Commodore Grace M. Hopper, USN (covered), popularized idea of machine-independent programming languages that led to development of COBOL, January 20, 1984 (U.S. Navy/James S. Davis)

Recruiting Cyber Specialists

Why the Services Must Modernize Qualification Standards

By Jesse P. Samluk, Mark A. Boeke, and Marcus A. Neal

Hardly a day goes by without another data breach concerning peoples' sensitive information—such as Social Security numbers, dates of birth, and payroll information—making the news. Billions of dollars are lost each year to data breaches and theft of intellectual property. Unfortunately, there is no end in sight. Despite our best cyber security efforts, criminal hackers seem to be one step ahead. Playing catchup to hackers is an infinite game of wits, brains, luck, and patience.

The uniformed services (to include here the Coast Guard, U.S. Public Health Service Commissioned Corps, and National Oceanic and Atmospheric Administration [NOAA] Commissioned Officer Corps) are also doing their version of playing catchup by forming their own siloed cyber elements.[1] Cyber issues are by definition not geographically bound, and they do not have a certain aspect to them that begs for assistance from any particular service component. This effort is *compounded* with the services recruiting and retaining cyber specialists in a decades-old personnel environment with even older medical, age, and prior service standards.

The uniformed services realize that cyber is its own distinct warfighting

Dr. Jesse P. Samluk is a Reserve Organization of America Member and an RF Engineer with the Department of Defense (DOD). Mark A. Boeke is a Lessons Learned Program Manager with DOD. Marcus A. Neal is a Lead Cyber Security Engineer with DOD.

domain, just like the land, sea, or air, where either nation-states or terrorist actors can target our country. It is a unique battlefield where no one receives direct fire, but the potential havoc created by a cyber attack could be more damaging than other forms of engagement. Cyber warfare does differ in that it knows no boundaries; even if the United States withdrew all its forces from foreign countries, it would still be vulnerable to cyber lines of operation from capable actors—both external and internal. Additionally, our assets in space are prime targets for hacking. Protecting the data of the recently established U.S. Space Force will place an additional demand on critically overburdened cyber professionals.[2]

Cyber security is among the fastest growing job markets, and such expansion is expected to continue rapidly over the next few years. Nearly every facet of society is under attack from state-sponsored hackers, including Russian attacks on classified government networks and North Korean ransomware attacks on average Americans. In this vein, the services are looking for the best and brightest and are actively recruiting to protect our government's critical systems. In return, the services offer the honor and privilege of wearing the uniform and assisting the Nation. However, the services are also competing for people against private industry, with familiar company names such as Google, Facebook, and Apple, as well as less familiar ones such as CrowdStrike and FireEye, to secure sensitive information of all stripes. Although private-sector employers can pay top dollar to attract new talent, government agencies (Federal, state, and local) cannot. That is not to say that cyber security experts are averse to government service; highly skilled cyber security professionals serve in the Nation's military and clandestine services and are perhaps the world's most potent offensive and defensive hackers. U.S. Code Titles 10 (Armed Forces), 18 (Crime and Criminal Procedure), and 50 (War and National Defense) work in concert to allow government cyber security professionals to operate under authorities that private industry cannot—a major point of appeal.[3] That said, promotion policies, frequent moves, long deployments, and less-than-competitive pay present retention challenges for cyber security experts in uniform—even more so for those who must support families.

To address this problem, the uniformed services are starting to adapt in innovative ways. The Army already offers direct commissioning into the cyber field and is considering expanding direct commission ranks through colonel (O6), while also paying accession and retention bonuses between $40,000 and $100,000.[4] General Paul Nakasone, USA, while in his previous role as commander of U.S. Army Cyber Command, agreed that the current level of direct commission ranking (O2) is hampering recruiting and retention efforts. He stated, "We are limited to bringing [cyber specialists] in as a first lieutenant, and so we would like greater flexibility on that."[5] Considering that the Public Health Service Commissioned Corps already direct commissions the Surgeon General and Assistant Secretary for Health at the flag officer ranks of vice admiral (O9) and admiral (O10), respectively, this problem, while somewhat controversial for the Public Health Service Commissioned Corps, should be a nonissue for the rest of the services.[6]

