Open Access License Notice

Citizen-to-Soldier-to-Citizen and Cyber Warrior: Building the Cybersecurity Workforce with Military Veterans

Charles E. Wilson, University of Detroit Mercy

Author Note

Correspondence concerning this paper should be addressed to Charles E. Wilson

Center for Cyber Security and Intelligence Studies
Department of Criminal Justice

4001 W. McNichols Street, Detroit, MI 48221

Contact: wilsonce@udmercy.edu

Abstract - The cyber threats facing America have escalated sharply in recent years and has emerged as a clear and present danger to the nation's homeland and national security, economic prosperity, intellectual capital, and critical infrastructure. In the face of such persistent and escalating cyber threats, the United States is determined to immediately develop the capability necessary to counter this threat. A key component of the national cybersecurity strategy includes building a qualified cybersecurity workforce with the competence, knowledge, and technical skills. The cyber workforce must be capable when necessary to not only respond to, effectively counter, and eventually prevent the occurrence of cyber attacks. This paper argues that the U.S. has an untapped resource that will enhance its ability to meet the cybersecurity workforce requirements. That resource is the available military veterans who have served this country with distinction and honor. Most veterans have demonstrated through their service that they possess the necessary potential, characteristics and experience to successfully participate in the cybersecurity workforce. This paper postulates that the cybersecurity workforce can be rapidly filled by focusing efforts on the recruitment, education, and employment of military veterans.

Keywords: Military veterans, cybersecurity, cyber threats, national security, and cybersecurity workforce

INTRODUCTION

This paper reflects the synthesis of empirical data gathered from an extensive review of research literature, open source government documents, and real world case studies culled from media reports and academic research materials. The paper will present the information in four sections: First, by highlighting the scope of the cybersecurity problem. Second, by presenting the American cybersecurity agenda developed to address the problem. Third, by describing the specific and unique characteristics, traits, and experiences gaining through military service that make the veteran an excellent candidate for the cybersecurity workforce. Fourth, by offering recommendations and options to facilitate the recruitment, education, and employment processes for military veterans seeking to enter the cybersecurity workforce. Because, the country is facing an increasing number of sophisticated cyber threats, there is a dire need to address the personnel shortfall of over one million qualified cybersecurity professionals. This paper suggests that the recruitment, education and employment of military veterans are a viable solution to this mounting problem.

This paper offers thought-provoking suggestions for tackling the cybersecurity workforce issue. The paper argues that the cybersecurity workforce can be rapidly filled by focusing efforts on the recruitment, education, and employment of military veterans. Because of their military pedigree and experience veterans can play a pivotal role in the next chapter of American cybersecurity prevention efforts. There is likely one question on the minds of the readers of this paper - what is it that makes veterans so special and unique when compared to any other job candidates? A recent study by Syracuse University's Institute for Veterans and Military Families (2012) presented a robust, specific, and compelling business case for hiring individuals with military background and experience. The report concluded that empirical research from multiple fields and disciplines, such as business, psychology, sociology, and national security support the hiring of military veterans. The report

noted that military veterans bring a unique set of knowledge, skills, and abilities that can enhance organizational performance and provide a competitive advantage in the dynamic business environment.

The aforementioned report, "The Business Case for Hiring a Veteran," identified specific characteristics that many veterans possess that help them excel in the workplace. The authors found, that veterans "exhibit high levels of resiliency, advanced team building skills, and strong organizational commitment" (p. 2). Additional, evidence of support for a focused cybersecurity workforce education and employment program for military veterans is included in the following sections of the paper.

SCOPE OF THE THREAT

The stark reality of the cybersecurity threat is manifested on a daily basis with repeated reports of cyber attacks being reported by both the private sector and the federal government. Since 2002, there have been a large number of advanced, well-orchestrated attacks against private sector, military and government information technology systems. The Computer Security Institute's, Computer Crime and Security Survey (Power, 2002) of large corporations and government agencies revealed that:

- 90 percent of respondents had detected computer security breaches;
- 80 percent of respondents had suffered financial losses as a result of computer breaches;
- 85 percent of respondents had detected computer viruses; and
- 78 percent of respondents had detected employees' abuse of Internet access privileges (e.g., downloading pornography or pirated software, or inappropriate use of e-mail systems).
- 75 percent of respondents cited their Internet connection as a frequent point of attack, and
- 33 percent cited their internal systems as a frequent point of attack.

Researchers Virilis, Serrano, and Dandurand (2014) categorized contemporary cyber attacks as advanced persistent threats (APT) with unique characteristics that differentiate them from traditional attacks. It is the combination of complexity, sophistication, and innovation that exacerbates the situation and elevates the contemporary cyber threat attacks to that of a top tier national security threat and critical business issue. Virilis et al., (2014) further suggested that cyber attackers employing APTs frequently use zero-day exploits or modified and obfuscated cyber attack methods to evade the majority of signature-based end points and network intrusion detection solutions. This reinforces the criticality of building a competent cybersecurity workforce capable of minimizing, countering and preventing cyber attacks. America must make every effort to mobilize its available resources to address a continuous growing menace that is becoming more capable with each attack.

