to parts of the American tech sector, where experience and time in service do not trump knowledge and capability. Starting off from scratch would allow a cyber force to establish its own ground rules and, therefore, shape its own culture, blending the aforementioned innovative solutions implemented at Google with the already granted USCYBERCOM specific authorities, among other distinctives.

A separate cyber force is also flexible and can determine its own pace for adaptation. If the existing cyber rank, advancement, or incentive structure is stagnant or ineffective, a new one could arguably be implemented much faster than it could within one of the conventional Services. This strength is crucial in a domain that is ever-changing.

Lastly, a separate cyber force could, in theory, compete at an equal level with the other services for money and resources that could help attract talent. Such a paradigm shift would elevate cyber warriors' priorities, where they would otherwise be buried among the other competing priorities of an individual service.

However, there are weaknesses and threats to the separate service model. While the German Cyber and Information Space Command has stated it intends to improve the salaries and career opportunities for its servicemembers, it has been slow to offer specifics, and even as a service, would be still bound to national governmental personnel laws. This is a problem in cyber, for just as the military pilot pool is directly linked to civilian demand for pilots, cyber is linked to civilian IT, which is a more volatile market than aviation. Additionally, a separate cyber force is susceptible to isolation and stovepiping, both of which are killers of innovation. At its worst, this could manifest itself in an inflexible cyber force incapable of integrating with other military disciplines or government instruments of national power. Service distinctions could also numb cyber to the personalities and needs of other services that it is meant to complement and support.

Despite its strengths, a separate cyber force is not a panacea, as it does not inherently solve the problems of talent management. While it may not be encumbered by the recruiting, retention, and advancement requirements of the existing military services, it still must compete against the private sector, which will likely still possess competitive advantages in salary and career flexibility. Moreover, relaxing entry standards could have the unintended consequence of significant personnel costs in the future, especially with regards to health care.

The independent service model reveals several key principles. First, the military cannot afford to "buy" talent against the tech sector, and must instead focus on providing meaningful missions, camaraderie, a culture of technical excellence, and unique career opportunities. Since "shoehorning" cyber warriors into legacy careers inhibits the development of this requisite unique cyber identity, a cyber force requires flexibility and some degree of autonomy in order to realize these goals. Therefore, the military should consider limited forms of institutional free rein for cyber warriors, akin to those granted USSOCOM but specific to the demands of the cyber domain.

Russian and Chinese Models

Our competitors have seen in cyber a field where they have some degree of natural advantage—namely, the field lends itself to cybernetic theories of controlling human thought and process, and these are well-trodden ground for both the Soviet and Chinese states.[27] Additionally, cyber coarsens boundaries of time and space, thereby eroding

the high industrial-era walls between the civil and the military sphere. The Russian model leverages the whole of society, in several tiers, to achieve cyber effects against an adversary. This begins in the interagency and, for historical reasons, the Russian cyber enterprise is led by the Federal Security Service, or FSB (the successor of the KGB), which performs national cyber actions, including propaganda and disinformation.[28] The wealth of expertise is owned by these national agencies, and they use them in hybrid warfare, or gray zone, approaches to national policies.[29] Similar to the United States, the Russian military considered cyber more in the realm of communications until relatively recently, and Russian military cyber troops were mostly concerned with maintaining computer connectivity and security.

In 2012 Russia created the Foundation for Advanced Military Research (FAMR), a cyber-military unit focused on offensive and defensive cyber operations. Like the United States and Germany, the country has difficulties recruiting qualified cyber warriors because of the competition for more lucrative civilian options. FAMR is an effort to develop its own organic cyber capabilities in order to expand the use of cyber to support conventional military operations.[30]

Until FAMR bears fruit, Russia's current whole-of-society and outsourcing model creates significant risk. Hackers learn each time they execute a mission, but so do those who are attacked. Outsourced hacking is hard to control, and Russia may find that the hacker exceeds the desired endstate as the hacker finds they can break further into the system. No internationally recognized redline exists on cyber warfare, and each instance may lead to unpredicted consequences for the Russian government, causing kinetic or reprisal cyber warfare.[31]

The good news is that "war is graded on a curve," and the Russians seem to have similar problems with talent attraction and retention. But their national cyber is formidable, and their ability to leverage the whole of society is extremely effective. Security services own the most sensitive missions and most advanced capabilities, but a second ring of state-owned industries provides both capacity and access to the global information space. A third ring of militia-guerrilla forces allows the state to put "asks" out on the Internet to encourage individual cyber actions. While national capabilities are retained by official organizations, these "patriotic hackers" can aid and abet national efforts through everything from defacement to identifying weaknesses and entry points in systems.[32] The Chinese employed a similar concept in the wake of the 2001 EP-3 Hainan Island incident, when patriot hackers conducted distributed denial-of-service attacks and probes on U.S. military Internet sites.[33] This outer tier is unruly and cantankerous, but it is low-cost and plausibly deniable.

