The Provision of Cyber Manpower
Creating a Virtual Reserve

Major Gregg Curley

Abstract: Cyber manpower demands raise challenges similar to other high-demand specialties. This article looks at the viability of adapting the manpower model of the Public Health Service's Reserve Commissioned Corps to the cyberdomain. A reserve paramilitary force could serve interchangeably across the military and interagency without law of war restrictions, would provide a lower-cost manpower option than full-time active duty, and could complement—not compete—with the civilian cybersector. Last, targeted training, education, and retention could shape this reserve force to meet emerging demands.

Keywords: cyber manpower, cyber and the military, history of cyber, military cyber reserve, public health service

First Google then Facebook went dark. Netflix, Yahoo, Twitter . . . the top 100 websites became unusable in quick succession. Banks, stores, and hospitals remained online but with degraded capability for a few hours—just long enough for all of the personal data to be taken. Cell phones became paperweights. Power plants started to go offline, and the electricity was intermittent across the country. Air traffic control was forced to ground flights, ground traffic was brought to a standstill as traffic signals jammed, and mass transit ceased to function. The economy literally stopped as the New York Stock Exchange

Maj Gregg Curley is a judge advocate for the U.S. Marine Corps. He earned his master of military operational art and science in 2017, master of laws in 2015, juris doctor in 2008, and bachelor and master of business administration in 2004 and 2005, respectively. Curley is presently assigned as senior trial counsel, Marine Corps Base Quantico, VA. His previous assignments include defense attorney, civil affairs team leader, aide-de-camp, and special assistant U.S. attorney. Maj Curley has been published in the *Marine Corps Gazette* and the *Army Lawyer*.

MCU Journal vol. 9, no. 1
Spring 2018
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.2018090108

(NYSE) and NASDAQ Stock Market suspended trading and the banks closed to prevent a run. The delivery of food and goods ceased and widespread looting ensued. It was complete chaos.

A coordinated and large-scale, state-sponsored cyberattack, such as the one outlined above, has the potential to be utterly devastating. The response requires a whole-of-government approach with a mechanism for mobilizing the best cybertalent in the country and surging talent to a specific problem set. Such a force should complement the military and be paramilitary in nature but should source from a broader section of society. The Public Health Service Ready Reserve Corps provides an adaptable model for the provision of top civilian cybertalent at a manageable cost.

History of Cyber

Unlike the other four domains (land, sea, air, and space), cyberspace—in all its forms—is less than a century old and entirely manmade. The Department of Defense (DOD) played such an integral role in the development of cyberspace, it would not be a stretch to credit the military with creating the domain. In a twist of irony, the DOD now has the responsibility of protecting a domain it helped create but lost control of once it was opened to the public at large. There are unique aspects of this domain that did not exist in any form 70 years ago. Understanding the genesis of the cyberdomain will provide context when determining how to best defend it from malicious attacks or incursions.

The first device to resemble a modern computer was Charles Babbage's 1834 design for an analytical engine.[1] Essentially, the analytical engine was a giant four-function mechanical calculator that utilized punch cards for inputting information and was capable of producing printed output. In 1943, during the height of World War II, a computer was built for the British military.[2] This computer, dubbed Colossus, was used to break the codes of the German Lorenz SZ40 cipher machine.[3] Colossus, as its name implies, was enormous—a by-product of its primitive vacuum tube technology.[4] Colossus and its vacuum tubes were characteristic of the first generation of computers, developed in 1937–46. Between 1947 and 1962, vacuum tubes gave way to transistors, and the second generation of computers was born. Second-generation computers had programming languages, memory, storage, and printing capabilities. Later, transistors ran their course and the integrated circuit ushered in the third generation of computers, spanning 1963–present.[5] However, cyberspace required one more crucial development that did not materialize until two decades after third-generation computers first appeared—the internet.

The history of the internet is also relevant to developing an understanding of the cyberdomain. With the development of the computer came the desire to transmit and receive information between computers. In the 1960s, the Cold

War forced the U.S. military to develop solutions for sharing information in the event of a nuclear attack. One of the solutions was the Advanced Research Projects Agency Network (ARPANET). ARPANET functioned like an archaic version of today's internet, but access was highly restricted—only the DOD and select contractors had access. A universal language for communicating among computer networks was developed—the Transmission Control Protocol/Internet Protocol (TCP/IP). On 1 January 1983, ARPANET officially adopted the TCP/IP language, and the internet was born.[6] The technological progress from the 1983 birth of the internet to the present is utterly mind-boggling.

Today, our technology has surpassed the then-futuristic wireless flip phones portrayed in *Star Trek*, there are justified concerns that Russia influenced elections in the United States using cybercapabilities, and autonomous vehicles will soon be commonplace.[7] The DOD's cyberstrategy explains, "We live in a wired world. Companies and countries rely on cyberspace for everything from financial transactions to the movement of military forces."[8] Millions have virtual presences via social media, virtual currency supports online commerce (i.e., Bitcoin), and the internet impacts issues of sovereignty, defense, transportation, human rights, commerce, and law. The internet permeates almost every facet of modern life.

The year 2000 provided a sobering waypoint illustrative of how interconnected the world has become and how important this domain is to our everyday lives. In the late 1990s, the United States mobilized to address a cyberthreat: the Y2K bug. When early computers were programmed between the 1960s and 1980s, they were programmed with only two digits to represent the year. The fear was that 1 January 2000 would cause significant problems in various fields such as transportation, energy, and banking as computer systems would incorrectly interpret the date as 1 January 1900 versus 1 January 2000.[9] This interpretive error was known as the Y2K bug. In response to this threat, the president formed a commission for Y2K conversion and civilian companies undertook significant reprogramming efforts.[10] While the fears associated with the Y2K bug never materialized, were overblown, or were avoided through diligent efforts, the Department of Commerce estimated the total cost of preparing for the Y2K bug at $100 billion.[11] In the ensuing 17 years, the level of interconnectedness, as well as the importance of the internet, has increased by orders of magnitude.

Cyber and the Military

Cyberspace was only formally recognized by the DOD as the fifth warfighting domain in 2005.[12] Air Force Lieutenant Colonel David T. Fahrenkrug, in his study titled "Cyberspace Defined," wrote that cyberwarriors "will be the recognized experts who understand the principals [*sic*] and techniques for conduct-

ing combat operations in cyberspace so that the [DOD] can deliver sovereign options for the defense of the United States of America and its global interests."[13] Because of the resources and lack of regulation that other nation-states and nonstate actors have, the DOD and the greater interagency need to be able to train, equip, and maintain a sufficient number of cyberwarriors to control and ideally dominate this domain. Raising and maintaining a skilled cyberforce is challenging, as the military is competing with the private sector, the training pipeline is extensive, and the work is highly specialized and technical. Additionally, the culture of the military and the modern technology worker are not wholly compatible. For a variety of reasons, traditional surge options (i.e., contracting, traditional reserve forces, internal sourcing, etc.), individually or combined, are suboptimal. The United States needs a cyber-specific ready reserve—a *Virtual Reserve*.