Even marching band members in the Air Force, as an incentive to join the band, are rapidly promoted to E6 after initial training.[7] The Army is considering letting cyber personnel leave the military, learn new skills in private industry, and reenter service.[8] This concept is not unlike training with industry programs—an existing option for selected servicemembers. Lieutenant General Lori Reynolds, former commander of Marine Corps Forces Cyberspace Command, has stated, "We need to start thinking outside the box on some of this stuff, because, monetarily, it's really difficult to keep up with what industry offers."[9] While some of the ideas presented here are outside the box, the uniformed services have not changed their extremely restrictive medical, age, and prior service standards, even though the need is so great. Therefore, the purpose of this article is to argue and demonstrate that, given the urgent need for recruiting and retaining cyber specialists, the time is at hand to make these necessary changes, so the uniformed services will be well prepared to defend our Nation in cyberspace. The clarion call is more revolutionary than evolutionary.

Medical Standard Barriers

In addition to meeting technical qualifications, cyber specialists also face other entrance standards that apply to all candidates: medical, age, and prior service reentry standards. No one is calling for the elimination of all criteria. The question is, what standards are appropriate for our modern and future cyber warriors?

The majority of current age-eligible prospects cannot meet the entrance standards; overall, this problem is catastrophic. According to a 2017 Pentagon report, 71 percent of those considered young enlistment age—that is, between the ages of 17 and 24—are ineligible to serve.[10] Of that number, close to 60 percent are ineligible due to either medical standards or physical fitness levels.[11] This problem is quickly becoming the next "looming national security crisis."[12] And of those deemed qualified to serve, only 15 percent exhibit any interest in service whatsoever.[13]

While the numbers are concerning, given the medical standards in their present state, it is also safe to say that most of the standards do not reflect the pace of advances in medicine. What was once considered a serious medical condition years ago can be treated successfully today. For example, consider a severe myopia condition from a detached retina as a result of an injury resulting from sports, a car accident, or even being a victim of an assault or other crime. Within the current medical standards, this particular eye condition is disqualifying and has a slim chance of receiving a medical waiver. Specifically, Department of Defense (DOD) Instruction 6130.03 disqualifies, "d. Retina. Any history of any abnormality of the retina, choroid, or vitreous."[14]

But eye surgery has improved over the years to treat such conditions so that a detached retina can be repaired, regardless of how it occurred. So, then, why are the uniformed services still regarding

some of these conditions as limiting for military service? Keep in mind that a detached retina is just one of many conditions that modern medicine has improved with consistent results, but the DOD instruction for medical standards has not evolved. That said, DOD has been known to evolve on the area of medical standards when there is a definite need: Due to a fighter pilot shortage, the Air Force no longer restricts applicants for being too short.[15]

The medical standards are written to treat everyone the same and to hold everyone to an equal standard regardless of military specialty. Not everyone can be or desires to be a fighter pilot, infantry, or even a special forces operator, which are specialties that require a stricter physical and specialized standard. Many who seek to join want to do something besides combat-related work. There are scores of other specialties in the services that people could join without being held to such stringent physical standards. In today's era, retired Army Major Scott Smiley continued to serve even after losing 100 percent of his vision after a suicide bomber attack in Iraq.[16]

The cyber domain is one of the specialties that does not require strict physical standards to do the job, and the uniformed services desperately need people to fill critical roles. Thus, the key question is whether the services will continue to perpetuate self-destructive and overreactive policies by maintaining questionably relevant standards. To further advance this point, conditions such as a detached retina (that has been corrected), previous back injuries (for example, herniated discs), asthma, or even eczema do not preclude a network operator from conducting a computer network attack on an adversary. Are the services willing to risk the exclusion of cyber experts because they have suffered injuries or have other minor medical conditions? Furthermore, do our adversaries reject technically gifted people because they have a medical condition that the uniformed services would consider a disqualifier?