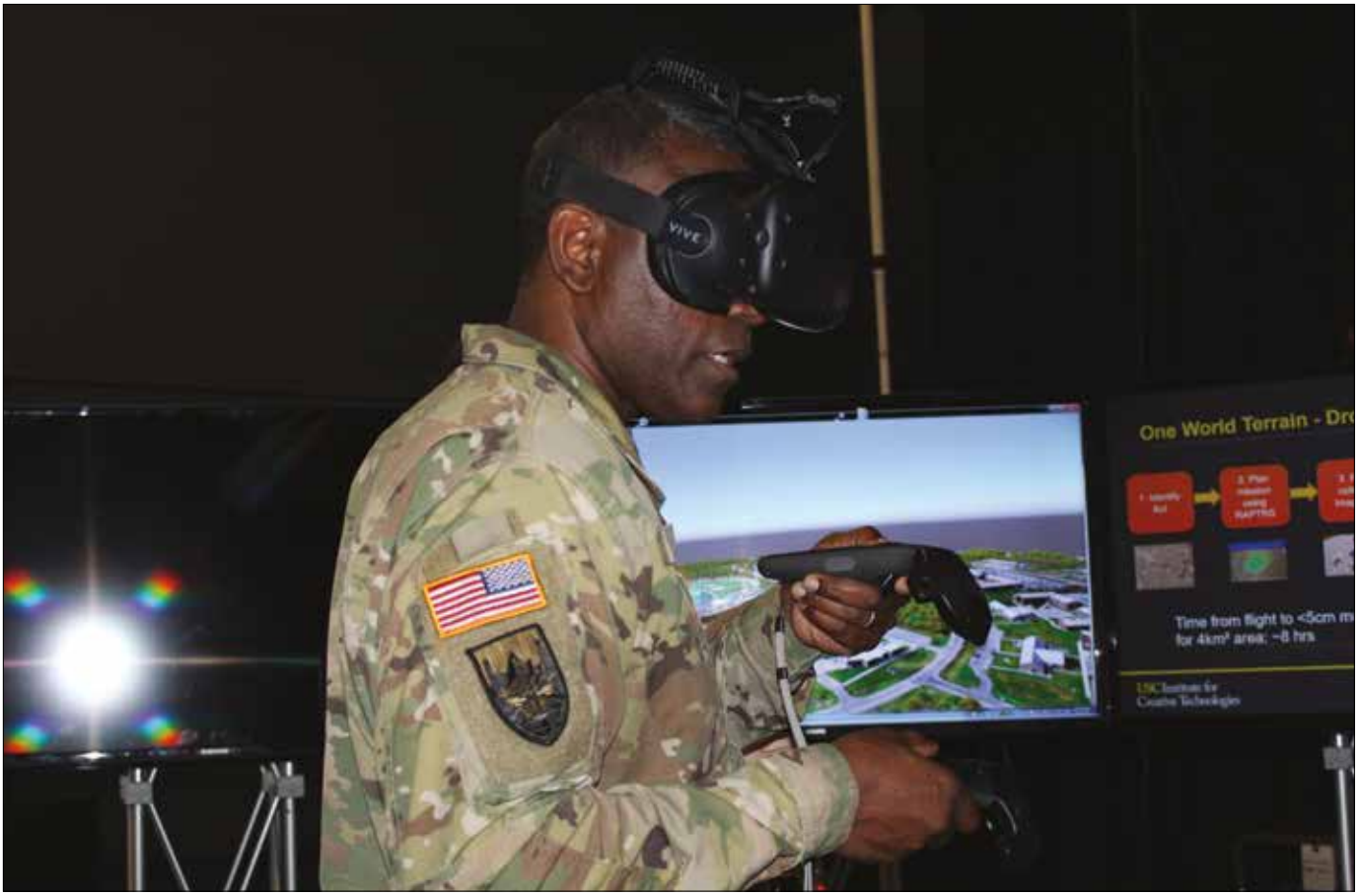
China, like Russia, has advanced cyber capabilities and strategies ranging from stealthy network penetration to intellectual property theft.[34] China has centralized its cyber force in the 2nd Bureau, Unit 61398, under the 3rd Department (SIGINT/CNO), which reports directly to the Chinese equivalent of the U.S. Joint Chiefs of Staff.[35] The People's Liberation Army's cyber command is fully institutionalized within the Communist Party of China (CPC) and able to draw on the resources of China's state-owned enterprises to support its operations. The CPC is the ultimate authority in mainland China; unlike in Western societies, in which political parties are subordinate to the government, the military and government in China are subordinate to the CPC.