Defending a Domain

The DOD has identified three primary mission sets for its cyberwarriors: "[1] defend DOD networks, systems, and information; [2] defend the nation against cyber attacks of significant consequence; and [3] support operational and contingency plans."[14] To accomplish these three missions, the DOD will dedicate 6,200 personnel, divided into 133 teams sourced from across the Services.[15] An additional 2,000 cyberpersonnel will exist in the reserve forces.[16] On 24 October 2016, all 133 teams reached initial operating capability with approximately 5,000 trained personnel.[17] *Initial operating capability* means "all Cyber Mission Force units have reached a threshold level of initial operating capacity and can execute their fundamental mission."[18] The full cyberforce will be mission-capable in 2018.[19]

The 133 cyberforce teams are provided by the various Services: 39 from the Air Force, 41 from the Army, 40 from the Navy, and 13 from the Marine Corps.[20] These Service-sourced teams are task-organized to achieve the cybermission. Within that construct, there are 13 national mission teams, 68 cyber protection teams, 27 combat mission teams, and 25 support teams. The national mission teams defend the United States and its interests against cyberattacks of significant consequence.[21] These teams are tasked with developing intelligence and warning capabilities, partnering with the interagency to defend the United States in cyberspace, sharing information with the Department of Homeland Security, and accessing and improving the United States' deterrence posture.[22] Each national mission team consists of 64 personnel.[23] Cyberprotection teams defend priority DOD networks and systems against threats.[24] Each cyberprotection team consists of 39 individual team members, and each team will be task-organized specifically for a given mission.[25] The 27 combat mission teams provide support to geographic combatant commands by generating integrated

cyberspace effects in support of operational plans and contingency operations.[26] Each combat mission team is made up of approximately 60 personnel.[27] The remaining 25 teams are support teams that provide analytic and planning support to the national mission and combat mission teams.[28] Each support team consists of 39 individuals.[29]

Description of the Problem

When it reaches full operational capacity, the DOD will have a cyberforce equivalent to one and a half cyberbrigades; with the reserve capacity there will be two brigades or a similar-size entity.[30] This is the force that is required to sustain current operations—there is no built-in reserve capacity. Developing, maintaining, and training this force poses some unique challenges. The size and complexity of a cyberattack could quickly overwhelm the United States' cybercapability. Sustaining a two-brigade-size force of highly skilled, technical, and in-demand servicemembers is a difficult task. Sustainment of the force is imperative given the power parity in this domain; one hacker with an internet connection can potentially inflict more damage on the United States than the entirety of some nations' traditional militaries.

Cyber is a new domain. As the DOD's cyberteams are building to full operational capacity, now is the time to look to developing an effective and efficient bank of human capital that can be mobilized. Such a pool of talent is required to deal with contingencies in three distinct circumstances: sustained operations, specialized mobilizations (e.g., the Ebola outbreak and Stuxnet), and mass mobilizations (e.g., World War II and Vietnam).

Mobilization

Mobilizing military forces generally follows three macro models: sustained, specialized, and mass mobilization. These three methods and the attendant cybercomponent are analyzed to establish a baseline and identify weaknesses within the current cyberconstruct.

Sustained Operations

The DOD has identified issues related to sustaining the current force: (1) Cyberprofessionals possess a highly specialized skill set requiring both an aptitude for the work and extensive training; (2) individuals with the required skill sets are in very high demand in the civilian sector; and (3) the Services have started to take targeted measures to retain and attract proven talent in this area. Ashton B. Carter, then secretary of defense, stated in a speech, "Military leaders have long complained that it is difficult to attract and keep cyber professionals in the services because they can make far more money in private industry."[31] Issues with sustaining operations in the cyberdomain boil down to manpower, partic-

ularly staying competitive with the civilian marketplace and providing the right balance of incentives and retention techniques to maintain a competent force.

The military must compete for personnel with the civilian sector. Whenever changes to military retirement, pay, and/or benefits are analyzed, one of the most important metrics is the competitiveness of the total package with the civilian sector. A military consisting of only those servicemembers that are incapable of marketing their skills in the civilian sector would be a hollow and ineffective force. In high-demand specialized fields, the incentives must be great enough to attract and retain a critical mass of highly competent individuals that, while they could have lucrative civilian careers, choose to serve instead.

The fields with civilian analogues (e.g., pilots, lawyers, doctors, and now cyber) are fields where additional incentives and retention techniques are required from time to time to remain competitive with the civilian sector. For instance, the Services are authorized to offer doctors entry-level commissions ranging from the 0-3 to the 0-6 level.[32] To ensure a steady stream of doctors, health scholarships are offered across the Services.[33] Military pilots, who benefit from very expensive government-funded training, incur longer service obligations to ensure full recoupment of the government's investment, whereas doctors' initial obligations can be shortened to two years to entice them to join.[34] Bonuses are paid to high-demand military occupational specialties.[35] Promotion precepts are utilized to quickly fill vacancies in undermanned specialties and school incentives are provided as reenlistment bonuses.[36] Lateral moves from one military occupational specialty to another are used to generate middle management in fields with critical shortages.[37] Generally speaking, these and similar strategies allow for the forces to appropriately shape military manpower. The success of these programs is reflected by the fact that, after 16 years of war, the United States still possesses an all-volunteer force; the stop-loss policy ended almost 8 years ago and there has not been a draft since Vietnam.[38]

A current example of employing these various manpower-shaping tools is reflected in the Air Force's approach to its pilot shortage. Proposed solutions to this crisis include lobbying the Federal Aviation Administration to increase the number of flight hours before military pilots may be hired by civilian airlines, offering bonuses, increasing aviation pay, liberalizing awards, and allowing return to active duty opportunities.[39] While the cyberforce will ultimately number around 6,200, reaching that initial number has required use of some similar strategies. There is not an abundance of personnel with the required skill sets that the U.S. government could turn to in a national emergency at a reasonable price.

The military must source its cyberwarriors from the greater population. This is a daunting challenge as the U.S. cybersecurity job market is expected to grow from $75 billion in 2015 to $170 billion in 2020.[40] In 2016, more than

200,000 cybersecurity jobs, in all sectors, went unfilled and job postings increased 75 percent during the previous five years.[41] To open the aperture worldwide, there is a projected shortfall of 1.5 million cybersecurity jobs.[42] It is clear that the demand for cybersecurity professionals has outstripped the supply. Basic economics dictate these market inefficiencies will pose challenges for the buyers in a seller's market—and the U.S. government is a buyer.

The Bureau of Labor Statistics (BLS) lists the annual median salary for an information security analyst at $92,600.[43] By comparison, a 10-year gunnery sergeant (E-8) receives a total regular annual military compensation of $94,966.[44] An E-4 with four years in service (the end of an enlistment) sees total regular military compensation of $50,746.[45] If the basic allowance for housing is removed from the equation—assuming the servicemember is required to live in the barracks—the annual compensation package drops to approximately $37,000.[46] Leaders have recognized this: "For troops who are trained in cyber security, six-figure salaries will be easy to find in the civilian job market—and the services know that money will be one important element of retention. For example, the Marine Corps has set aside 16 percent of its total retention bonus budget for targeting its small but growing cyber force."[47]

While the compensation is not particularly competitive, especially at the lower ranks, the military does have a few advantages over the civilian sector. The military will provide training and education, whereas the civilian sector will generally expect a viable skill set prior to hiring. The military can provide money for college, food, shelter, tax advantages, travel opportunities, and health and dental insurance. There is also the ever-present pride that comes from serving. The military has already conceded to lawmakers that competing for talent with the civilian sector on the basis of pay alone is futile: "We are not going to compete on the basis of money. Where we're going to compete is the idea of ethos, culture . . . that you're doing something that matters, that you're doing something in the service of the nation."[48] These inherent competitive advantages to military service may be sufficient to generate and maintain a force of 6,200, but the drawbacks attendant to service, such as deployments, constant moves, danger, and Service standards, coupled with the lure of lucrative civilian options, will siphon off a large amount of talent and pose significant barriers to quickly increasing the force size. Cloaking service in the flag will only go so far. There are already indications and warnings that the current way of doing business will be inadequate vis-à-vis cyber manpower, as then-Secretary of the Air Force Deborah Lee James states: "We've made progress over the last year or two, but it's not good enough. We need to do more, to be open to different ways of bringing people on and retaining people so we can bring the best and brightest into our ranks."[49]

DOD leaders have proposed a variety of strategies to gain and maintain

parity with civilian-sector cybercompetence. Secretary Carter proposed colonel-level direct commissions for cyberwarriors, and the Air Force is exploring changing physical fitness standards for cyberpersonnel.[50] The Marine Corps is considering allowing cyberwarriors to bypass boot camp—a rite of passage in this Service.[51] The Marine Corps also will allow cyberwarriors to stay in the cybermilitary occupational specialty.[52] To civilians, each one of these initiatives appears to be a relatively innocuous force-shaping measure; however, each one runs counter to the culture of the Services. Many uniformed servicemembers were indignant over these proposed changes.[53]

The potential negative impacts to morale of favorable treatment afforded to cyberwarriors should not be underestimated. Napoleon Bonaparte famously stated, "There are only two forces in the world, the sword and the spirit. In the long run the sword will always be conquered by the spirit."[54] When building our cybersword, it must be done in such a way that does not weaken the overall military spirit. During the course of building the cyberforce, Lieutenant General Gina M. Grosso, deputy chief of staff for Manpower, Personnel and Services, U.S. Air Force, states, "How much brawn does the military need, and how much intellect? I think about a cyber warrior. Do I care what a cyber warrior weighs? Do I care if he can run a mile and a half in 12 minutes?"[55] If the goal is to build a cyberforce, the answer is no, the Air Force should not care. If the goal is to build an armed force with an integrated cybercomponent—because of the impact on morale and unit cohesion—the answer is yes, the Air Force should care quite a bit. Favoritism for one specialty can only be pushed so far before the rank and file will bristle at the disparate treatment for similarly situated individuals (e.g., Air Force E-4s from different occupational fields). The incentive scheme for an infantryman or a pararescue airman will quickly become inadequate if a cyberwarrior in an air-conditioned building can receive better pay, education benefits, and promotion opportunities while not shouldering similar personal risk or having to maintain typical military standards.