In April 2009, a reporter for the Wall Street Journal wrote in a front page story that the networks that control the electricity grid in the U.S. had been penetrated by Russian and Chinese cyber-spies (Gorman, 2009). Additionally, USA TODAY reported that federal records showed that cyberattacks on U.S. government computer networks increased by 40 percent that year (Eisler, 2009). In 2010, numerous Fortune 500 companies reported a wave of new and sophisticated attacks against U.S. industry. Google (Arrington, 2010) announced that it, along with more than 70 high-tech companies, had lost important intellectual property. That same year, Exxon-Mobil, Marathon, and Conoco-Phillips also revealed their systems had been penetrated by sophisticated nation-state actors (Clayton, 2010).

Recent attacks on various U.S. government entities (Inserra & Rosenzweig, 2014), private sector enterprises, and critical infrastructure assets, such as Google, Sony, Target, JP Morgan, and Chase emphasize the urgency of acquiring the capacity to prevent such attacks. Moreover, alarm continued to rise when in 2011 the Office of the National Counterintelligence Executive (ONCIX) reported that "foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security." In 2013, the cybersecurity firm Mandiant disclosed that hundreds of terabytes of data from 141 companies in 20 different industries had been stolen remotely by hackers

in China. According to the Symantec (2014) Internet Security Treat Report there were more than 41 million attacks detected, eight mega breaches, and 253 total breaches which exposed over 552 million personal identification of end users. (p. 14) Large retailers like Staples Inc., Neiman Marcus Inc., Michaels, Home Depot Inc. and eBay Inc. announced breaches, where millions of customers' credit card information and personal data were stolen by cyber attackers. But it wasn't just retail giants: Firms in health care (Community Health Systems), finance (JPMorgan Chase & Co.) and entertainment (Sony Pictures) were also victims to cyberattacks. In addition to breaches, attacks, other major software vulnerabilities also surfaced: (1) The Open SSL Heartbleed vulnerability shook confidence in Internet security; and (2) Shellshock exposed a majority of Internet-facing services to attack (Steinberg, 2014). Many cybersecurity experts stated that these two Internet attacks are prime examples of the serious cyber threats menacing critical elements of the Internet and the global information infrastructure. Moreover, these two cyber attacks add evidence to the argument that building a capable cybersecurity workforce is an absolutely essential element for the protection of the cyberspace environment. For example, Jose Pagliery (2014) noted that when Heartbleed was discovered, the Internet security function (Open SSL) was maintained by a handful of volunteers, only one of whom worked full-time.

At the individual level over 556 million people per year are victims of cybercrime, 1.5 million per hour, 18 people per second, and with an annual price of $110 billion (McAfee, 2014). This figure represents 46 % of online adults who have been victims of cybercrime in the past twelve months, compared with the findings from 2011 at 45 percent (Symantec). In total, cybercrime costs the world significantly more than the global black market in marijuana, cocaine, and heroin combined. McAfee (2014) estimated that the likely annual cost to the global economy from cybercrime is more than $400 billion. They further estimated that the range of losses would be between $375 billion and as much as $575 billion. According to Kaspersky Lab (2012), cyber criminals launched 1.5 billion web attacks throughout 2012, used 6.5 million unique domains (2.5 million more than

in 2011), and seeded malicious code into Internet servers and zones of 202 countries around the world.

A Government Accounting Office (GAO) report (2012) noted that the number and complexity of cyber-attacks has been increasing steadily in recent years. For instance, the report stated that cyber attacks on the Federal Government alone increased 680% from 2006 to 2011 Moreover, according to a recent survey more than 60 percent of IT experts interviewed by the Pew Internet and American Life Project, a major cyberattacks will happen between now and 2025. . The rise in the number of cybersecurity attacks and the increasing sophistication of the various methods used to perpetrate many of the cyber intrusions means that the traditional, education and human resource models used to educate and employ cybersecurity workforce must be modified. The country cannot afford to wait until the "cyber Pearl Harbor" predicted by the former Secretary of Defense Leon E. Panetta (2012).

According to a report from Verizon "Data Breach Investigations" (Baker, 2014), the most common cybersecurity crimes come from various small online attacks, such as people clicking on malicious web links and choosing easy-to-guess passwords. The Verizon report is one of the top annual reports of Internet-related crime, it includes information from more than 50 organizations around the world and is used to analyze more than 63,000 security incidents and 1,300 confirmed breaches. Verizon analyzed 10 years of data breach data, and specifically stated that most organizations cannot keep up with cybercrime, and the bad guys are winning. The above examples of cyberattacks provide a sobering explanation for why it is so important that the country rapidly formulate a comprehensive and proactive strategy to recruit, prepare, train and educate, and then deploy a competent cybersecurity workforce.