The centralization of action is a key factor and explains the focused targeting process directly related to China's strategic goals, as observed by Mandiant, a leading cybersecurity firm. Organizing and directing are useless without the talent to operate in cyberspace. China launched a countrywide effort to find cyber talent, pledging to increase the number of scholarships to attract students pursuing cyber security and running special recruitment for "maverick geniuses," which constitutes a part of nationwide efforts to train cyber security talent.[36] This effort is akin to China's efforts to produce athletes for the Olympic games, in which it scours the countryside for the best and brightest, training athletes from a young age to bring the country glory.[37] China is working with companies to cultivate "the world's top cyber security talent" by recruiting top graduates, both from China and overseas and from cyber contests. Traditionally, China has placed people in targeted programs based on exam scores; however, it seems that potential cyber recruits are evaluated on performance and provided practical training to hone key cyber skills.[38]

The effort of cultivating and recruiting cyber talent feeds Unit 61398, which is housed in a 12-story building and staffed by hundreds to thousands of people who are trained in computer security and computer network operations, and proficient in English. The scale and duration of attacks against a wide set of industries tracked to the known location of Unit 61398 demonstrate China's capability and capacity to execute economic, offensive, and defensive cyber operations.[39]

The strength of this model is its ability to leverage the whole of interagency and society toward cyber objectives, which is a key enabler for hybrid warfare capabilities. Concentric rings of capabilities, combined with the levée en masse principle, allow both national forces to conduct precise attacks with the most controlled tools and guerrilla forces to conduct deniable, unpredictable hit-and-run attacks. However, in order to employ the levée en masse principle in an authoritarian country, a state must roil its people into a foment in order to yield the patriotic hackers, often exposing the government to the threat of its hackers getting out of control and going too far. They also do not need to consider the authorities' problems in using such a model, but untangling this would be challenging.

An effective cyber model should extract this principle of multilayered civil-military cybersecurity partnerships. It should also consider the value of collaboration with industry and "cyber militias" where there are shared interests or values. However, as part of a liberal democracy, the American military must



Commanding general of U.S. Army Research, Development, and Engineering Command tries hand at One World Terrain, March 2018 (U.S. Army)

consider proper authorities, control, and civil society immunities involved in the use of force.

The Policy/Strategy Mismatch

With this survey of available models complete, our analysis returns to the cyber talent management problem and identification of potential solutions. Chuck Spinney, acolyte of Colonel John Boyd, once described a "Plans/Reality Mismatch"[40] between the budgetary process and results of said process. The current talent management crisis is a symptom of a policy/strategy mismatch, as evinced by the Air Force pilot shortage,[41] our difficulties in attracting cyber talent,[42] and the myriad persistent difficulties induced by an up-or-out system as described in Tim Kane's book *Bleeding Talent*.[43] The root of these problems is a generational mismatch between industrial-era human capital management systems, the hallmark of rust-belt corporations, and contemporary talent management systems such as those used in the Silicon Valley tech sector. The former focuses on transactional optimization tools, which means matching the right number of faces with the right (easily categorized) qualifications to fill all the places on the organizational chart. The latter "expects the unexpected," embracing unique and self-identified talents, and hence it is a model uniquely suited to a creative economy. The mismatch between the creative economy and our lagging industrial-era military personnel systems drives out many of our best people.[44] In one particularly concerning turn, U.S. competitors have been able to incorporate many features similar to those used by Silicon Valley into their systems in order to optimize the same sorts of talents that a rigid industrial-age system is driving out of the U.S. Defense establishment writ large.

This problem is especially pressing in light of the Third Offset Strategy[45] efforts to leverage advanced technologies in pursuit of a new revolution in military affairs (RMA).[46] An RMA is a tectonic shift in military operations, a rapid synthesis resulting from long-term shifts in society and technology. For instance, the invention of rifles held the potential for revolution, but they could not be fully applied until nationalism allowed for major changes in distributed command and control, as manifest in the small-unit tactics used in the American Revolution. The possibilities of hardware cannot be realized without evolution on the human side of the equation. For instance, artificial intelligence (AI) is one of these key advanced technologies changing the role of the human workforce. By automating simple, repetitive tasks—the sorts of tasks that industrial systems embrace—AI is forcing humans to refocus on creative tasks, where they will still outpace machines for the foreseeable future. However, the traditional industrial-era military training and recruitment

system tends to focus on processes for reproducing these repetitive tasks. Just as these technologies drove major structural changes in the civil economy, they will have to drive major changes in the military workforce in order to unlock the full potential of a fighting force increasingly composed of millennials.