Culture and morale concerns are by no means limited to the Air Force. As the Marine Corps' mantra states, every Marine is a rifleman. While a pithy saying, because every enlisted Marine attends recruit training, it is also grounded in truth. Changing that accession pipeline solely for the cyberfield will strike a significant blow to Marine Corps culture. Aside from Marines that serve within Marine Corps Forces, Special Operations Command (MARSOC), all Marines are required to serve in "B" billets—jobs such as recruiters, drill instructors, or embassy security—to remain competitive for promotion, reenlistment, and retention. These changes would strike at the very heart of what it means to be a Marine. These strategies also run counter to the culture of the Service, erode morale, and marginalize other specialties. A solution that can satisfy manpower requirements without negatively impacting morale will be ideal.

Specialized Mobilization

Certain contingencies do not require the military to grow, but they do require surge capacity in a specific field. Additional personnel were required to support the response to the 2014–15 Ebola outbreak in Africa.[56] When the civilian air traffic controllers went on strike during the Ronald W. Reagan administration, military air traffic controllers were brought in to keep civilian airlines flying.[57] In the wake of Hurricane Katrina, the Army Corps of Engineers had a massive response to the relief efforts.[58] There is no such surge capability in the cyber-community. Offensive cyberattacks will become more numerous and complex, requiring more specialized manpower in the future. Any internal solution that does not come with additional manpower and funding represents an opportunity cost; the Services must make cuts elsewhere to resource the cybermission. The 133 cyberteams are all being used on sustainment missions.[59] Any emergent requirements will necessitate degradation to sustainment, contracting costs, or training additional personnel—all of which incur costs and delay.

Mass Mobilization

Mass mobilization of U.S. forces has not taken place since World War II. In assessing the capability for a mass mobilization, current assets, domain-specific surge strategies, and stop-gap measures must be assessed.

Existing Resources

If the hypothetical horde was to ride over the hill tomorrow and the United States was required to mobilize, the military would grow shockingly fast. In World War II, the Army alone grew from 174,000 to 11 million soldiers in the span of six years.[60] Such a proportional mobilization today would mean the Army would go from 541,000 to 34.2 million soldiers. Given modern societal norms, females would most likely be required to register for the draft, significantly increasing the pool of people eligible for military service compared to World War II. While a mass mobilization can occur relatively quickly, the United States will not blindly add manpower and capacity. The government has substantial mechanisms in place that allow for intelligent mobilization. Even in the direst of situations, the United States will not conscript doctors to pull triggers, linguists to sweep for improvised explosive devices, or pilots to captain submarines—that is inefficient, ineffective, and a losing strategy. When exploring the viability of creating a cyber reserve, it is informative to understand the various mechanisms the government will employ if an intelligent mobilization is required.

Ground Forces

In a massive mobilization, the standing military would be quickly augmented

with the reserve forces. The Army Reserve is 202,000 strong, and the Marine Corps Reserve boasts 39,200 members.[61] The Army also would nationalize the National Guard, which would instantly add another 350,200 to the rolls.[62] With these mechanisms alone, the size of the standing army could more than double overnight. These forces are already trained, equipped, and organized into units.

For additional instant manpower, members of the Inactive Ready Reserve—"a manpower pool consisting mainly of trained individuals who have previously served in [active component] units or in the [selective reserve]"—could be called up.[63] Military members who have retired could be called up with a mobilization of the retired reserve.[64] As was done in World War II, the curriculum at the Service academies and Reserve Officers' Training Corps could be truncated to provide additional entry-level officers.[65]

Naval Forces

Naval forces would be increased in a fashion similar to the ground forces, calling on all components to activate and then relying on conscription for new recruits. Additionally, the Coast Guard would transfer from the Department of Homeland Security to the Department of the Navy.[66] An additional resource pool would be the Coast Guard Auxiliary.[67] The Merchant Marine also would be nationalized under the Department of the Navy to provide shipping and transport capacity.[68] For ships, the Reserve Fleet—retired warships—could be returned to service appreciably faster than building new ships. The Reserve Fleet consists of 46 vessels that the United States keeps in "mothball" status in the event there is a national emergency.[69] These ships are kept in various stages of maintenance. Additionally, there is a 99-ship National Defense Reserve Fleet (NDRF)—commercial vessels that sit at anchor and are kept ready for military use as troop or cargo transport.[70] As with the Reserve Fleet, these ships could be pressed into service appreciably quicker than building or requisitioning new ones.

Growing the U.S. Navy through reserves will take longer than growing the ground and air forces through reserves due to the different hurdles they must overcome. Even mothballed ships would require time before they could be recertified and activated. To compensate for lack of sea duty time, active duty crews would need to be paired with reservists, and the crew as a whole would need to pass their certification. Even with the domain-specific lag times associated with mobilization, the U.S. Navy would still outpace other nations in growing the size of the force. The Navy is the most powerful blue-water navy in the world.[71] Because the Service will start from a position of advantage and has such programs as the Naval Reserve, the Reserve Fleet, and the NDRF, the U.S. Navy would maintain a significant competitive advantage relative to potential

adversaries. Mobilizing the full might of the Navy's reserve options would be a massive undertaking that would only be initiated if a conflict were against an adversary that boasted a formidable blue-water navy and the conflict had a long projected duration—otherwise mobilization would be a waste of time and resources.

Air Power

The Air Force will quickly augment with members of the Air Force Reserve and the Air National Guard. The Civil Air Patrol (the Air Force Auxiliary) would see its civilian mission expand.[72] For assets, the Air Force has the Civil Reserve Air Fleet (CRAF). The CRAF is a fleet of civilian airliners that can be pressed into national service in a time of war if the military's airlift capabilities are inadequate. The federal government also contracts with civilian airlines directly for troop transport.[73] Similar to the Navy, the Air Force maintains a mothballed fleet.[74] This fleet is located at Davis-Monthan Air Force Base, Tucson, Arizona, and contains assets that can be updated, refurbished, or fixed relatively quickly and pressed into service if required.[75] Each of these mobilization options capitalize on existing trained manpower and equipment.

New Resources

The military would need to martial new resources in the event that a major mobilization were needed—both materiel and manpower.

Materiel

One of the United States' greatest assets is its economy. The military-industrial complex would be expected to satisfy the need for additional equipment. In World War II, American industry was able to successfully construct a troop transport ship in just four days.[76] Today, the U.S. economy is the largest and most powerful in the world. The size and breadth of the country ensures it has ample supplies of natural resources and power required for manufacturing. The nation's economic might is so great that a tank factory is kept running, not because more tanks are needed, but to ensure that if tanks are needed they can be produced without the delay of having to retool a factory and relearn the lost manufacturing skills.[77] The U.S. economy, under most conditions, is capable of out-building, out-resourcing, outspending, and outlasting our military enemies.