The above noted array of information, statistics, and data illustrate the mounting threat presented by the contemporary malevolent attackers in the cyber space. Clearly, the threats in cyber space are growing in frequency, severity, sophistication, and level of risk. The cyber space threat encompasses a broad spectrum of activities including cyber crime, cyber terrorism, and cyber espionage. A comprehensive and

systematic cybersecurity strategy is sorely needed to counter this threat in an effective and efficient manner. An essential component to an effective solution will also require the growth and sustainment of a capable cybersecurity workforce. The pool of available military veterans offers the country a viable and valuable resource that should and can be tapped immediately for the cybersecurity workforce.

THE UNITED STATES NATIONAL CYBERSECURITY AGENDA

Clearly, securing American cyberspace means that the country must develop a technologically-skilled workforce comprised of educated cyber-skilled personnel, and establish an effective pipeline of future employees. Billions of dollars are spent on new technologies to help secure the U.S. in cyberspace. However, it will also take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet the challenge of securing cyberspace. The Bush administration addressed the cybersecurity threat by formulating and implementing the Comprehensive National Cybersecurity Initiative (CNCI) in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23).

Upon taking office in 2008, President Barack Obama stated that the cybersecurity risk faced by America was a serious economic and national security threat. The President ordered a thorough review of federal efforts to defend the U.S. information and communications infrastructure and the development of a comprehensive approach to securing the nation's digital infrastructure. President Obama determined that the CNCI initiatives should become key elements of a comprehensive U.S. national cybersecurity strategy. These CNCI will play a key role in supporting the achievement of many of the key recommendations of the Cyberspace Policy Review. The Cyberspace Policy Review published in May 2009, concluded that our information technology and communications infrastructure was extremely vulnerable and that numerous attacks have resulted in the loss of hundreds of millions of dollars to cyber criminals. Additionally, the policy review noted that nation-states and other non-state entities have stolen vital intellectual

property from the private sector, and sensitive national security and military information.

The CNCI consists of mutually reinforcing initiatives with the major goals of securing the United States in cyberspace: (1) to establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events... and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions. (2) To defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies. (3) To strengthen the future cybersecurity environment by expanding cyber education… and develop strategies to deter hostile or malicious activity in cyberspace. Specifically, CNCI Initiative #8 "Expand cyber education" is the core function that must be effectively implemented to ensure the successful staffing and sustainment of a quality cybersecurity workforce.

The National Initiative for Cybersecurity Education (NICE) was established to lead the effort aimed at meeting the goals outlined in CNCI Initiative 8, which addresses the nation's cybersecurity needs related to public awareness, education, professional development, and talent management. In simple terms, the need for cybersecurity specialists is growing exponentially due to increasing criminal, state-sponsored, and terrorist threats. Currently, there are not enough cybersecurity professionals to meet the volume and ever-changing nature of cybersecurity work. Compounding the gap between need and available workforce is the length of time cybersecurity specialists need to adequately develop the necessary skills. The cybersecurity field necessitates that its practitioners grow, evolve, and maintain highly-technical skills that take a significant amount of time to mature. Therefore, it is imperative that both the government and private sector organizations practice effective workforce planning in cybersecurity.

Congress codified the nation's cybersecurity policy by enacting the Cybersecurity Enhancement Act of 2010 (HR 4061), which authorized "hundreds of millions of dollars for cybersecurity research and education." This appropriation

included funding for the National Science Foundation "to increase the size and skills of the cybersecurity workforce" and aimed to increase "research and development, standards development and coordination, and public outreach" in cybersecurity. Congress subsequently enacted follow-on legislation in the form of The National Cybersecurity and Critical Infrastructure Protection Act of 2014. Within that Act two specific sections are focused countering the cybersecurity threat. First, Title I: Securing the Nation Against Cyber Attack - (Sec. 102) amends the Homeland Security Act of 2002 (HSA) to require the Secretary of Homeland Security to conduct cybersecurity activities, including the provision of shared situational awareness among federal entities to enable real-time, integrated, and operational actions to protect from, prevent, mitigate, respond to, and recover from cyber incidents. Second, Title III: Homeland Security Cybersecurity Workforce - (Sec. 301) amends the HSA to add provisions entitled the Homeland Security Cybersecurity Boots-on-the-Ground Act, requiring the Secretary of the Department of Homeland Security (DHS) to: (1) develop occupation categories for individuals performing activities in furtherance of DHS's cybersecurity mission, (2) ensure that such categories may be used throughout DHS and are made available to other federal agencies, and (3) conduct an annual assessment of the readiness and capacity of the DHS workforce to meet its cybersecurity mission.

It is evident that the United States government and its policy makers have recognized that existing and emerging cybersecurity threats are menacing the country on a daily basis. Both President Obama and Congress have put forth national policies and implementing actions to build the nation's cybersecurity capabilities and workforce staffing. National efforts to address the cyber-based needs include the establishment of federally funded programs, initiatives, and systematic approaches that serve as a viable launching platform for the strategy to enhance the recruitment, education and retention of the US cybersecurity workforce. However, there are still significant deficiencies that must be addressed if America is going to be successful in cyberspace.