Policy Recommendations

Analysis of these three models yields three design principles toward building such a force. The mission focus of the German model demonstrates the value of flexible career tracks that focus on craftsmanship. The Russian model reveals the importance of decentralization and organizational flattening, as their multilayered approach provides span and innovative tactical options. Finally, the Silicon Valley model illustrates the imperative to trust the initiative of our people, as many of the most profitable products of Google began as individual discretionary projects.

Building on these design principles, there are three recommendations that are both within the realm of the possible and within a policy-relevant timeframe. First, DOD should consider supercharging the increasing institutional independence of our cyber forces by granting increased latitude over standards and advancement for cyber operators. Second, realizing that cyber is a non-industrial, creativity-and-collaboration-driven, and extremely perishable skillset, DOD should consider a technical track for cyber operators that focuses on elite technical skills but retains the broad authorities of officers. This maps well onto Silicon Valley precedents of legendary senior coders who are disproportionately productive, as well as practices of our competitors. Finally, following the principle that cyber is part of the larger 21st century's "democratization of production," the national security enterprise must consider coarsening some of the civil-military distinctions along the lines of the early Republic. A multitiered "cyber auxiliary force," which leverages Reserve and National Guard authorities, and potentially revives constitutional "letters of marque and reprisal" authorities, brings the cyber talent of our society to bear without endangering our freedoms, providing a version of the Russian model more appropriate for a liberal democracy.

Increased Control over Standards and Advancement. No matter what system is ultimately adopted for cyber talent management, it should exert expanded influence over the standards to which members are held and their opportunities for advancement and retention. Perhaps implemented as coordinating authority with the Services, paralleling the expansion of SOF authorities, this influence would address key issues previously highlighted in the existing force structure. First, control of standards would allow recruiters to open their aperture and accept highly talented individuals who would not otherwise qualify for military service. Since cyber warriors do not need to hump miles to charge an enemy hill, the flexibility to refocus standards (within reason) on cyber-relevant requirements would prevent the loss of otherwise premier talent.[47]

Next, control over advancement boards would ensure that the right qualities, qualifications, and skills are retained, independent of Service biases, as to which blocks should be checked under an up-or-out system. Control over retention tools would allow for a tailored incentive system that could overcome existing indiscriminate systems that seek to retain a body to operate a computer terminal without regard to whether that body is the most qualified.[48] Money might not always be the most effective retention tool, but it is currently the easiest tool given current processes and authorities.

Technical Track for Cyber. The Air Force is presently considering a technical track.[49] Triggered by an aircrew retention crisis, the Service is realizing that flight skills are perishable and difficult to replace and that many of those who hold them would prefer to continue to exercise them on a technical track rather than to pursue a management-style promotion career path. Such a path, as described below, would allow a branching between those who wanted to pursue and maintain proficiency and mastery of cyber tools and those who will maintain a functional knowledge but focus on managing and integrating the capability within the larger force. This is a functional split that is evident in many high-tech fields—for example, the National Aeronautics and Space Administration hires excellent engineers, and many focus their careers on honing that craft, while others go on to run the organization. One key cultural feature of this split is that one is not clearly superior to the other, but they are mutually reliant. This is a feature of the tech sector as well—few things will drive out technical talent more quickly than a technically illiterate manager dictating technical decisions to a craftsman.

In many aspects, recurring themes from the tech sector and adversary models parallel aspects of aviation and surgical culture, with high levels of value on technical mastery and collaboration, and the self-policing of performance and values.[50] In a technical track model, career operators would recognize the (to their mind, likely unenviable) role of their peers on a management track in instructional governance, and those peers would recognize the value and province of technical experts. Performance pays for technical track officers could offset these lost promotion opportunities. These technical leaders might even enjoy special privileges and opportunities, such as the standardization and evaluation roles, to further create interdependencies. Another advantage of a technical officer corps is the idea of intrinsic authority, which is a requirement for mission sets that are expected to navigate complex problems with national-level consequences, which might not have approved solutions. Given the prospect of a technical expert, deep in an enemy's network, running a time-critical exploit, he will likely not have time to ask for guidance for all unforeseen problems and will need to make some command decisions in the course of his action. A technical officer would have the broad authorities to make these calls.