Personnel

Such a large-scale mobilization would also require personnel. Enlistment waivers would become both more lenient and more prevalent. Additional new manpower would be added through conscription. Congress would pass legislation

authorizing a draft.[78] Once the legislation is passed, the Selective Service will activate its reserve officers and a lottery will start drafting registered individuals.[79] A draft would require a significant catalyst to become politically palatable; however, if conditions necessitated one, a draft would provide a substantial influx of personnel.

While an all-hands mobilization effort would be effective, there are inherent inefficiencies. By definition, a U.S. military draft is a lottery. The manpower will increase, but it will not increase in direct proportion to the need in certain fields (e.g., medical, legal, and cyber). To ensure that a conscripted force is the most effective it can be, mechanisms need to be in place to guarantee optimized assignments across all military occupational specialties. In sum, it is not about the sheer size of the force; how it is shaped is equally important. A force without sufficient shaping is a horde; a force without sufficient quantity is easily marginalized, bypassed, or defeated (i.e., ineffective).

Across the traditional domains, the United States has a well thought out mobilization plan. This smart approach to mobilization is a national security hedge—it allows for a smaller standing military because a high-capacity military is waiting in the wings—and an absolute behemoth can be mustered in a very short period of time. Given the interconnectedness of today's society and potential damage an attack in the cyberdomain could inflict, an intelligent mobilization plan for this domain should be developed.

Select Solutions

Recognizing that a need to quickly increase number and capacity of the country's cyberwarriors is a likely contingency, an analysis of select solutions follows: (1) maintain the status quo, (2) contract any shortfalls, and (3) create a cyber-specific reserve force.

Status Quo

The first and least expensive option is to maintain the status quo. If and when a situation presents itself that requires more cybercapacity than the United States can bring to bear, traditional methods of addressing the capability gap will be utilized. At the entry level, these methods include increased recruiting incentives, truncated training pipelines, enlistment bonuses, and even direct accessions. At the force-sustainment level, retention measures include stop-loss clauses, retention bonuses, promotions, awards, return to active duty opportunities, and schooling. Contracting will be used to address gaps present in the active force until the active force can recruit, train, and resource the shortfalls.

The drawbacks to maintaining the status quo include the potential for a drop in morale as cyberwarriors in effect become conscripts through programs such as stop-loss—where servicemembers' active duty commitments are unilat-

erally extended by the government—or selfless sacrifice is subsumed by obligation garnered through retention incentives so lucrative that freedom of choice is illusory. In addition to the morale drop in the maintained force, any training of new troops will have a very long pipeline. The training pipeline will vary depending on the required skill set; in any event, additional and effective new manpower could not be applied to the capabilities gap without a significant lag time. Any required additional capacity that cannot be generated in a timely manner or maintained long-term within the military will need to be contracted.

Contracting Solution

One option is to contract for cyberwarrior services. In an age where a contract infantry can be created, a cyberforce could likewise be contracted.[80] If the United States needs firewall protection for critical infrastructure, programmers for defense satellites, or countermeasures to corporate contractor espionage—contract it. This has been a solution to bridge manpower and expertise shortfalls in the past, as James Lisher notes: "[C]ontractors were used to support new weapons systems in [Operation Iraqi Freedom] OIF and [Operation Enduring Freedom] OEF. The dynamic nature of these contingencies resulted in employment of new weapons systems before the uniformed Services were manned to support them. Contractors, again, were used to fill this capabilities gap."[81]

Contracting does come with significant drawbacks. These drawbacks are highlighted by the high-profile leaks of classified information by contractors Edward J. Snowden and Reality Leigh Winner.[82] Granted, this problem is not isolated to contractors. Then-U.S. Army Private Chelsea Manning released significant classified material but, generally speaking, there are relatively few military prosecutions for leaks.[83] The United States will need to develop better ways of securing networks and information while also ensuring that control of the domain is not ceded to the contractors. One way to accomplish this is to decrease reliance on contractors.

Military contractors in the cyber realm also are subject to limitations placed on U.S. civilians relative to warfare. Civilians—including contractors—are barred from conducting offensive cyberattacks because "a cyber network attack [CNA] is 'a category of fires employed for offensive purposes in which actions are taken through the use of computer networks to disrupt, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/networks themselves.' CNA is the manifestation of combat operations in the cyber realm."[84] CNAs may only be executed by uniformed personnel.

At the macro level, the requirement for military personnel stems from the *Tallinn Manual*—NATO's analysis of the law of armed conflict as applied to the cyberdomain. The *Tallinn Manual* states in Rule 20: "Cyber operations

executed in the context of an armed conflict are subject to the law of armed conflict."[85] The law of armed conflict "bestows legal protections as a full-fledged combatant, which has implications that range from ensuring prisoner-of-war status under international law to immunity from prosecution in court."[86] U.S. contractors conducting CNAs would be state-sponsored criminals, which would violate the Geneva Conventions. Violations of the Geneva Conventions would undermine the entire treaty, potentially expose all of our servicemembers to terrible atrocities, and would do irrevocable harm to the law of armed conflict.

To comport with the treaty and ensure appropriate legal protections under the law of armed conflict, DOD policy holds that only uniformed servicemembers conduct certain types of attacks. These operations are considered inherently governmental (IG), which "is defined by the Federal Activities Inventory Reform Act of 1998 as 'a function so intimately related to the public interest as to require performance by Federal government employees'."[87] In a military context, IG functions include: "plan[ing], prepar[ing], and execut[ing] operations to actively seek out, close with, and destroy a hostile force or other military objective by means of . . . employment of firepower and other destructive and disruptive capabilities."[88] Offensive network attacks are specifically listed as a planned use of destructive combat capabilities under *Department of Defense Instruction (DODI) 1100.22, Policy and Procedures for Developing Workforce Mix*.[89] This construct is problematic when a force is mixed military/contractor. A military member must be the one to carry out the attack.

It makes sense that if the U.S. government is waging war on another sovereign or entity, the individuals conducting the actions should be a part of that government. As the *DODI 1100.22* states, "The U.S. government has exclusive responsibility for discretionary decisions concerning the appropriate . . . use of destructive or deadly force on behalf of the United States."[90] This retention of responsibility stems from the high-stakes life-and-death nature of warfare, liability for destruction and damage, and the critical national interests implicated by combat operations.[91] To ensure appropriate decisions are made, decision-making authority may only be delegated to military commanders; military commanders are held accountable for their decisions, they receive extensive military training, and they are held responsible for the training and readiness of their force.[92] The government can exercise limited control over contractors with the only recourse short of criminal action often confined to economic measures: cancel the contract or withhold payment(s).

Cyber would not be the first area in which the government has turned to contracting to fix an emerging need. Contracted cooks, security, sanitation, billeting, and linguists have been and currently are a pervasive presence in Afghanistan. However, the cyberdomain poses special challenges to contracting. As James R. Lisher II points out in an article for the *Journal of Contract Man-*

agement: "In the past, the DOD faced similar challenges using contractors to fill emergent personal security and interrogation needs following the launch of Operation Iraqi Freedom. The DOD must not rush to fill cyber capability gaps without doing a proper manpower analysis to prevent the outsourcing of inherently governmental functions."[93] To the extent the government contracts for cyberservices, a careful analysis of specific missions and functions must be conducted to ensure compliance with the law of armed conflict, policies, and directives.

Another drawback to contracting stems from the fact that many cyber issues are new, unique, and require a time-sensitive response. It is nearly impossible to contract for services and capabilities that are undefined until they are needed. Take for instance the Mine-Resistant Ambush-Protected (MRAP) tactical vehicles of OIF and OEF vintage. At the start of those conflicts, the thin-skinned High Mobility Multipurpose Wheeled Vehicle (HMMWV) was the tactical vehicle of the Services. A procurement program for an up-armored, V-hulled, desert-combat vehicle would have been summarily rejected in 2000. However, by 2005, as the enemy employed improvised explosive devices, it quickly became apparent that HMMWVs were a liability. Once the need was identified, an up-armored, V-hulled, desert-combat vehicle was quickly designed, procured, assembled, and delivered—the MRAP. The MRAP, a solution to an unanticipated need, became a model for expedited government procurement.[94]

Last, contracting is an expensive option. While the legacy costs in contracting are not a concern for the government, contractors will require more up-front money to compensate employees for this risk. Additionally, the more dire the need, the more the cost; this is basic economics. Contractors cannot be deployed anywhere strictly by executive fiat like the military—companies must entice them, and they do so with money. These financial considerations would render a contracted cyberforce an expensive option—an option that still may not be able to generate real-time effects for unanticipated cyberthreats or legally conduct the types of operations needed, all while simultaneously exposing the United States to a higher information-security risk. Undoubtedly, some contracting will be required, as it always has been in warfare. However, a more robust government cadre of skilled cyberprofessionals needs to be readily available to address emergent threats. Avoiding a foreseeable overreliance on contracting will provide more sovereign options to the United States while enabling the United States to be proactive in its cyberstrategy rather than reactive.