In 2000, the National Science Foundation (NSF) implemented the Scholarship for Service program (SFS) to fund undergraduate and post-graduate students'

education in exchange for employment in a Federal, State, Local, or Tribal government's IT workforce after graduation. In December 2011, the National Science and Technology Council partnered with the NSF to expand the coordinated federal strategy and program for cybersecurity education and employment. The joint federal effort was built around two focused tracks: *Scholarship Track and Capacity Track*. The *Scholarship Track* provides funding to colleges and universities for scholarships to students studying in the information assurance and cybersecurity fields. The *Capacity Building Track*, provides funds to colleges and universities to improve the quality and increase the production of high-quality information assurance and cybersecurity professionals by providing support for education efforts within higher education institutions teaching Science, Technology, Engineering and Mathematics (STEM) disciplines (National Science Foundation, 2014). The federal funds available from these two tracks can be combined with the veteran's benefits provided by the G.I. Bill for education to enhance the overall education process. Moreover, this combined scholarship/stipend package can serve as a motivational incentive for the interested and qualified veterans to enter the cyber education pipeline and continue into the cybersecurity workforce. An additional incentive could include the establishment of a retention/performance bonus based on years of service, excellent performance, continued professional development, and for remaining in the cyber workforce for a specified period of time.

At approximately the same time, the Department of Defense started a similar effort, the Information Assurance Scholarship Program (IASP). Both programs also provide capacity-building grants to academic institutions to bolster cyber security education and workforce development. Nevertheless, the efforts to date have failed to adequately recruit, educate, and employ sufficient numbers of qualified cyber-skilled personnel to meet the nation's needs. Therefore, this paper argues that another approach is warranted that involves focusing human resources and education efforts on integrating military veterans into building the nation's cybersecurity workforce. The innovative use of programs, such as Scholarship Track and Capacity Track can enable the education pipeline to increase the number of

students of the United States higher education enterprise to produce cybersecurity professionals. Moreover, these types of focused approaches to cyber education and employment are especially suited for bringing the military veteran into the cyber education process and subsequently into the cybersecurity workforce.

THE MILITARY VETERAN: A CYBERSECURITY WORKFORCE SOLUTION

The U.S military is comprised of the Army, Navy, Air Force, Coast Guard, and Marine Corps, which are all under the command of the U.S. President as Commander in Chief. Over the country's history the military has played a vital role in the geopolitical arena of international affairs related to national security and defense. The U. S. military has evolved with America from a new nation fighting Great Britain for independence (1775–83); through the historical American Civil War (1861–65); through two World Wars, and numerous other smaller conflicts (The Korean War and the War in Viet Nam); the Cold War era (1945 – 91); and the War on Terrorism (2001–present) (HQDA, 2003). U.S. Statutory law, 38 U.S.C. § 101 defines a veteran as an individual who served in the active military, naval, or air service, and who was discharged or released under honorable conditions.. For the purposes of this paper, a veteran is defined as anyone who served on active duty in any job capacity while a member of the Army, Navy, Air Force, Marines or Coast Guard active components, or of the National Guard or Reserves, and was not discharged dishonorably.

Today, America is often described as the world's sole remaining superpower of the 21st century. The remarkable fact is that as great as the country has been and as great as it is, its military force has always consisted of citizens who are willing to serve and defend the nation. It is the citizen-turned-soldier serving as a dedicated member of the nation's military who has demonstrated the character, honor, sense of duty, and sacrifice necessary to make America great. The premise of this paper's thesis is that it is the cultivation of the military culture that serve as the incubator of the military veteran's unique experience, knowledge, skills, and intellectual capacities. Moreover, it is the development and reinforcement of the tenets of the

military culture that contributes to the growth of a system of beliefs that manifest themselves as invaluable attributes like leadership, accountability, resiliency, problem solving, and adaptability in these veterans.

Over America's history there are numerous examples of military veterans who have risen to the occasion and helped the country through some very trying times. Former military personnel have long had successful careers in both the public and private sectors, following their return to civilian life. Many of these men and women have left an indelible mark on American history, rising to the upper echelons of U.S. government - Presidents George Washington, Ulysses S. Grant, Dwight D. Eisenhower, Theodore Roosevelt, Harry S. Truman, John F. Kennedy, Jimmy Carter, and Ronald Reagan were all military veterans. For these reasons and others, Americans have more confidence in the military than any other institution or group in the country. The American confidence is well placed, and it is in our Nation's interest to continue to invest in our military veterans. They have much to offer our communities long after they hang up the uniform (Mendes & Wilke, 2013).

While the vast majority of veterans are not going to become president, in general they strengthened our country by their service and as a result, are civic assets with great potential to continue serving and leading in our communities, businesses, and governments. Examples of veterans continuing to serve abound, all you have to do is look for them. Consider the following examples in the private sector and the corporate world, where veterans are represented by the likes of Alex Gorsky, the chief executive and chairman of Johnson & Johnson, and Bob McDonald, who guided Procter & Gamble to extraordinary growth while serving as its chairman, president, and chief executive, from 2009 to 2013. Another noted military veteran who has provided service while occupying a key civilian positions is retired General Colin Powell, former Chairman of the Joint Chiefs of Staff and Secretary of State. Moreover, business representatives report that hiring veterans is good business, according to detailed and lengthy interviews with 87 individuals representing 69 companies. The companies cited numerous reasons for hiring military veterans,

with an emphasis on veterans' leadership and teamwork skills, character, discipline, and expertise (Harrell & Berglass, 2012).