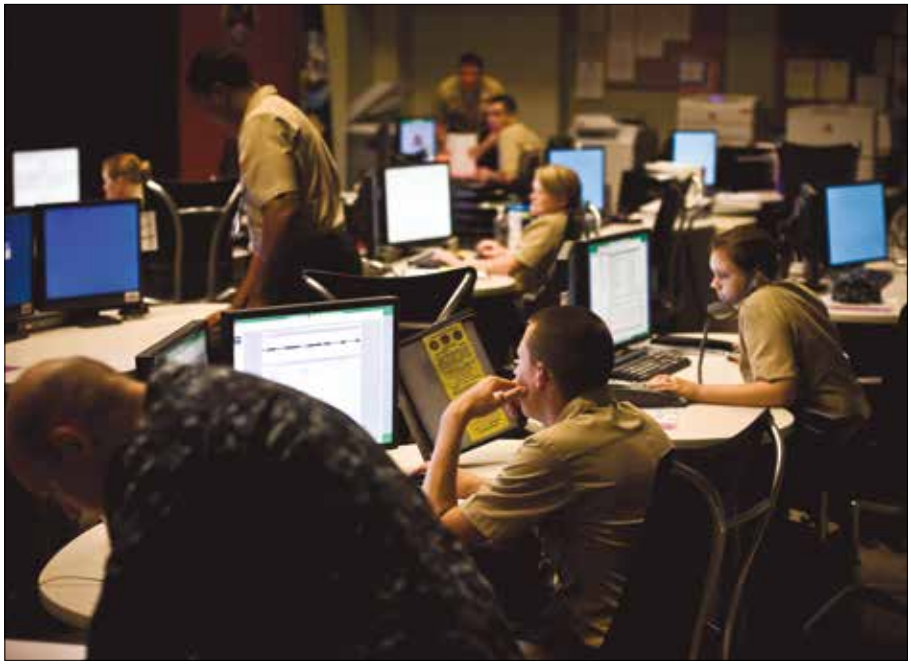
In another idea from the Air Force's efforts to remedy its manning crisis, virtual staff tours could allow a cyber force member to remain in place at an operational assignment, gain a Pentagon phone number, email, and office symbol,

and do her staff job while maintaining a basic operational currency. Any meetings that could not be done via video teleconferencing could be attended through a temporary duty assignment. This is similar to the tech sector telecommuting model, which is wildly popular in Silicon Valley.

Cyber Reserve and Auxiliary. Two fundamental options supplement our full-time cyber force: a cyber Reserve force and auxiliary cyber force that allows DOD to leverage talent when needed, while also allowing them the opportunity to continue their work in the private sector. The Reserve force model must be modified to accommodate and attract talent to support this venture.

The 2017 National Defense Authorization Act (NDAA) provides the Secretary of Defense flexibility to adjust hiring and retention of cyber personnel.[51] This provides an avenue for DOD to fundamentally change the structure for key personnel in support of the cyber mission. In many cases, Reservists who are civilian cyber professionals could do many of the same tasks for the government under a Reserve commission, which provides the authorities with what they need to execute their "wartime" mission. Placing them in an Individual Ready Reserve status where they are on-call provides access to their talents without competing with the private sector. This model is akin to keeping a lawyer on retainer for future work, and with a flexible drill days option, they could be activated to deal with an emergent problem or even if they identified a problem through their civilian work.

Change in the cyber world is accelerated; this allows key people to maintain their skills and support the private sector while also protecting the homeland from cyber attacks through their company's day-to-day operations of defending their applications and networks. Our competitors attack both government and private-sector entities; therefore, skills need to be consistently maintained to counter the current threat. A yearly virtual drill would allow U.S. Cyber Command to test and provide updates on defense-related targets, but daily work might count as a drill given arrangements with industry. Specifically, given state-sponsored attacks against American civilian economic interests, cybersecurity industries or major corporations may often find their interests aligned with military cyber objectives. These Reservists might serve as a bridge using both Federal and corporate authorities, much as Merchant Marine officers do, whose civil and military authorities are blended and take on different flavors in war and peacetime.[52] This would require extensive ethics training and legislative clarification, but is likely a necessity against competitors who do not observe a "Cyber Geneva Convention" in differentiating military versus civil cyber infrastructure.



Cyber Defense Operations Command Sailors monitor, analyze, detect, and respond to unauthorized activity within information systems and computer networks at Joint Expeditionary Base Little Creek–Fort Story, Virginia, August 4, 2010 (U.S. Navy/Joshua J. Wahl)

As a salient example, the shipping industry realized that governments were unable to completely secure sea lines of communication against piracy, thus demanding a private-sector security solution. Governments initially resisted this effort but accepted that active defense measures deployed by owners, along with insurance providers, helped deter attacks. The bottom line—the private sector filled a critical gap in protection.[53] This is the idea of "letters of marque and reprisal" discussed by cybersecurity expert and Georgetown professor Catherine Lotrionte.[54] Distinct from the Merchant Marine–analog Reserve model, this model is more like raising a militia or privateering.