Reserve Capacity

The United States could increase the capacity of DOD and interagency cyberwarriors through a specialized reserve force. Reserve forces have their genesis

in the military medical community. Prior to the Spanish-American War, the military retained enough doctors to satisfy the peacetime mission. During the war, the Army turned to contracting the capability. However, drawbacks to contracting physicians quickly became evident—most notably the lack of flexibility with regard to where and under what conditions they would work. The solution to this problem was to offer reserve commissions to physicians who agreed to be activated in a time of war. This part-time construct for gaining and maintaining qualified personnel was so effective that it morphed into today's Army Reserve—a force of approximately 450,000.[95]

Reserve forces, because they are on a retainer, are significantly less expensive than standing armies—some estimates quantify activated reserve forces at only 80 percent of the cost of active duty servicemembers. The reductions in cost are mostly attributed to reduced retirement obligations and reduced support costs (e.g., schools, housing, etc.). The reserves provide unique levels of experience and maturity that members acquire in the civilian sector. The greatest advantage to such a reserve force is the ability to shape the expertise contained within the force for a relatively low cost. If more network professionals are needed, offer scholarships in this field in return for a Service commitment. If the technology is changing, take high performers and send them to specialized schools. Offer bonuses in high-demand areas, recruit specific skill sets, or offer direct commissions to attract the talent necessary. As covered when addressing manpower, a variety of incentives can be used by the U.S. government to build and shape the force when it exists in a reserve capacity.

The drawback to a traditional reserve force is that it would require military standards—difficult for some of the more desirable cyberwarriors. For example, it is unlikely regulation haircuts and cybersecurity skills are positively correlated; however, the requirement for regulation haircuts may be negatively correlated with recruitment. In the cyberdomain, typing speed is more important than foot speed. A great cyberwarrior may be paralyzed from the waist down—currently that recruit would not be eligible for military service. There are other physical, mental, and training standards that are necessary for a traditional kinetic force that may be counterproductive to developing and maintaining a cyber-specific force. Doing away with some of the standards for one specific subspecialty is anathema to the military culture—the traditional reserve forces are subject to this constraint. This culture clash is represented by comments made by the commanding general of Marine Corps Forces Cyberspace Command: "You can let them in with purple hair but we're going to shave it off anyways and plug up whatever holes [piercings] they have if they're smart enough."[96] The problem is if the purple-haired cybergenius is in fact smart enough, there are sufficient civilian opportunities that are more lucrative and will not require them to shave their head and plug their holes.

Reserve military service within the interagency is not very seamless. Billets must be created, funding dedicated, and manpower applied. Every reserve member that is provided to another entity is one less that the unit can utilize to accomplish its primary mission. A reserve cyberunit would rightly demonstrate institutional inertia with respect to fragmenting the force and distributing it across the interagency. Additionally, military members are specifically prohibited from conducting certain activities (law enforcement), and congressional appropriations with specific earmarks further limit interoperability of a military force.

Proposed Solution

A hybrid of the three options provides the best solution. The standing cyberforce needs to remain competitive across the board. The force must be continuously shaped and honed. If a requirement emerges that necessitates a surge in cybermanpower, the traditional methods of incentives, training, and compulsion should be employed to organically grow both force and capacity. Special cyber reserve units will provide additional cybercapacity while also serving as a low-cost means for retaining trained personnel whose active duty commitments have been fulfilled. Contracting should be utilized to supplement the active and reserve forces and to bridge any capability gap while buying time for the military to increase capacity. All three options are currently being pursued in earnest; however, an additional nuance—a nonmilitary specialized reserve cyberforce—should be added to the mix to maximize capability while minimizing cost.

A specialized reserve force should be created that provides a low-cost nonmilitary option for sourcing some of the best talent in the cybersector. Such a force already exists in the medical community. In addition to military active duty, reserve, and contracted medical personnel, a complementary nonmilitary specialized reserve exists to supplement the medical field across the interagency: the Public Health Service. This effective model can be adapted to cyberwarfare and will address the remaining drawbacks of the current three-pronged approach.

The Public Health Service Model

An existing model could be adapted to provide cybermanpower. The Reserve Commissioned Corps of the Public Health Service, a paramilitary organization, provides the United States and the interagency with a bench of qualified manpower, at a lower cost, and without the legal restrictions of contractors.

History

An Act for the Relief of Sick and Disabled Seaman was signed into law by President John Adams in 1798. This law required American ships entering a U.S.

port to remit a portion of each seaman's salary on arrival. The funds collected in this manner were used to create hospitals for sick and disabled seamen and fund doctors to care for them.[97] In 1889, Congress approved the Public Health Service (PHS) Commissioned Corps to constitute the uniformed arm of the Marine Hospital Service. The PHS Commissioned Corps was organized with rank and authority in the same manner as the military, and the PHS officially became one of the uniformed services of the United States. The name was shortened to the Public Health Service in 1912 and the mission set was expanded to include sanitation and preventive medicine.[98]

Like most government entities, the PHS expanded during World War II. In addition to doctors, it received authorization to commission nurses, dieticians, physical therapists, scientists, and public health officers.[99] Today, the PHS consists of 6,700 uniformed officers.[100] The PHS has responded to a laundry list of significant events over the past decade:

> The [PHS] Corps has deployed to events ranging from terrorist events (9/11, Boston Marathon Bombings, anthrax) to natural disasters (Hurricanes Katrina, Rita, Wilma, and Sandy; Red River flooding; Northeast ice storms); from humanitarian assistance (Haiti and Japan earthquakes, Indian Ocean tsunami) to reconstruction and stabilization (Iraq, Afghanistan); from public health crises (H1N1, suicide clusters on Indian Reservations) to hospital rescue (Mariana Islands). Over the past 10 years, the Corps has undertaken over 15,000 officer deployments in support of nearly 500 distinct missions and events.[101]

The most recent deployment by the PHS was to provide support to Hurricane Harvey relief efforts in the Houston, Texas, area.[102]

Section 5210 of the Patient Protection and Affordable Care Act of 2010 established a Ready Reserve Corps within the PHS.[103] Functionally, the Ready Reserve Corps of the PHS is designed to be a low-cost supplement to the active duty force designed for "service in time of national emergency."[104] This ready reserve has not been fully implemented; however, the Ready Reserve Corps of the PHS is the proposed model for low-cost and highly effective cybersurge capacity because it presents many unique mechanisms that do not exist in the cyber domain.

Interoperability

While not technically a military Service, the interoperability between the DOD and the PHS was on full display during the Ebola outbreak of 2014–15. The PHS mobilized and provided rotating 70-man teams for 60-day deployments.[105]

The PHS does not have a logistics arm, so the DOD provided that capability, as Rear Admiral Lushniak explains: "DOD will provide support for the officers, including billeting, food, water, and other basic living support. DOD construction of an Expeditionary Medical Support (EMEDS) unit included adaptations for infection control, plumbing, septic systems, structures for the family visitation centers and behavioral health counseling, and security measures."[106]

The military already has doctors in the Army, Navy, Air Force, and respective reserve components. From time to time, the military calls on PHS doctors to provide services, as does the greater interagency. This ability to provide medical surge capacity is valuable, as evidenced by the fact that the PHS is an asset the United States has utilized for 220 years. The PHS/DOD construct recognizes the requirement for an organic medical capability within the military, yet provides a complement to the existing active duty and reserve cadre of military doctors and health support personnel.