Further examples of the value added contribution of military veterans include the following individuals. David Oclander, an army veteran, who moved to Chicago to help disadvantaged kids in the tough neighborhoods in the city. He is now a Principal Fellow at the Noble Network of Charter Schools (Warner, 2014). David's service after the military has helped the Noble Network schools achieve an overall college matriculation rate of 90% and eight of their ten campuses ranked among the top ten schools based on ACT performance in 2014. Tammy Duckworth was one of the first Army women to fly combat missions during Operation Iraqi Freedom until her helicopter was hit by an RPG (Carter and Almasy, 2013). She lost her legs and partial use of her right arm in the explosion. Despite these injuries, she continued to serve our Nation, first as an Assistant Secretary of Veterans Affairs and now as a Congresswoman for Illinois's 8th Congressional District (Office of the Joint Chiefs of Staff, 2014). Or consider Jacob Wood, who honorably served four years in the Marine Corps, deploying to Iraq in 2007 and Afghanistan in 2008. He graduated Scout-Sniper School at the top of his class and in 2007 he was awarded the Navy and Marine Corps Commendation Medal with "V" for actions in Iraq. Following his service in the Marines, Jake co-founded Team Rubicon, a non-profit disaster relief organization that puts veteran volunteers to work in responding to disasters around the world (Martinez, 2015). Jacob Wood is another example of the service pedigree that resides within most military veterans. Veterans often continue their faithful service by channeling their unwavering commitment and dedication to fulfill critical needs in their communities.

These few examples represent the immense potential that most veterans have to continue serving after they've hung up their uniform. They are counted among the many veterans who have demonstrated the competencies, traits, and leadership skills they acquired while serving in the military and later in essential civilian roles. Empirical support for reintegration of veterans into the cybersecurity workforce includes academic research from the fields of business, psychology, and sociology.

In general, the literature strongly links characteristics that are generally representative of military veterans to enhanced performance and organizational advantage in the context of a competitive and dynamic business environment (Cooker, 2014). In other words, the academic research supports a robust, specific, and compelling argument for hiring individuals with military background and experience (Berglass & Harrell, 2012). According to Steve Cooker, more than two-thirds of employers report having special talent needs that a veteran candidate would be more qualified to fill than a non-veteran candidate. So employers recognize the unique skills that veterans possess.

THE GI BILL: THE EDUCATION ENABLER

Because America felt a moral obligation to help prepare our veterans to live a fulfilling life after they have served honorably, the country established the first GI Bill of Rights in 1944, which was signed into law by President Franklin D. Roosevelt. Almost eight million veterans took advantage of the education and training benefits it offered. Since the establishment of the first GI Bill millions of veterans from later conflicts benefited from similar measures. Seventy-one years after the first GI Bill was signed, Congress passed the Post-9/11 Veterans Educational Assistance Act. The Post-9/11 GI Bill expands the educational benefits of the original GI Bill, providing veterans with full funds to attend a public undergraduate program for four years, with additional stipends for housing and books. A review of available statistics reveals that each version of the G.I. Bill had an important and positive influence on improving the lives of returning veterans, by providing access to higher education. A significant number of each generation of military veterans have avail themselves to G.I. Bill education benefits. A greater percentage of Vietnam veterans used G.I. Bill education benefits (72 percent) than World War II veterans (51 percent) or Korean War veterans (43 percent). More recently, the Post-9/11 G.I. Bill has paid for nearly 1 million veterans of the Iraq and Afghanistan wars to go to school at a cost of about $30 billion since 2009 (Wagner, Cave, & Winston, 2013).

On August 3, 2009, President Barack Obama attended a ceremony marking the creation of the GI Bill benefits program over sixty-five years earlier. During the ceremony he acknowledged the contributions of military veterans over the history of the country in both peace and war. The president noted that education is the currency that can purchase success in the 21st century, and that the opportunity to participate in the education process was earned by our military veterans. In November 2009, President Obama further acknowledged both the service of military veterans by issuing an executive order promoting the recruitment and employment of veterans within the Federal Government. The executive order established an interagency Council on Veterans Employment, which is co-chaired by the Secretaries of Labor and Veterans Affairs. In support of this initiative, the Federal Government have established various websites to assist veterans with employment and training opportunities.

Applicants for military service must meet academic, moral, and physical requirements that disqualify most of their peers. In fact, only 25 percent of Americans ages 17 to 24 are physically, mentally, and morally qualified for military service (Gilroy, 2013). According to the U. S. Census Bureau (2012) all Army and Marine Corps and 99% of Air Force and Navy enlisted personnel accessions were high school graduates in FY 2012. Consequently, a higher percentage of veterans ages 25 and over have a high school diploma than their non-veteran counterparts. According to Thomas Meyer from Philanthropy Roundtable noted, the current generation of service members "exceed national norms, on average, in education and intelligence, health and character qualities." In sum, the current generation of veterans exceeds, on average, national norms in education and intelligence; moreover, more veterans seek some post-secondary education than do their non-veteran peers. These facts are strong evidence that the nation's military veterans possess the necessary knowledge, skills, abilities, and potential to successfully meet the requirements for completion of education and employment in the cybersecurity workforce.