Government should produce guiding principles for active cyber defense versus laws and regulations that it cannot enforce.[55] This provides a framework to leverage private solutions to defend public and private cyberspace deterring future attacks. Defensive posture operations would be managed by the private sector; however, offensive operations require a different model.

An offensive auxiliary force co-exists with the Reserve force, meaning a Reserve officer, with DOD authorities, leads a team of cyber patriots to execute offensive missions in support of our national defense. Building a national defense entity similar to "Anonymous" allows us to focus efforts and leverage talent in a nonattributable way while defending our national interests, as long as alignment with the values of a free and secure society could be ensured. This is different from the Russian model, in which they leverage hackers by placing asks in cyberspace without controlling their actions or effects, good or bad. This

nationalizes the risk and creates an ability to control actions against adversaries, while allowing access to talent that may not be immediately available otherwise.

Implementation Strategy: Spiraling Authorities

To put these concepts into practice, the most promising approach is a spiral design, where each iteration can reduce risk for the next. The logical place to begin is within the authorities already granted under the current Defense Officer Personnel Management Act (DOPMA), and the most profitable of those authorities for cyber is competitive categories. Under DOPMA, placing cyber within a competitive category ensures that cyber officers will get promoted at a rate similar to their peers in other career fields. Perhaps more importantly, a competitive category means that the board for cyber officers will be calibrated to the uniqueness of their career field. Additionally, this competitive category will provide the ability to decide when boards will meet; for instance, the O4 board may meet later than other categories in order to keep cyber officers coding longer, but the O5 board may meet earlier to make up the time. The findings from this first spiral will inform follow-on actions.

Further spirals would then explore options beyond the bounds of current authorities, which would require congressional engagement. Prior to this point, the joint force should compare talent management lessons across its cyber corps, identify best practices, and then identify capability gaps. An eye to competitors would come in useful here. For instance, if the Russians are finding success in commissioning cyber forces off the street, then we may want to consider doing so as well. The second spiral would then focus on creative accessions into the current military force structure, whether readapting standards to a new archetype for cyber warfare, as Crispin Burke suggested in *War on the Rocks*,[56] or providing for lateral entry and options for veterans who work in cybersecurity fields, ideally with some apprenticeship and acculturation process for nonveterans. A third spiral, adjusting for conditions, might make use of "letters of marque and reprisal" and empower businesses or individuals to act as cyber-privateers in the defense of their own interests.[57]

While we imagine the implementation of such a concept well off in the future, the intertwined nature of military and civilian value and capabilities in cyberspace blurs lines between civilian security and military defense, and frontier militia models might prove of use. While this third spiral would depend on the trajectory of the technology and on our competitors' investments, we recommend opening the historical and conceptual aperture wide in seeking out appropriate models.

Cyber as the First Fruits of Talent Management

This analysis borrowed many principles from current pilot reform initiatives, and our further development of these concepts might enrich that discussion. The unprecedented distribution velocity and wide availability of information, democratization of violence (as seen in cheap and lethal quadcopters deployed by the so-called Islamic State and employed in Ukraine), and AI integration all serve to bring about a revolution in political, economic, and military affairs. Therefore, these principles, and perhaps even these polices, could be migrated toward these facets.

Still, one thing remains: humans are more important than hardware, and when considering the Third Offset Strategy, even if the joint force gets all the strategy and technology right, these will fail without the right people. With the right people and enough time, American warfighters will redeem and repair whatever strategies and technologies they are given. American society and culture powerfully apply technology to solve problems. Once again, a nation's strongest military is the one that can best leverage these societal strengths, and this requires change in how the joint force manages and empowers talent. Warfare is a human endeavor, amplified by technology, and the U.S. military must attract and retain people who understand technology to perform it well. **JFQ**

Notes

[1] See "SOF Truths," available at <www.socom.mil/about/sof-truths>.

[2] Max Weber, "The Essentials of Bureaucratic Organization: An Ideal-Type Construction," in *Reader in Bureaucracy*, ed. Robert K. Merton et al. (Glencoe, IL: Free Press, 1952), 19–21.

[3] Government Accountability Office (GAO), *Military Compensation: Additional Actions Are Needed to Better Manage Special and Incentive Pay Programs*, GAO-17-39 (Washington, DC: GAO, February 2017), available at <www.gao.gov/assets/690/682508.pdf>.