A counterargument could be that the guidelines are strict to avoid any medical issues flaring up while the servicemember is deployed. That may be a valid case in some specialties, but servicemembers in cyber operations are generally in computing centers far away from any danger zone and could launch successful attacks with little more physical exertion than the touch of a keyboard and click of a mouse. Obviously, those cyber operators embedded in tactical units would need to meet more rigorous physical standards. Regardless, those members in cyberspace are dedicated to protecting systems and will go where they are needed. For this reason, *obsolete medical standards cannot be a barrier to recruiting cyber specialists if the uniformed services want to best achieve the offense—a principle of war.*

The solution is for the services to readily waive standards—as they often do for other critical specialties, such as physicians, lawyers, and chaplains—as long as these individuals can still perform the mission.[17] If waivers are required, then the process must be lean for shorter processing time. One possible way to speed up the process is to include retired military and civilian doctors' recommendations. Another proposed idea is to have an assisted accessions process in which applicants are evaluated holistically instead of just looking at a disqualifying condition on face value.[18] As an even better alternative, the services could adapt separate medical standards suited to the duties that would be performed as part of a particular specialty. Effectively, separate medical standards are already adopted today, in that troops in units such as the 75th Ranger Regiment meet higher standards than those of the Army in general. Case in point, rest assured that, regardless of medical issues, *these cyber professionals can still do the job.*

Age Standard Barriers

The same argument for outdated entrance standards could be made with age. Current guidelines for age vary by service but are mainly in place to ensure that 20 years of service can be completed when someone hits his or her sixties. To date, only the NOAA Commissioned Officer Corps has no age limit for applicants.[19] The Public Health Service Commissioned Corps allows nonprior military service applicants the highest maximum age cutoff: age 44.[20]

The uniformed services have shown an ability to adapt to adjusting outdated age standards when faced with filling a critical specialty. In 2018, Tyrone Krause, a 63-year-old cardiothoracic surgeon, was commissioned into the Navy at the rank of commander (O5).[21] If this surgeon can commission later in life, at a higher rank, then are age standards really necessary in an era where people live longer and are more vigorous well into their seventies and beyond?

For another example, consider Grace Hopper, who was born in 1906, earned a PhD in mathematics from Yale in 1934, and joined the Navy Reserve in 1943. She became a pioneer with the new compiled computer language COBOL in the 1950s.[22] Commander Hopper retired from the Navy Reserve in 1966 but was recalled to Active duty to continue her work with COBOL. Her second retirement was as a Rear Admiral, lower half, in 1986, when she was nearing age 80.[23]

The key point here is a familiar adage: "With age comes wisdom and experience." Even Commander Krause, at the time of his commissioning, stated, "A lot of people in the private sector have a lot of skills they can bring to the Navy and military in general. You can be 40 years old, 50 years old, and your profession may be something that's necessary. . . . You can certainly give back."[24]

Commander Krause's statement resounds within the cyber community. Would the services scoff at someone who has 25 years in the cyber arena just because he or she did not meet an age standard? Did the Navy deride former White House Chief of Staff Reince Priebus for an age waiver at age 46 to become a human resource officer in the Naval Reserve?[25] If the age limit has to do with ensuring 20 years of service just to earn a full pension, then that argument is now a moot point. The uniformed services implemented an agile forward-looking pension plan, known as the Blended Retirement System, which allows members to have their Thrift Savings Plan retirement account if they leave before 20 years of service.[26]

Captain Scott M. Smiley, first blind officer and second Wounded Warrior to hold position of command, passes guidon back to 1st Sergeant Deon E. Dabrio during U.S. Army Warrior Transition Unit at West Point change of command ceremony, February 1, 2010 (U.S. Army/Tommy Gilligan)

Trying to change age standards is nothing new. In 2012, Representative Paul Broun, Jr. (R-GA), tried to enact legislation that would allow people at any age to join the uniformed services as long as the candidates could meet minimum health and fitness requirements. The House at that time voted down the measure. Congressman Broun, a retired Navy medical officer, even stated that the age cap is "an arbitrary policy."[27] This age cap is also extended to Federal law enforcement agencies. These agencies, such as the Federal Bureau of Investigation, control key components of America's coordinated cyber efforts. Such agencies are also hampered by these restrictions, as a candidate must be younger than age 37, thus also eliminating that avenue for patriots of a certain age who still want to contribute.[28]

Counter to the proposed legislation eliminating an age limit is the argument made by Representative Susan Davis (D-CA) that "risks outnumber gains" and that older personnel are more likely to become injured and take longer to heal.[29] We must reject this age bias. The services seem perfectly happy and content to relax standards for medical personnel, as previously mentioned, so why not cyber? It is understood that medical professionals are always in demand, as they possess unique skills. So are cyber professionals. For instance, as medical devices become increasingly "connected," who is going to ensure that those devices are secure, especially in remote environments where lives are on the line? Is age really going to affect those sitting at a workstation performing information security?