Deployability

The PHS is unique in both the United States and across the world. The PHS "Corps officers . . . can be deployed at a moment's notice anywhere in the world to meet the needs of the President and the Department of Health and Human Services."[107] Members can be ordered to communicable disease hotspots, military conflicts, humanitarian missions, or any place on Earth they are required. While the mission set of the PHS may be unique, there are nuances to its manpower structure that make such a format very valuable to cyberwar fighters.

Whole of Government

The PHS primarily supports the myriad programs administered by the Department of Health and Human Services; however, PHS also supports the DOD. Additionally, PHS serves almost interchangeably across the interagency. Currently, members of PHS serve with the District of Columbia, the Environmental Protection Agency, the Federal Bureau of Prisons, the National Oceanic and Atmospheric Administration, the National Park Service, the U.S. Department of Agriculture, the U.S. Department of Homeland Security Division of Immigration Health Services, the U.S. Coast Guard, and the U.S. Marshals Service.[108] The ability to plug and play across the interagency is a relatively unique role within the executive branch and a concept that could be of great value in certain areas (i.e., engineering, cyber, etc.).

Flexibility

Clearly, PHS serves across the interagency. If the Coast Guard can be said to live a dual existence (Title 14, law enforcement and Title 10, military), PHS lives a multifaceted existence. When serving with a different interagency entity,

PHS members are not subject to the same restrictions as the military. For instance, the military is prohibited under the Posse Comitatus Act of 1878 from enforcing domestic law. PHS members serving with the Department of Justice would not be subject to the Posse Comitatus Act, because they would not be a force specifically prohibited by statute from enforcing domestic law.[109] While the image of doctors enforcing the law might be hard to imagine, a cyberforce could, and most likely would, be involved in domestic law enforcement; in that case, the distinction does matter.

Based on the *Tallinn Manual*, the law of armed conflict applies to actions in cyberspace.[110] The law of armed conflict has significant implications in the cyberdomain. Members of the armed forces enjoy combatant status, which entitles them to combatant immunity and prisoner of war status.[111] Cybercontractors or civilians who are not members of the armed forces would be classified as "unprivileged belligerents" and afforded no protection under the law of armed conflict.[112] The PHS mission set does not authorize its members to conduct offensive military operations; however, as a paramilitary organization, if PHS members were authorized to conduct offensive military operations, they would be afforded the protections of the law of armed conflict.[113] A paramilitary cyberforce authorized to conduct offensive operations would enjoy the protections of the law of armed conflict.

Centralized Control

PHS is answerable to the surgeon general. The surgeon general is responsible for training, equipping, and manning the force. The benefit of having a specialized force answerable to one individual is that it promotes unity of effort. PHS still maintains administrative control over its members when assigned to the interagency. While interagency PHS members are answerable to the supported entity chain of command, there are still lines of communication to PHS and the surgeon general.

Standards

As a uniformed service of the United States, PHS has its own standards and regulations. For instance, the physical fitness requirements are different from other Services.[114] PHS, as a standalone organization, has its own eligibility criteria, award system, and policies. It does utilize sea-service uniforms and military pay and benefit schemes, but it maintains a distinctly unique service culture. This culture is very effective in addressing the simple and direct PHS mission: "protect, promote, and advance the health and safety of our Nation."[115] The PHS construct will translate nicely to the cyberdomain—a domain that would benefit from a similar laser-focused mission.

Adaptation of the PHS Model to Cyber

A Virtual Reserve modeled after the PHS would have many beneficial attributes. First and foremost, a Virtual Reserve would consist of a small—but not insignificant—force that can be pressed into service with minimal delay. There would be no requirement for recruitment or training delays before being able to instantly use the skill sets of these individuals. Members of the Virtual Reserve would be subject to orders just as with any other uniformed Service and receive the benefits and protections of the Uniformed Services Employment and Reemployment Rights Act of 1994.[116]

Second, no matter how technologically advanced or interconnected the world may become, the trigger puller will not become obsolete. Relaxing standards for an occupational field (as opposed to a Service) would create a special class within a Service that does not have to follow the same rules or live up to the same expectations as their peers. Such a construct would have a devastating impact on morale, readiness, and ultimately warfighting prowess. These concerns would be moot if this special class belonged to a unique nonmilitary uniformed service with its own homogenous culture, norms, and standards. Such a service would better navigate the tension between cyberdomain operational requirements and the available talent pool. The Virtual Reserve could promulgate Service-specific standards and requirements that ensure the nation is receiving the correct mix of brawn and intellect in the cyberdomain. Such a construct would also appeal to individuals in a lucrative career field that feel compelled to serve without the full commitment attendant to traditional enlistment or commissioning options. A cybersecurity executive could unlock a military retirement, health insurance, and benefits while still maintaining a civilian career. The United States can benefit from that executive's knowledge and expertise at a fraction of the cost relative to purchasing it on the open market.

Third, the prohibitions on law enforcement present in the military would not apply to this service—similar to the Coast Guard. If a criminal cyberincident of national importance were to emerge, there are no restrictions on the Virtual Reserve assisting the Federal Bureau of Investigation; the Department of Justice (DOJ); the Bureau of Alcohol, Tobacco, Firearms and Explosives; Federal Marshals; or any other law enforcement entity. Criminal cyberattacks are quite common; just this year, there have been major ransomware attacks (Wannacry and Petya), leaks (voter records, Cloudbleed), and hacking (Central Intelligence Agency [CIA], President Emmanuel Macron's campaign in France, and the National Security Agency [NSA]).[117] The United States must be able to mobilize a surge capability to help prevent, fix, patch, thwart, and counter these criminal attacks and then assist in identification, investigation, and prosecution of the criminal perpetrators.

Fourth, the proposed model comports with the law of armed conflict. A cyber reserve—even if it is generally a nonmilitary force—may lawfully participate in hostilities and receive protections: "[A] party to a conflict may incorporate a paramilitary or armed law enforcement agency into its armed forces."[118] The *Tallinn Manual* clarifies further that "once such groups have been properly incorporated into the armed forces, their members may conduct cyberoperations to the same extent as members of the regular armed forces."[119] As a uniformed service of the United States, members of this service component could conduct inherently governmental functions—including offensive network attacks.

Fifth, such a force may be shaped through all of the aforementioned manpower-shaping tools. If the force projects a shortfall in programmers, then tailored recruitment and scholarships, coupled with retention bonuses and lateral moves, would adequately address the capability gap. If top-level IT leadership is lacking, offering direct commissions at the 0-6 level for a Google or Cisco executive would be an option. High-level direct commissioning in a new and specialized force that specifically authorizes it would avoid some of the problems inherent in utilizing the same construct in the established military hierarchy. The message that is sent to a 20-year lieutenant colonel with three combat tours if the Air Force made a civilian Google executive an overnight colonel would be that the lieutenant colonel's contributions are not valued as much. Contrast that with a direct commissioned 0-6 in a reserve cyberentity with specified policies for specific skill sets within the domain. In that hypothetical situation, the stated policies would prevent an equivalent morale drop and would not alienate the rest of the force. It is the practical difference between creating a GS-15 position versus disregarding Service culture, tradition, and hierarchy.

Sixth, current cybermodels exist in stovepipes. The CIA and DOJ cyberteams have significantly different missions than DOD cyberteams. The DOD is not aware of what the CIA and DOJ are doing unless those entities are task organized for a specific crisis. Additionally, there is no unity of effort or unity of command. A Virtual Reserve with a centralized surgeon general-equivalent and personnel assigned throughout the interagency would facilitate the sharing of information and best practices. If a whole-of-government approach were needed, members of this Virtual Reserve would be ready-made liaisons with built-in unity of command/effort.

Finally, the cost of a reserve cyberforce would be much less than a standing force of equivalent size and capability. The civilian talent pool, including academia, has the inherent expertise and currency required for success in a free market. Tapping into that talent pool would generate cost savings over the alternative—training and maintaining an equivalent-size active duty force capability. The standing support costs associated with an active force would be avoided; this reserve force would be the same as any other reserve entity from

the perspective of personnel costs. Additionally, there could be some other creative cost savings that are unique to the domain. When an internet connection and a computer are all that are needed to access the domain, crowd sourcing, teleworking, and various other cost-saving measures become viable options.