[4] Kris Osborn, "Air Force to Finalize New Cyber Mission Forces," Defense Systems, May 30, 2017, available at <https://defensesystems.com/articles/2017/05/30/air-force-cyber.aspx>.

[5] See "U.S. Marine Corps Forces Cyberspace Command," U.S. Marine Corps Concepts & Programs, available at <www.candp.marines.mil/Organization/Operating-Forces/US-Marine-Corps-Forces-Cyberspace-Command/>.

[6] Personal interview, Department of Defense (DOD) Cyber Leader, fall 2017.

[7] Michael V. Hayden, "The Future of Things Cyber," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton, FL: Taylor & Francis, 2013).

[8] Bernard Rostker et al., *The Defense Officer Personnel Management Act of 1980: A Retrospective Assessment*, R-4246-FMP (Santa Monica, CA: RAND, 1993), available at <www.rand.org/content/dam/rand/pubs/reports/1993/R4246.pdf>.

[9] Eric Schmidt and Jonathan Rosenberg, "How Google Manages Talent," transcript, *Harvard Business Review*, September 2014, available at <https://hbr.org/2014/09/how-google-manages-talent>.

[10] See "Modernizing HR at Microsoft," June 2015, available at <https://itshowcasecontent.blob.core.windows.net/pdffiles/3723_Modernizing_HR_at_Microsoft_BCS.pdf>.

[11] Michal Lev-Ram, "The Global Talent Crunch," *Fortune*, September 4, 2014, available at <http://fortune.com/2014/09/04/the-global-talent-crunch/>.

[12] Schmidt and Rosenberg, "How Google Manages Talent."

[13] David A. Garvin, "How Google Sold Its Engineers on Management," *Harvard Business Review*, December 2013, available at <https://hbr.org/2013/12/how-google-sold-its-engineers-on-management>.

[14] Vijay Govindarajan and Srikanth Srinivas, "The Innovation Mindset in Action: 3M Corporation," *Harvard Business Review*, August 6, 2013, available at <https://hbr.org/2013/08/the-innovation-mindset-in-acti-3>.

[15] James Kaplan, Naufal Khan, and Roger Roberts, "Winning the Battle for Technology Talent," McKinsey & Company, May 2012, available at <www.mckinsey.com/business-functions/digital-mckinsey/our-insights/winning-the-battle-for-technology-talent>.

[16] Katie Fehrenbacher, "Elon Musk's Vision Includes New Cars, Car Sharing, and SolarCity Deal," *Fortune*, July 21, 2016, available at <http://fortune.com/2016/07/20/elon-musk-master-plan-2/>.

[17] Simon Sinek, "How Great Leaders Inspire Action," video, 17.58, TEDxPuget Sound, September 2009, available at <www.ted.com/talks/simon_sinek_how_great_leaders_inspire_action>.

[18] Laura Arrillaga-Andreessen, "Five Visionary Tech Entrepreneurs Who Are Changing the World," *T Magazine*, October 12, 2015, available at <www.nytimes.com/interactive/2015/10/12/t-magazine/elizabeth-holmes-tech-visionaries-brian-chesky.html>.

[19] Michael Mankins, "How Leading Companies Build the Workforces They Need to Stay Ahead," *Harvard Business Review*, September 6, 2017, available at <https://hbr.org/2017/09/how-leading-companies-build-the-workforces-they-need-to-stay-ahead>.

[20] Tom O'Connor, "German Military Battles Foreign Hacking with New Cyber Soldiers," *Newsweek*, April 5, 2017, available at <www.newsweek.com/german-military-launches-new-cyber-division-amid-russian-hacking-claims-579573>.

[21] Andreas Maisch, "German Rolls Out New Cyber Defence Team," Euractiv, December 6, 2017, available at <www.euractiv.com/section/cybersecurity/news/germany-rolls-out-new-cyber-defence-team/>.

[22] Ibid.

[23] Ibid.

[24] James Stavridis, "Time for a U.S. Cyber Force," U.S. Naval Institute *Proceedings* 140, no. 1 (January 2014), available at <www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force>.

[25] Isabel Skierka, "Bundeswehr: Cyber Security, the German Way," ORF, available at <www.orfonline.org/expert-speaks/bundeswehr-cyber-security-the-german-way/>.

[26] Ibid.

[27] Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004), 237–256.

[28] Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Arlington, VA: Center for Naval Analyses, March 2017), available at <www.dtic.mil/docs/citations/AD1032208>.

[29] Ibid.

[30] Ibid.

[31] William Haynes, "NATO's Cyber Capabilities Are Only Defensive Without Cyber 'Red Lines,'" *Georgetown Security Studies Review*, September 28, 2016, available at <http://georgetownsecuritystudiesreview.org/2016/09/28/natos-cyber-capabilities-are-only-defensive-without-cyber-red-lines/>.

