YOTTA
POWERING CYBER SECURITY READINESS

An Ecosystem for Cyber Workforce Education, Training, and Readiness

George W. Hinckley | Yyotta LLC | Stafford, Virginia

Yyotta Thought Leadership Series

www.Yyotta.com

Abstract

Historically, Computer Network Defense (CND) training has been conducted through “school-house” learning followed by some practical application with little to no hands-on follow-up training. The Department of Defense (DoD) Information Assurance (IA) Range was developed to provide a safe, virtualized environment within which realistic CND training could occur. The advent of the DoD IA Range has allowed for more realistic practical application during the formal training process but its use can be expanded. To broaden the scope of the environment, this paper will propose an innovative ecosystem for training the United States’ Cyber Workforce. This ecosystem includes formal military and academic training enabled by industry-, academia- and military-based education. By providing equal access to and for military, academia, and industry, the knowledge base (e.g., attack vectors, effective methods, etc.) can be widened and shared in a cooperative and collaborative environment. Academia and industry are critical components of the ecosystem and enable cyber workforce education, training, and readiness (CWETR). Academia is on the forefront of standards-based curriculum development and industry supports both technology development and manpower. The proposed ecosystem would enable collaboration among government, academia, and industry thus allowing for baselining the education and training of the cyber workforce as well as an environment within which operational readiness for tactical cyber operations can be evaluated and assessed. Additionally, the ecosystem proposes access to the DoD IA Range by military, academic, and industry experts, practitioners and researchers, thus providing a common resource to learn, research, test, and share from. Further, this paper will explore the benefits of providing access to the DoD IA Range to tactical forces, creating the ability to push cyber training (including attack and defense) to the lowest levels of the operating forces thereby enhancing the efficacy of the cyber workforce and further protecting our tactical networks and ultimately our national networks. This paper was originally present at the *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) in 2013.*

About the Author

Mr. Hinckley serves as a Managing Partner at Yyotta LLC where he is responsible for corporate and strategy development, as well as lead strategic and business architect and planner of the Yyotta community of practice platforms and ecosystems. Shortly after graduation from high school, Mr. George Hinckley enlisted in the Marine Corps and was subsequently commissioned a 2nd Lieutenant upon graduation from the University of Missouri with a Bachelor of Science Degree in Mechanical Engineering. Primary military occupational specialties in the Marine Corps were Signals Intelligence/Electronic Warfare. In 1992, he retired from Marine Corps Systems Command, Program Manager Intelligence Systems at Quantico, VA and joined Vitro Corporation as a Group Supervisor then Program Manager supporting Army Intelligence/Communications Programs. He left Vitro in 1996 and spent nine years with BRTRC Inc. as Program Manager then Vice President supporting program management at Marine Corps Systems Command and S&T development at the Office of Naval Research. During the period 2005 to 2011, he worked with MTCSC Inc. as Senior Advisor and Director of the Center for Technology where he supported the establishment of the DoD IA Range. Currently, he serves as: President, Associates in Business, Engineering & Technology Inc.; Founder & Chief Executive Officer (CEO), The Applied Research & Education Institute, Inc., a non-profit corporation for education, workforce & economic development; and, Senior Assistant to the President, Cyber Workforce Education, Northern Virginia Community College.

An Ecosystem for Cyber Workforce Education, Training, and Readiness

George W. Hinckley | Yyotta LLC | Stafford, Virginia | GeorgeHinckley@yyotta.com

Introduction

Our nation is under attack. The "Cyber" threat is everywhere and proliferating. The malicious threat against us is being executed by both state and non-state actors. However, our networks are also being probed by individuals having no malicious intent, at least not initially, but simply pursuing the art of the possible. This threat must be met with a very strategic approach that leverages the best of what can be offered by government, academia, and industry. In order to prepare for and meet this national security challenge we must establish a collaborative ecosystem among these three primary stakeholders. Each stakeholder group has something to gain and this paper will address each in its own right.

Cyber Workforce

It is officially recognized that we do not have the workforce necessary for deployment against this threat. The US Cyber Command has stated that there is a need for 30,000 newly trained "cyber warriors" within the next few years. To adequately meet the requirement, the workforce "pipeline" needs to be established in a similar manner to how other manpower needs are met by the Armed Services. It needs to be viewed quantitatively as input flow considerate of attrition, for whatever reason. However, a unique aspect of this Services-based workforce is that they, most likely, will eventually transition to the larger community of interest whether government civilian or contractor. Holistically, the overall Cyber Workforce will benefit.