Recommendation

The United States should establish a nonmilitary reserve uniformed service that contains a cadre of highly skilled cyberwarriors. This entity should resemble the envisioned Ready Reserve arm of the PHS—a cadre of highly skilled medical professionals that can complement the armed forces' active and reserve medical personnel but also serve across the interagency. This paramilitary force would enjoy the benefits and legal protections associated with military service, while also operating under a unique culture and set of standards that facilitate fielding the most capable force for mission accomplishment in the cyberdomain. Once such a force is established, it can be shaped through a variety of incentives to ensure it has the correct mix of talent, competence, and leadership. This Virtual Reserve would provide surge capacity when needed by the military for offensive network attacks or military network defense, while benefiting from the protections afforded to lawful combatants. Additionally, this force would be equally adept and employable in combating corporate espionage on behalf of the DOJ, gathering intelligence for the CIA, or preventing data breaches at the Office of Personnel Management; essentially, this force would provide support to any agencies and/or mission sets that the president may direct. The Virtual Reserve would serve as the cyberdomain's quick reaction force—capable of being employed on a national scale without the limitations of contractors, legal liability of civilians, or encumbrances placed on military personnel.

Conclusion

Regardless of the domain, a trained, skilled, and effective pool of manpower is required. There is nothing so unique about the cyberdomain that it should be the exception. Colonel Walt Yates describes this point effectively in his *Marine Corps Gazette* article entitled "Affordable and Effective Cybersecurity": "[W]e have treated cyberspace as a mystical warfare domain with properties that are different from three-dimensional battle space. In truth, there are far more similarities between warfare in cyberspace and three-dimensional space than there are differences."[120] Similar to the other domains, the cyberdomain will need the ability to increase manpower quickly and efficiently, but in a manner that takes into account the unique aspects of the cyber domain. The U.S. government must find a way to cost-effectively capitalize on civilian expertise, use that expertise interchangeably across the DOD and interagency, and tap into that expertise very quickly. Accomplishing this will require an entity that

would be open to a wider talent pool than the traditional military force. In the health field, that model exists in the Public Health Service's Commissioned Corps Ready Reserve; a similarly organized and employed cyber reserve should be created—a Virtual Reserve.

Notes

1. See generally, "The Babbage Engine: The Engines," ComputerHistory.org.
2. Beverly Steitz, "A Brief Computer History," Introduction to Computers, Boston University, fall 2006.
3. "Colossus: Birth of the Digital Computer," CryptoMuseum.com, 24 February 2018.
4. "Colossus."
5. Steitz, "A Brief Computer History."
6. "A Brief History of the Internet," Online Library Learning Center, USG.edu, accessed 26 August 2017.
7. "How Startrek [*sic*] Inspired an Innovation—Your Cell Phone," Destination-Innovation.com; Nicole Perlroth, Michael Wines, and Matthew Rosenberg, "Russian Election Hacking Efforts, Wider than Previously Known, Draw Little Scrutiny," *New York Times*, 1 September 2017; and Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution Act (SELF DRIVE Act), H. R. 3388, 115th Cong. (2017). The House unanimously passed the SELF DRIVE Act on 6 September 2017.
8. *The DOD Cyber Strategy* (Washington, DC: DOD, 2015), 1.
9. "Y2K Bug," NationalGeographic.org, 27 August 2017.
10. See William J. Clinton, "Amendment to Executive Order 13073, Year 2000 Conversion," E.O. 13127, *Federal Register* 64, no. 116 (17 June 1999): 32, 793.
11. Dennis O'Brien, "Price to Kill the Y2K Bug: $100 Billion," *Baltimore (MD) Sun*, 23 December 1999.
12. "Preface," in *Cross-Domain Synergy in Joint Operations, Planner's Guide: United States Joint Staff Joint Force Development (J7)—Future Joint Force Development* (Arlington, VA: Joint Chiefs of Staff, 2016).
13. LtCol David T. Fahrenkrug, USAF (Ret) "Cyberspace Defined," Air University, Air Force, 17 May 2007.
14. *The DOD Cyber Strategy*, 3.
15. *The DOD Cyber Strategy*, 6.
16. Mark Pomerleau, "DOD's Long Path to Creating a Cyber Warrior Workforce," *Defense Systems*, 4 March 2016.
17. U.S. Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operating Capability," press release, 24 October 2016, hereafter DOD press release.
18. DOD press release.
19. "Cyber Strategy," Defense.gov, accessed 27 April 2018.
20. Mark Pomerleau, "Here's How DOD Organizes Its Cyber Warriors," *Marine Corps Times*, 25 June 2017, hereafter Pomerleau, "Cyber Warriors."
21. "Cyber Strategy."
22. "Fact Sheet: The Department of Defense (DOD) Cyber Strategy," Defense.gov, April 2015.
23. Pomerleau, "Cyber Warriors."
24. "Cyber Strategy."
25. Mark Pomerleau, "Cyber Protection Teams Need More Intelligence, Say Officials," *C4ISRNET*, 19 June 2017.
26. "Cyber Strategy."
27. Thomas H. Barth et al., *Staffing for Cyberspace Operations: Summary of Analysis* (Alexandria, VA: Institute for Defense Analyses, 2016), 4.
28. "Cyber Strategy."
29. Pomerleau, "Cyber Warriors."

30. Rod Powers, "U.S. Army Military Organization from Squad to Corps," *Balance*, 13 October 2017.
31. Lolita C. Baldor, "Pentagon Chief Considers Easing of Enlistment Standards," *CNS News*, 30 March 2015.
32. Qualifications for Original Appointment as a Commissioned Officer, 10 U. S. C. § 532 (2011).
33. See "Medical School Scholarships," Medicine+Military, accessed 27 April 2018.
34. See Members: Required Service, 10 U. S. C. § 651 (2011). The code explains that "the [military service obligation] for initial appointment in a critically short health professional specialty may be reduced by the Service Secretary to the greater of 2 years or the period of obligated service incurred by the officer upon accepting an accession bonus." See also Minimum Service Requirement for Certain Flight Crew Positions, 10 U. S. C. § 653 (2011). This code states that "the minimum service obligation is to be set at 6 years for all pilots and at 8 years for all fixed-wing jet aircraft pilots."
35. See *Marine Administrative Message (MARADMIN) 350/17, Fiscal Year 2018 (FY18) Selective Retention Bonus (SRB) Program and Broken Service SRB (BSSRB) Program* (Washington, DC: Headquarters Marine Corps, 6 July 2017).
36. Ray Mabus, secretary of the Navy, memo to LtGen Mark A. Brilakis, USMC, "Precept Convening the Fiscal Year 2017 U.S. Marine Corps Colonel Promotion Selection Board and Lieutenant Colonel Continuation Selection Board," 28 August 2015, 4; and *MARADMIN 0539/09, FY10 Reenlistment School Seat Incentives*, 9 September 2009.
37. *Marine Corps Order 1040.31, Enlisted Retention and Career Development Program* (Washington, DC: Headquarters Marine Corps, 8 September 2010), A-4.
38. Charles A. Henning, "Summary," in *U.S. Military Stop Loss Program: Key Questions and Answers* (Washington, DC: Congressional Research Service, 2009).
39. Secretary of the Air Force Public Affairs, "Air Force Announces Initiatives to Lessen Pilot Shortage," press release, 25 August 2017.
40. Steve Morgan, "One Million Cybersecurity Job Openings in 2016," *Forbes*, 2 January 2016.
41. Morgan, "One Million Cybersecurity Job Openings in 2016."
42. Morgan, "One Million Cybersecurity Job Openings in 2016."
43. See "Occupational Outlook Handbook: Information Security Analyst," BLS.
44. Regular military compensation takes into account rank, years in service, tax filing status, basic pay, basic allowance for housing, basic allowance for sustenance, and the total tax advantage. For purposes of this calculation, the inputs were a single E-8 with 10 years of service living on post at Fort Belvoir, VA. See "Regular Military Compensation (RMC) Calculator," Military Pay, Department of Defense.
45. Figure based on the RMC Calculator. For this calculation, the inputs were a single E-4 with four years of service living on post at Fort Belvoir, VA.
46. Figure based on the RMC Calculator. For purposes of this calculation, the inputs were a single E-4 with four years of service living in the barracks at Fort Belvoir, VA.
47. Andrew Tilghman, "Cyber Force Grows as Do Retention Concerns," *Military Times*, 14 March 2015.
48. Tilghman, "Cyber Force Grows as Do Retention Concerns."
49. Steve Fyffe, "U.S. Military Needs More 'Cyber Warriors'," *FSI News*, 12 January 2016.
50. Andrew Tilghman, "The Pentagon's Controversial Plan to Hire Military Leaders Off the Street," *Military Times*, 19 June 2016; and "Air Force Finally Coming Around on Fitness," *John Q. Public* (blog), 13 October 2016.
51. James Clark, "Could Cyber Geeks Make It into the Marines without Going to Boot Camp?," *Task and Purpose*, 8 May 2017.
52. Jeff Schogol, "Coming Soon: Sweeping Personnel Changes for Marine Cyber Operators," *Marine Corps Times*, 4 April 2017.
53. Tilghman, "The Pentagon's Controversial Plan to Hire Military Leaders Off the Street."
54. "Napoleon on War," Napoleon Guide.