There is some hope: Private industry is starting to see the value of older workers.[30] Even physically demanding and dangerous occupations akin to military service, such as career fire departments in major cities like Philadelphia, do not have age limits for new recruits.[31] For recruiting older cyber professionals, the Army wants to remove the retirement-age requirement, which could, in turn, render irrelevant the age restriction.[32] Additionally, in 2018 a relatively unnoticed request for comments in the *Federal Register* indicated that the services may be modifying the selective service process for those with "cyber skills, and science, technology, engineering, and mathematics skills for which the Nation has a critical need, without regard *to age* or sex."[33] While it appears that there may be a shift in thinking about age, the solution here is that the uniformed services need to reflect NOAA Commissioned Officer Corps policy on having no age limit in place. There is no reason to have an arbitrary age limit in place, especially with what we are up against in cyberspace.

Prior Service Barriers

Prior service barriers are also lasting administrative obstacles. There are

"The President's Own" U.S. Marine Band performs during retirement ceremony for General Thomas D. Waldhauser at Marine Barracks Washington, DC, September 27, 2019 (DOD/James K. McCann)

potential recruits with prior service who were discharged honorably, but something may have affected their reentry—perhaps a particular narrative statement or a reentry code on their discharge certificate. Some may even have been discharged under less-than-honorable conditions (such as a general discharge). Whatever the circumstances at the first discharge, those contexts may now be a moot point. It is not unheard of for some of these prior servicemembers to have turned their lives around and matured from when they were younger; today, they could be looking for a second chance to serve.

Unfortunately, the services would rather grant waivers to those who have more serious background problems, like felonies and drug use, than to take back those members who may have had minor issues similar to those aforementioned at the time of discharge.[34] Some of those members seeking a second chance often serve in other ways, perhaps in the police force, as emergency medical technicians, or in career/volunteer fire departments; some have even deployed to dangerous areas alongside the uniformed services, albeit in a civilian role. These individuals have demonstrated themselves through selfless service in their communities and have put their lives on the line. There are even prior service cyber professionals who feel the calling to serve in the military yet again; however, it seems as though the services turn a blind eye to these individuals who want to return—and who have a clean record—because their narratives and/or reentry codes appear to be worse than felonious crimes or drug use. To say that the uniformed services place objective guilt on former members for matters that happened years ago and have since been corrected is an understatement. Because society in general—and the services in particular—gives second chances to those who have committed serious crimes, *there is no reason for not giving a second chance to former members, discharged under adverse conditions, who have proved themselves.*

To address the current need, as the saying goes, "Desperate times call for desperate measures." And, indeed, we are in desperate times, especially on the cyber front. Although some may vigorously argue that the concern is solely a retention issue and not a recruitment issue—even though retention is in the forefront too—there is resounding evidence to the contrary that has even been acknowledged by Pentagon officials.[35] Even if the problem were solely a retention issue, recruiting is an inherent part of the process, and adjustments need to be made for the future.[36] Moreover, because there is a problem no matter what, DOD and other services are simply too selective when it comes to former uniformed

Sergeant Brittany Deturo, 401st Army Field Support Brigade, positions herself to practice deadlift element of new Army Combat Fitness Test during familiarization training at Camp Arifjan, Kuwait, August 17, 2020 (U.S. Army/Kevin Fleming)

servicemembers trying to help in this field. The solution is clear: Let those who have prior experience have a second chance. The need is too great in the cyber domain to be so fastidious.

Conclusion: Modernizing Standards

The future is ours to create the opportunity for talented, skilled, and driven people. In light of the current cyber situation, agencies of the U.S. Government are taking the challenge head-on, each and every day. In particular, the uniformed services have made serious headway to counter cyber adversaries. But significant obstacles remain, and the most important issue is attracting, recruiting, training, and retaining a world-class force of people to serve in this field in uniform. We need them if we are to gain and maintain the initiative—an offensive principle of war.[37]