There is a recognized persistent national shortage of skilled cyberspace personnel that negatively impacts the social, economic and political dimensions across the

nation and potentially putting national security at risk (Evans & Reeder, 2010). In response to this challenge, America must expand education and employment opportunities to cultivate talent from within the available personnel most capable of successfully completing the rigors and challenges of an aggressive education process. The military veteran is uniquely qualified to cope with the stressors, mental and physical conditions, and academic endurance necessary to complete the cyber security educational program.

The military profession is unlike any other profession. The demands of military life creates and reinforces a unique set of personal qualities and attributes in its service members built on the inculcation of professionalism, ethics, ethos, and belief in a value system. In the military every service members' performance is evaluated and all members are developed, counseled and mentored throughout their career. The military emphasizes discipline and order, priority of the group over the individual, and use of specific rituals and symbols to convey important meanings and transitions. For example, the Army emphasizes seven (7) core values to establish and instill a shared set of beliefs, way of thinking and behavior expectations in every soldier:

- **Loyalty** – Bear true faith and allegiance to the U.S. Constitution, the Army, your unit, and fellow Soldiers.
- **Duty** – Fulfill your obligations. Accept responsibility for your own actions and those entrusted to your care.
- **Respect** – Treat others as they should be treated.
- **Selfless Service** – Put the welfare of the nation, the Army, and your subordinates before your own.
- **Honor** – Live the Army Values.
- **Integrity** – Do what's right, both legally and morally.
- **Personal Courage** – Face fear, danger, or adversity, both physical and moral.

Each of the military branches has established and consistently reinforced a pattern of behaviors based on a set of beliefs that epitomizes its cultural system. The military culture is instilled and reinforced in each service member from the very first day that each of them takes their oath of oath of enlistment and oath of office (for commissioned officers). Moreover, within each service there is a constant emphasis on core values which serve as a normative guide for personal and professional behavior patterns. Service members learn these values in detail during initial training, and from then on they are expected to live them every day in everything they do - whether they're on duty or off. These values are the building blocks for the military culture and the most fundamental element of the institutional identity of the military services. The Army's Training and Doctrine Command Culture Center (2007) defines culture as a "dynamic social system," containing the values, beliefs, behaviors, and norms of a "specific group, organization, society or other collectivity" learned, shared, internalized… by all members of that society. Another way of stating this is by using the term "cultural competence" which implies that an individual is able to perform effectively in a number of diverse environments and refers to an ability to interact effectively with people of different cultures and socio-economic backgrounds (Chamberlain, 2005). This paper argues that the dynamics of exposure, acceptance, faithfulness, and routine performance of duties pursuant to the principles and tenets of the military culture makes the military veteran an excellent candidate for cybersecurity education for the express purpose of employment in the cyber security workforce.

RECOMMENDATIONS FOR THE WAY AHEAD

- Create a national cybersecurity clearinghouse for veterans, key stakeholders, private sector entities and higher education communities – for the sharing of knowledge, resources, education and employment opportunities to help increase cybersecurity capabilities, and optimizing collaboration to eliminate unnecessary duplication.
- Establish an aggressive education and employment outreach and support program aimed specifically at recruiting and training military veterans for these cybersecurity workforce.

- Maximize use of social media and networking to enhance the reintegration process for military veterans.
- To aid in translating military skills and facilitate the transition process, DOD, DHS and the Department of Veterans Affairs (VA) should seek public-private partnerships with American companies and qualified nonprofit organizations that specialize in employment and supporting veterans.
- Create both national and regional education consortiums to serve as national facilitators and advocators for cybersecurity education.
- DOD and Department of Labor (OL should provide guidance for companies to help them interpret which veteran candidates were successful, or even highly successful, in performing their duties while in uniform.

CONCLUSION

As explained above, most veterans possess valuable traits, characteristics and attributes that empower them with great potential to serve and lead our nation's communities after their service. Moreover, they are especially capable and very suited for the cyber security workforce. It is important to remember that every service member came from our communities and that they all will return to our communities. America has an obligation to offer our veterans every opportunity to continue their service and become better citizens upon completion of their military service. Otherwise, we might miss an opportunity to incorporate veterans into our cyber security workforce as the essential assets that they are. Veterans via their military service, acquire and/or increase personal qualities, and their sense of duty, therefore, they possess exceptional potential to help fill the gaps and vacancies currently existing in the US cyber- security workforce. America should take advantage of the opportunity to capitalize on a proven human capital asset by focusing a special effort on placing its military veterans into the cybersecurity workforce. America can enhance its cybersecurity capabilities by implementing a proactive and aggressive effort to integration military veterans into the cybersecurity workforce in order to utilize their specialized skills, experiences and training.