55. "Air Force Finally Coming around on Fitness."
56. *Hearing, Update on the U.S. Public Health Response to the Ebola Outbreak, Before the House Energy and Commerce Subcommittee on Oversight and Investigations* (18 November 2014) (statement of RAdm Boris D. Lushniak, USN), 5, hereafter, Lushniak statement.
57. Andrew Glass, "Reagan Fires 11,000 Striking Air Traffic Controllers Aug. 5, 1981," *Politico*, 5 August 2008.
58. Roberta Berthelot, "The Army Response to Hurricane Katrina," *Army Worldwide News*, 10 September 2010.
59. Pomerleau, "DOD's Long Path to Creating a Cyber Warrior Workforce."
60. "Expanding the Size of the U.S. Military in World War II," Warfare History Network, 26 July 2017.
61. "2015 Index of U.S. Military Strength," Heritage Foundation; and Col Richard J. Dunn III, USA (Ret), "2016 Index of U.S. Military Strength: America's Reserve and National Guard Components," Heritage Foundation.
62. "2016 Index of U.S. Military Strength."
63. *Defense Manpower Requirements Report, Fiscal Year 2015* (Washington, DC: Office of the Assistant Secretary of Defense for Readiness and Force Management, 2014), v.
64. See, *Department of Defense Directive 1352.1, Management and Mobilization of Regular and Reserve Retired Military Members* (Washington, DC: Department of Defense, 16 July 2005).
65. Alex Jackson, "War Accelerated Graduation for Naval Academy Class of 1945," *Capital Gazette* (Annapolis, MD), 9 June 2014.
66. Department in which the Coast Guard Operates, 14 U. S. C. § 3 (2012).
67. Coast Guard Auxiliary, 14 U. S. C. §§ 821–832 (2016), chapter 23.
68. "Frequently Asked Questions about the Merchant Marine," USMM, 29 September 2014.
69. "National Defense Reserve Fleet," MARAD (Maritime Administration).
70. "National Defense Reserve Fleet."
71. Kyle Mizokami, "The Five Most-Powerful Navies on the Planet," *National Interest*, 6 June 2014.
72. "Who We Are," U.S. Air Force Auxiliary, Civil Air Patrol.
73. Ian D'Costa, "This Is the Pentagon's Not-So-Secret Civilian 'Ghost' Aircraft Fleet," *Business Insider*, 16 August 2017.
74. Roc Morin, "This Scrapyard Contains the World's Second-Largest Air Force," *Vice*, 8 April 2015.
75. Morin, "This Scrapyard Contains the World's Second-Largest Air Force."
76. "Liberty Ship SS *Robert E. Peary* Built in 4 Days, 15 Hours, 29 Minutes," USMM, 5 June 2000.
77. Associated Press, "Ohio Budget Hawks in Congress Push for Ohio-built Tanks Army Doesn't Want," Cleveland.com, 28 April 2013.
78. "Sequence of Events," Selective Service System.
79. "Sequence of Events."
80. See Tim Shorrock, "Blackwater: One of the Pentagon's Top Contractors for Afghanistan Training," *Nation*, 31 March 2015.
81. James R. Lisher II, "Outsourcing Cyberwarfare: Drawing the Line for Inherently Governmental Functions in Cyberspace," *Journal of Contract Management*, no. 12 (Fall 2014): 7–24.
82. Charlie Savage, Scott Shane, and Alan Blinder, "Reality Winner, N.S.A. Contractor Accused of Leak, Was Undone by Trail of Clues," *New York Times*, 6 June 2017.
83. Eyder Peralta, "Chelsea Manning Says She Leaked Classified Info Out of Love for Country," NPR, 15 June 2014.
84. Lisher, "Outsourcing Cyberwarfare."
85. Michael N. Schmidt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press, 2013), 100.
86. Tilghman, "The Pentagon's Controversial Plan to Hire Military Leaders Off the Street."

87. Federal Activities Inventory Reform Act of 1998, P. L. no. 105-270, 105th Cong. (19 October 1998); and Barth et al., *Staffing for Cyberspace Operations*, 2.
88. *Department of Defense Instruction (DODI) 1100.22, Policy and Procedures for Determining Workforce Mix, with Change 1* (Washington, DC: DOD, 1 December 2017), 18.
89. *DODI 1100.22*, 19.
90. *DODI 1100.22*, 18.
91. *DODI 1100.22*, 18–19.
92. *DODI 1100.22*, 18–19.
93. Lisher, "Outsourcing Cyberwarfare," 7.
94. See *Testimony Before the Defense Acquisition Reform Panel of the House Armed Services Committee*, 111th Cong. (8 October 2009) (statement of Michael J. Sullivan, director, acquisition and sourcing management, GAO).
95. Col James T. Currie, USA (Ret), "A Proposed Model for a Public Health Service Officer Reserve," *Unreserved* (blog), Reserve Officer's Association, 22 November 2016.
96. Tilghman, "The Pentagon's Controversial Plan to Hire Military Leaders Off the Street."
97. An Act for the Relief of Sick and Disabled Seaman, 5th Cong., 2d. session, Chap. 77, section 3–5 (1798).
98. "History," U.S. Public Health Service, 5 September 2014.
99. "History."
100. Lushniak statement, 2.
101. Lushniak statement, 3.
102. Federal Emergency Management Agency, "Federal Government Mobilized to Support Federal, State, Local and Tribal Partners as Hurricane Harvey Approaches the Gulf Coast," press release, 25 August 2017.
103. Patient Protection and Affordable Care Act, 42 U. S. C. § 18001 Sec. 5210 (2010).
104. Patient Protection and Affordable Care Act.
105. See Lushniak statement, 5.
106. Lushniak statement, 4.
107. Lushniak statement, 2.
108. "Non-HHS Agencies and Programs," U.S. Public Health Service, 22 November 2011.
109. Posse Comitatus Act, 18 U. S. C. § 1385 (1878).
110. See Schmidt, *Tallinn Manual*.
111. Schmidt, *Tallinn Manual*, 96.
112. Schmidt, *Tallinn Manual*, 100.
113. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.
114. "Readiness and Deployment Operations Group (RedDOG): Annual Physical Fitness Test (APFT)," Commissioned Corps, PHS.
115. "Mission and Core Values," U.S. Public Health Service, 3 February 2014.
116. Uniformed Services Employment and Reemployment Rights Act of 1994, 38 U. S. C. §§ 4301–4335 (13 October 1994).
117. Lily Hay Newman, "The Biggest Cybersecurity Disasters of 2017 So Far," *Wired*, 1 July 2017.
118. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.
119. Schmidt, *Tallinn Manual*, 87.
120. Col Walt Yates, "Affordable and Effective Cybersecurity," *Marine Corps Gazette* 101, no. 9 (September 2017): 9.