To their credit, the services recognize that there is a big problem in this area. Some of the concern is based on compensation, but what the services fail to realize is that there are some cyber professionals out there who are not interested only in money. These professionals would sacrifice a higher salary in private industry, endure the prolonged application and boarding process, and get the necessary clearances and polygraphs just to have the honor of wearing the cloth of this Nation. These are the type of people that the uniformed services need—those who are loyal and will never give up. If the services could only seek out and recognize these individuals and give them a chance—or a second chance, in some instances—they could prove themselves and, without a doubt, make a real contribution to closing U.S. cyber deficiencies. Unfortunately, common sense does not necessarily prevail, and we are increasing risk in this area just to maintain antiquated standards in the face of adversaries who seem to have the upper hand in the cyber domain. Our adversaries would gladly accept into their ranks a cyber operator who can wreak havoc but who also has a condition that the services would find disqualifying. Relating back to the principles of war, more and better talent allows us to gain and maintain the initiative in this battlespace, which we arguably have ceded.

Changing standards for the uniformed services is not unheard of; they have had a long history of adjusting or even ignoring standards to allow for talented recruits in specialized fields, and, given the nature of cyber warfare, it may even be possible to accept individuals with physical disabilities.[38] The services used to grant field commissions in times of need as well. Another possibility is that the services could also retrain those who

Civilian QF-4E Pilot/Controller Lieutenant Colonel Jim "Wam" Harkins, USAF (Ret.), hugs his wife, Annette, after being showered with champagne upon exiting cockpit of his McDonnell Douglas F-4 Phantom II for last time following ceremonial final military flight of storied aircraft at Holloman AFB, New Mexico, December 21, 2016 (U.S. Air Force/J.M. Eddins, Jr.)

are wounded and have limited means to serve in a fuller capacity. Instead of medically discharging these wounded warriors, the services should allow them to serve with honor and retrain them to engage in the cyber threats we face.

Some critics may argue that adapting standards for cyber personnel could affect overall readiness and that there are always civilian positions instead.[39] This argument stems from a larger problem surrounding the culture of the services—specifically the cultural biases of what a warrior looks like.[40] The counterargument is that future warriors will need science, technology, engineering, and mathematics skills in order to adapt to high-tech threats in real time.[41] There is a need for uniformed members under Title 10 authority whose jobs cannot be outsourced to contractors or civilians.[42] Furthermore, not everyone who joins the uniformed services, explicitly the Armed Forces, need be a "trigger puller." The Marine Corps' "President's Own" marching band musicians do not "attend recruit training or basic combat training because of their unique mission to provide music for the President and the Commandant [of the Marine Corps]."[43] These highly skilled musicians also occupy permanent positions and hence cannot be transferred.[44] Perhaps our cyber model reflects the "President's Own" to a degree, but significantly more than the current model of the Marine Corps Cyber Auxiliary.[45]

To this end, it does take talented people to address the cyber problem. The services should consider themselves fortunate that people want to join them in the cyberspace community and should embrace these professionals with open arms, adjusting the standards to allow their entry. It would be a grave mistake to turn them away if the goal of the services is to "own" the boundless cyberspace. It will be difficult to defend against our adversaries in the cyber domain if the military continues to have unfilled cyber positions because of outdated standards. **JFQ**

The authors acknowledge the following individuals for their assistance in shaping this article: Lieutenant Colonel Susan Lukas, USAF (Ret.); Major Crispin Burke, USA; Lieutenant Colonel Chris Lusk, USA (Ret.); Cryptologic (Maintenance Branch) Chief Petty Officer Tim Paul, USN (Ret.); and Dr. Irene M. Zoppi Rodriguez.

Notes

[1] U.S. Cyber Command components include U.S. Army Cyber Command (headquarters in Fort Gordon, Georgia), Marine Corps Forces Cyberspace Command (headquarters in Fort Meade, Maryland), U.S. Fleet Cyber Command (headquarters in Fort Meade, Maryland), and Air Forces Cyber (headquarters in Joint Base San Antonio, Texas).

[2] Space Policy Directive–4, *Establishment of the United States Space Force* (Washington, DC: The White House, 2019).

[3] *U.S. Code,* available at <https://www.govinfo.gov/app/collection/uscode/2017/>.

[4] Kathleen Curthoys, "How the Army Is Competing with Google for These Ninjas," *Army Times*, August 6, 2018; Jeffrey E. Phillips, "'Lateral Entry': Direct Commissioning of Civilians, a Pro and Con," *ROA*, August 3, 2016, available at <https://www.roa.org/blogpost/1434064/253796/Lateral-entry—Direct-commissioning-of-civilians-a-pro-and-con>; Crispin J. 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>; Armed Forces Communications and Electronics Association (AFCEA), "U.S. Army Introduces Cyber Fast Track for Civilians," *AFCEA*, February 13, 2017, available at <https://www.afcea.org/content/Blog-us-army-introduces-cyber-fast-track-civilians>.