REFERENCES

[1] Arrington, M. (2010). Google defense against large scale Chinese cyber attack: May cease Chinese operations. Tech Crunch. Retrieved from http://techcrunch.com/2010/01/12/google-china-attacks/.

[2] Baker, W. (2014). Verizon's data breach investigations report series. Retrieved from http://www.verizonenterprise.com/DBIR/2014/.

[3] Carter, C. J. and Almasy, S. (2013) CNN News Report: Former troops say time has come for women in combat units. Retrieved from http://www.cnn.com/2013/01/23/us/women-combat-troop-reaction/.

[4] Chamberlain, S. P. (2005). Recognizing and responding to cultural differences in the education of culturally and linguistically diverse learners. Intervention in School & Clinic, 40 (4), pp. 195-211.

[5] Clayton, M. (2010). US oil industry hit by cyberattacks: Was China involved? The Christian Science Monitor, 25 January 2010. Retrieved from http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China.../

[6] Congress (2014). H.R.3696 - 113th Congress (2013-2014): National cybersecurity and critical infrastructure protection act of 2014 - Title I: securing the nation against cyber Attacks. Retrieved from https://www.congress.gov/bill/113th-congress/house-bill/3696

[7] Conley, D. T. New conceptions of college and career ready: a profile approach to admission. *Journal of College Admission*, No. 223, April 2014, pp. 12–23.

[8] Cooker, S. (2014). Fighting veteran unemployment by closing the skills translation gap. Monster.com. Retrieved from http://www.military.com / veteran-jobs / career-advice / 2014 / 11 / 18 / fighting-veteran-unemployed....

[9] Duckworth, A L., Christopher P., Michael D. M., and Dennis D. R., "Grit: perseverance and passion for long-term Goals," *Journal of Personality and Social Psychology*, Vol. 92, No. 6, 2007, pp. 1087–1101.

[10] Duckworth, A. L., and Patrick D. Q., Development and validation of the short grit scale (Grit-S). *Journal of Personality Assessment*, Vol. 91, No. 2, 2009, pp. 166–174.

[11] Dweck, Carol S., Gregory M. W., and Geoffrey C. L. Academic tenacity: Mindsets and skills that promote long-term learning. Retrieved from http://collegeready.gatesfoundation.org/article/ academic-tenacity-mindsets-and-skills-promote-long-term-learning.

[12] Evans, K. and Reeder, F. (2010). A human capital crisis in cybersecurity - technical proficiency matters. Washington, D.C: April 2010.

[13] Eisler, P. (2009). "Reported raids on federal computer data soar. USA TODAY, 17 February, 2009. Retrieved from http://30.usatoday.com/news/washington/2009-02-16-cyber-attacks_N.html.

[14] Franken, Robert E. *Human Motivation*, 3rd ed., Pacific Grove, Ill.: Brooks/Cole, 1993.

[15] Gilroy, Curtis, Dr. (2009) Statement to the House, Committee on Armed Services, Recruiting, Retention and End Strength Overview, Hearing, March 3, 2009. Retrieved from http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg50088/pdf/CHRG-111hhrg50088.pdf.

[16] Government Accounting Office. Executivegov.com. (2012). Retrieved from http://www.executivegov.com/2012/04/gao-federal-cyberspace-incidents-up-680-over-5-years/.

[17] Gorman, S. (2009). "Electricity grid in U.S. penetrated by spies," Wall Street Journal, 8 April 2009. Retrieved from http://online.wsj.com/article/SB123914805204099085.html.

[18] Griffin, P. E., and Esther C. "Project method overview," Patrick Griffin and Esther Care, eds., Assessment and Teaching of 21st Century Skills, Vol. 2: Methods and Approaches, Dordrecht, the Netherlands: Springer, 2015.

[19] Hamilton, L. S., Heather L. S., Brian S. S., & Steele, J. L. Improving accountability through expanded measures of performance," *Journal of Educational Administration*, Vol. 51, No. 4, 2013, pp. 453–475.

[20] Harrell, M. & Berglass, N. (2012) Employing America's veterans. Military, Veterans and Society Program for a New American Security (CNAS). Retrieved from http://www.cnas.org/files/documents/publications/ (retrieved October 27, 2014).

[21] Headquarters, Department of the Army. (2003) Field Manual, No. 1–20 *Military History Operations*, Washington, DC, 3 February 2003. Retrieved from http://www.train.army.mil

[22] Heckman, J, J. Schools, skills, and synapses," *Economic Inquiry*, Vol. 46, No. 3, July 2008, pp. 289–324.

[23] Inserra, D. and Rosenzweig, P. (2014). Continuing federal cyber breaches warn against

[24] Cybersecurity regulation. Heritage Foundation Issue Brief No. 4288, http://www.heritage.org/research/reports/2014/10/continuing-federal-cyber-breaches-warn-against-cybersecurity-regulation.

[25] Kane, M. T. (2006) *Validation in Educational Measurement*. Robert L. Brennan, ed. 4th ed., Westport, Conn.: Praeger Publishers. pp. 17–64.