[32] Connell and Vogler, *Russia's Approach to Cyber Warfare*.

[33] Jose Nazario, "Politically Motivated Denial of Service Attacks," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, vol. 3, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009), 163–181.

[34] Ashton Carter, "Remarks to the Air Force Association," DOD transcript, National Harbor, MD, September 16, 2015, available at <www.defense.gov/News/Speeches/Speech-View/Article/617405/remarks-to-the-air-force-association/>.

[35] See "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, February 19, 2013, available at <www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>.

[36] Cao Siqi, "China Launches Cyber Security Talent Training Nationwide, *Global Times* (Beijing), September 20, 2016, available at <www.globaltimes.cn/content/1007158.shtml>.

[37] David Barboza, "Chinese Gymnast Endured Childhood Sacrifice," *New York Times*, August 5, 2008, available at <www.nytimes.com/2008/08/05/sports/05iht-gymnast.1.15012163.html>.

[38] Siqi, "China Launches Cyber Security Talent Training Nationwide."

[39] "APT1: Exposing One of China's Cyber Espionage Units."

[40] Franklin Spinney, *Defense Facts of Life: The Plans/Reality Mismatch* (Boulder: Westview Press, 1985).

[41] "Congress Probes Military Pilot Shortage," DOD, March 30, 2017, available at <www.defense.gov/News/Article/Article/1135200/congress-probes-military-pilot-shortage/>.

[42] Jack Moore, "In Fierce Battle for Cyber Talent, Even NSA Struggles to Keep Elites on Staff," Nextgov, April 14, 2015, available at <www.nextgov.com/cybersecurity/2015/04/fierce-battle-cyber-talent-even-nsa-struggles-keep-elites-staff/110158/>.

[43] Tim Kane, *Bleeding Talent: How the U.S. Military Mismanages Great Leaders and Why It's Time for a Revolution* (New York: Palgrave Macmillan, 2013).

[44] Ibid.

[45] Robert Work, "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence," transcript, DOD, available at <www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/>.

[46] N.A. Lomov, *Scientific-Technical Progress and the Revolution in Military Affairs (A Soviet View)* (Washington, DC: Headquarters Department of the Air Force, 1973).

[47] Brian Everstine, "Is Uniformity Needed for All in Uniform?" *Air Force Magazine*, October 13, 2016, available at <www.airforcemag.com/DRArchive/Pages/2016/October%202016/October%2013%202016/Is-Uniformity-Needed-for-All-in-Uniform.aspx>.

[48] Stavridis, "Time for a U.S. Cyber Force."

[49] Chris Busque, "Finding the Inside Track in the Race for Talent," RAND Project Air Force, Air Force Fellows Program, April 2018; and Tom Philpott, "The Arguments Behind New Tech-Track Career Paths," *Stars and Stripes*, August 20, 2015, available at <www.stripes.com/news/us/the-arguments-behind-new-tech-track-career-paths-1.363770>.

[50] Geert Hofstede, Gert Jan Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind*, 3rd ed. (New York: McGraw-Hill Education, 2010); and Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (Cambridge: Harvard University Press, 1957).

[51] U.S. House, *National Defense Authorization Act for Fiscal Year 2017*, Conference Report, 114th Cong., 2nd sess., November 30, 2016, available at <www.congress.gov/114/crpt/hrpt840/CRPT-114hrpt840.pdf>.

[52] Harold C. Hutchison, "Everything You Need to Know about the Merchant Marine," We Are The Mighty, December 10, 2017, available at <www.wearethemighty.com/military-life/everything-you-need-to-know-about-the-merchant-marine>.

[53] Wyatt Hoffman and Ariel (Eli) Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?* (Washington, DC: Carnegie Endowment for International Peace, June 14, 2017), available at <http://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236>.

[54] Catherine Lotrionte is currently Brent Scowcroft Scholar at the Atlantic Council with the Cyber Statecraft Initiative in the Scowcroft Center for Strategy and Security; see also "Catherine Lotrionte," available at <www.atlanticcouncil.org/about/experts/list/catherine-lotrionte>.

[55] Hoffman and Levite, *Private Sector Cyber Defense*.

[56] Crispin Burke, "The Pentagon Should Adjust Standards for Cyber Soldiers—As It Has Always Done," *War on the Rocks*, January 24, 2018, available at <https://warontherocks.com/2018/01/pentagon-adjust-standards-cyber-soldiers-always-done/>.

[57] Jeremy A. Rabkin and Ariel Rabkin, "To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict," Hoover Institution, January 19, 2012.