[5] Lauren C. Williams, "Military Looks for Ways to Bring in Cyber Talent at Better Salaries," *Federal Computer Week*, March 14, 2018.

[6] U.S. Department of Health and Human Services, "Leadership," available at <https://www.hhs.gov/about/leadership/index.html>; Richard Carmona, "Instant Admirals and the Plague of Politics in the United States Public Health Service: Back to the Future," *Military Medicine* 182, no. 5–6 (May 2017), 1582–1583, available at <https://doi.org/10.7205/MILMED-D-17-00039>.

[7] Air Force Bands, "Auditions and USAF Band Career Information," available at <https://www.music.af.mil/Bands/The-United-States-Air-Force-Band/About-Us/Careers-in-The-United-States-Air-Force-Band/Frequently-Asked-Questions/>.

[8] Kathleen Curthoys, "Army Cyber Should 'Let Nerds Be Nerds,' Experts Say," *Army Times*, October 11, 2017.

[9] Sean Gallagher, "DOD Needs Cyberwarriors So Badly It May Let Skilled Recruits Skip Boot Camp," *Ars Technica*, May 9, 2017, available at <https://arstechnica.com/information-technology/2017/05/dod-needs-cyber-warriors-so-bad-it-may-let-skilled-recruits-skip-boot-camp/>.

[10] Thomas Spoehr and Bridget Handy, *The Looming National Security Crisis: Young*

Americans Unable to Serve in the Military (Washington, DC: The Heritage Foundation, February 13, 2018), available at <https://www.heritage.org/defense/report/the-looming-national-security-crisis-young-americans-unable-serve-the-military>.

[11] *Ready, Willing, and Unable to Serve* (Washington, DC: Mission: Readiness, 2009), available at <http://cdn.missionreadiness.org/MR-Ready-Willing-Unable.pdf>.

[12] Spoehr and Handy, *The Looming National Security Crisis.*

[13] Dennis Laich, Jonathan Askonas, and Gil Barndollar, "The Armed Forces Arithmetic Isn't Adding Up," *The Hill*, December 6, 2018, available at <https://thehill.com/opinion/national-security/419641-the-armed-forces-arithmetic-isnt-adding-up>.

[14] Department of Defense (DOD) Instruction 6130.03, *Medical Standards for Appointment, Enlistment, or Induction into the Military Services* (Washington, DC: DOD, May 6, 2018), 12.

[15] Oriana Pawlyk, "The Air Force Will No Longer Reject Pilot Applicants for Being Too Short," *Military.com*, May 22, 2020, available at <https://www.military.com/daily-news/2020/05/22/air-force-will-no-longer-reject-pilot-applicants-being-too-short.html>.

[16] *Hope Unseen*, available at <https://hopeunseen.com/about/>.

[17] Burke, "The Pentagon Should Adjust Standards for Cyber Soldiers."

[18] Joe Schuman, "Department of Disqualified: Fixing the Broken Military Medical Accessions Process," *War on the Rocks*, November 20, 2018, available at <https://warontherocks.com/2018/11/department-of-disqualified-fixing-the-broken-military-medical-accessions-process/>.

[19] National Oceanic and Atmospheric Administration Commissioned Corps, "Frequently Asked Questions," available at <https://www.omao.noaa.gov/learn/noaa-corps/join/frequently-asked-questions>.

[20] U.S. Public Health Service Commissioned Corps, "How to Apply," available at <https://www.usphs.gov/how-to-apply>.

[21] J.D. Simkins, "Ensign Commissions Her 63-Year-Old Father as a Navy Officer," *Navy Times*, July 14, 2018.

[22] COBOL (common business-oriented language) was designed in 1959 by the Conference/Committee on Data Systems Languages and was partly based on the programming language FLOW-MATIC (the first English-like data processing language), which was designed by Grace Hopper.

[23] Yale University Office of the President, "Biography of Grace Murray Hopper," available at <https://president.yale.edu/biography-grace-murray-hopper>.