[26] Kaspersky Lab. (2012) Security Bulletin: By the Numbers. Retrieved from http://www.kaspersky.com / about / news / virus / 2012 / 2012_by_the_numbers_Kasp....

[27] Martinez, S. (2015). Team Rubicon's co-founder tells West Michigan about the importance of veteran volunteers. The Grand Rapids Press. Retrieved from MLive.com Online. http://www.mlive.com / business / west-Michigan / index.ssf / 2015 / 01 / co-founder_of_team_rubicon...

[28] McAfee (2014). "Net losses: estimating the global cost of cybercrime". Retrieved from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

[29] Mendes, E. & Wilke, J. (2013). Americans' confidence in congress falls to lowest level on record. Gallup. Retrieved from http://www.gallup.com/poll/163052/americans-confidence-congress-falls-lowest-record.aspx (retrieved Nov. 4, 2014).

[30] Meyer, T. (2013). Serving Those Who Served: A wise giver's guide to assisting veterans and military families. Washington: The Philanthropy Roundtable, 2013, 153.

[31] Moule, Jean (2012). Cultural competence: A primer for educators. Wadsworth/Cengage, Belmont, California.

[32] National Science Foundation. (2013). NSF joins forces with Intel and GE to move the needle in producing U.S. engineers and computer scientists," press release 13-081, May 8, 2013. Retrieved from http://www.nsf.gov/news/news_summ.jsp?cntn_id=127902.

[33] National Science Foundation. (2014). CyberCorps(R) scholarship for service (SFS): Defending

[34] America's cyberspace. Retrieved from http://www.nsf.gov/pubs/2014/nsf14510/nsf14510.htm.

[35] Office of the National Counterintelligence Executive, (2011). Foreign spies stealing U.S. economic secrets in cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011. (ONCIX 2011 Report). Retrieved

from http://www.ncix.gov / publications / reports / fecie_all / Foreign_Economic_Collect...

[36] Pagliery, Jose (2014). Your internet security relies on a few volunteers". CNN Money. Cable

[37] News Network.com. Retrieved from http://money.cnn.com/2014/04/18/technology/security/heartbleed-volunteers/

[38] Panetta, L. (2012) Remarks to the business executives for national security. New York City, October 11, 2012. retrieved from www.defense.gov

[39] Pellegrino, J. W., & Margaret L. H. (2012). Education for life and work: Developing transferable knowledge and skills in the 21st Century, Washington, D.C.: National Academies Press.

[40] Power, R. (2002). CSI/FBI computer crime and security survey. *Computer Security Issues and Trends*, vol. 8, no. 1 (Spring 2002).

[41] Saavedra, A. R. & Opfer, D. V. (2012). Learning 21st-century skills requires 21st-Century teaching," Phi Delta Kappan, Vol. 94, No. 2, October 2012, pp. 8–13.

[42] Steinberg, J. (2014). Massive Internet security vulnerability: Here's what you need to do.

[43] Forbes. Retrieved from http://www.forbes.com / sites / joseph steinberg / 2014 / 04 / 10 / massive-internet-security.

[44] Symantec Internet Security Threat Report. (2011). Retrieved from https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf.

[45] Symantec Internet Security Threat Report (2014) Volume 19. Retrieved from http://www.itu.int / en / ITU-D / Cybersecurity / Documents / Symantec_annual_internet....

[46] U.S. Army Training and Doctrine Command Culture Center. (2007). Culture education and training strategy for the U.S. Army. Fort Huachuca, AZ: U.S. Army Intelligence Center.

[47] U.S. Census Bureau (2012). Veteran status, 2012 American community survey estimates. Retrieved from http://factfinder2.census.gov/faces/tableservices/jsf/pages/html.

[48] Virilis, N., Serrano, O., & Dandurand, L. (2014). Big data analytics for sophisticated attack detection. Retrieved from http://www.cis.aueb.gr / Publications / ISACA%20-%20Big%20data%2.

[49] Wagner, M., Cave, A., and Winston, H. (2013). National security: GI bill covered tuition for nearly

[50] a million post-9/11 veterans without tracking their progress. The Center for Public Integrity. Retrieved from http://www.publicintegrity.org / 2013 / 09 / 03 / 13297 / gi-bill-covered-tuition.

[51] Warner, Margaret. (2014). A veteran's tough love message to at-risk kids and fellow vets. PBR News Hour. Retrieved from http://www.youtube.com/watch?v=0hL9F08wRWM .

[52] White House (2009). The Comprehensive national cybersecurity initiative. Retrieved from http://www.whitehouse.gov / issues / foreign-policy / cybersecurity / national-initiative.

[53] White House (2013). Can we instill productive mindsets at scale? A review of the evidence and an initial R&D agenda, white paper prepared for White House meeting on excellence in education: The importance of academic mindsets. Washington D.C.

[54] Yuan, K. & Vi-Nhuan L. (2014). Measuring deeper learning through cognitively demanding test items: results from the analysis of six national and international exams. RAND Corporation, Santa Monica, Calif. Retrieved from http://www.rand.org/pubs/research_reports/RR483.html.