[24] Simkins, "Ensign Commissions Her 63-Year-Old Father as a Navy Officer."

[25] Mark D. Faram and Leo Shane III, "A 46-Year-Old Ensign Who Once Ran the White House?" *Navy Times*, December 14, 2018.

[26] "Uniformed Services Blended Retirement System," *Military Compensation*, available at <https://militarypay.defense.gov/blendedretirement/>.

[27] Jeff Ousley, "Military Age Restrictions: How Old Is Too Old to Serve?" *Veterans United*, June 21, 2018, available at <www.veteransunited.com/network/military-age-restrictions-how-old-is-too-old-to-serve/>.

[28] Federal Bureau of Investigation, "Frequently Asked Questions," available at <https://www.fbi.gov/about/faqs/how-old-do-you-have-to-be-to-become-an-agent?>.

[29] Ousley, "Military Age Restrictions."

[30] Erika Prafder, "Mature People Are Working Longer, and That's a Benefit for Companies," *New York Post*, June 24, 2018.

[31] Monica Peters, "The Philadelphia Fire Department Is Hiring," *The Philadelphia Sunday*, September 1, 2016.

[32] Carten Cordell, "Army Officials Are on the Hunt for More Cyber Talent," *Fed Scoop*, October 11, 2018, available at <https://www.fedscoop.com/army-cyber-officials-hunt-for-talent/>.

[33] Williams, "Military Looks for Ways to Bring in Cyber Talent at Better Salaries"; National Commission on Military, National, and Public Service, "Request for Information on Improving the Military Selective Service Process and Increasing Participation in Military, National, and Public Service," *Federal Register*, February 16, 2018, available at <https://www.federalregister.gov/documents/2018/02/16/2018-03261/request-for-information-on-improving-the-military-selective-service-process-and-increasing>. Emphasis added.

[34] Spoehr and Handy, *The Looming National Security Crisis*; Lolita C. Baldor, "Army Using Drug Waivers, Bonuses to Fill Ranks," *Army Times*, August 1, 2018, available at <www.armytimes.com/news/your-army/2018/08/01/army-using-drug-waivers-bonuses-to-fill-ranks/>.

[35] Justin Lynch, "Why Recruiting Cyberwarriors in the Military Is Harder Than Retaining Forces," *Fifth Domain*, November 1, 2018, available at <www.fifthdomain.com/dod/2018/11/01/why-recruiting-cyber-warriors-in-the-military-is-harder-than-retaining-forces/>.

[36] Isaac R. Porche et al., *Cyber Power Potential of the Army's Reserve Component*, RR-14900-A (Santa Monica, CA: RAND, 2017), available at <https://doi.org/10.7249/RR1490>.

[37] William T. Eliason, "An Interview with Paul M. Nakasone," *Joint Force Quarterly* 92 (1st Quarter 2019), 4–9.

[38] Burke, "The Pentagon Should Adjust Standards for Cyber Soldiers."

[39] Mark Cancian, "Blue-Haired Soldiers? Just Say No," *War on the Rocks*, January 18, 2018, available at <https://warontherocks.com/2018/01/blue-haired-soldiers-just-say-no/>.

[40] Jacquelyn Schneider, "Blue Hair in the Gray Zone," *War on the Rocks*, January 10, 2018, available at <https://warontherocks.com/2018/01/blue-hair-gray-zone/>.

[41] Ibid.

[42] Raj M. Shah, *Military Service Hearing: Creating New Pipelines to Service and Fostering Critical Skills*, Testimony Before the National Commission on Military, National, and Public Service, Washington, DC, May 16, 2019, available at <https://inspire2serve.gov/_api/files/268>.

[43] Patrick Cirenza, "The President's Own as a Model for the Marine Corps Cyber Auxiliary," *War on the Rocks*, September 18, 2019, available at <https://warontherocks.com/2019/09/the-presidents-own-as-a-model-for-the-marine-corps-cyber-auxiliary/>.

[44] Ibid.

[45] U.S. Marine Corps, "Marine Corps Established Volunteer Cyber Auxiliary to Increase Cyberspace Readiness," *Marines*, May 13, 2019, available at <https://www.marines.mil/News/Press-Releases/Press-Release-Display/Article/1845538/marine-corps-establishes-volunteer-cyber-auxiliary-to-increase-cyberspace-readi/>.