Education

NIST NICE Framework

Previous Committee on National Security Systems (CNSS) standards used by Centers of Academic Excellence (CAEs) in educational programs evolved from earlier Telecommunications Security Group standards. CNSS standards have received criticism from industry and academia for being too focused on National Intelligence community systems. In 2001, the National Institute of Standards and Technology (NIST) was tasked to create an interagency taskforce to define professional requirements in cybersecurity. The NIST National Initiative on Cybersecurity Education (NICE) Framework, shown in Figure 1 below, defines more than 31 specialization roles in cybersecurity, each with associated tasks and knowledge, skills, and abilities (KSAs). These KSAs form the basis of new educational standards for the Centers of Academic Excellence institutions – defined as "Knowledge Units" by the National Security Agency (NSA) and Department of Homeland Security (DHS).

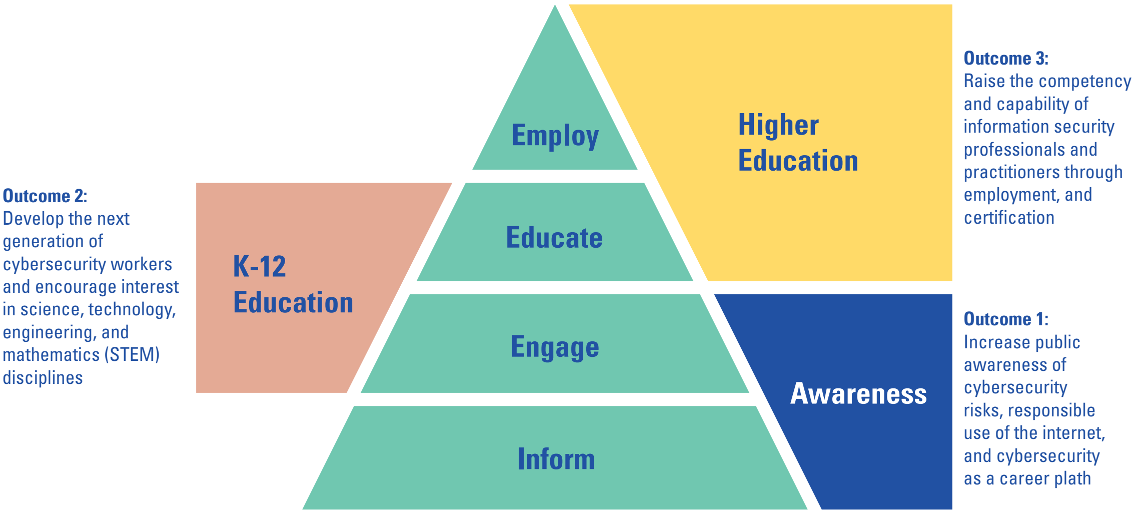
Employ
Educate
Engage
Inform
Higher Education
K-12 Education
Awareness
Outcome 3:
Raise the competency and capability of information security professionals and practitioners through employment, and certification
Outcome 2:
Develop the next generation of cybersecurity workers and encourage interest in science, technology, engineering, and mathematics (STEM) disciplines
Outcome 1:
Increase public awareness of cybersecurity risks, responsible use of the internet, and cybersecurity as a career plath

Figure 1. The NIST NICE Framework. (Taken from NIST NICE Strategic Plan)

Cybersecurity Education and Training Pipeline

The Cybersecurity Education and Training Pipeline, depicted in Figure 2, is a long term strategy for the Cyber Workforce. Although not a near term issue for the military services, participation with academia and industry relative to professionalizing the Cyber Workforce is expected to yield "recruiting" benefits. For example, the Army Recruiting Battalion located at Fort Meade, Maryland has implemented a Science, Technology, Engineering, and Math (STEM) outreach program to the middle and high schools within their region of responsibility for the primary purpose of mentorship by technology savvy soldiers. The overall Cyber Workforce will benefit from this type of activity whether a young person joins a service or becomes a member of the Cyber Workforce community of interest as a government civilian or contractor. Operational entities such as the Marine Corps Network Operations and Security Center (MCNOSC) will require this flow of, hopefully qualified, personnel

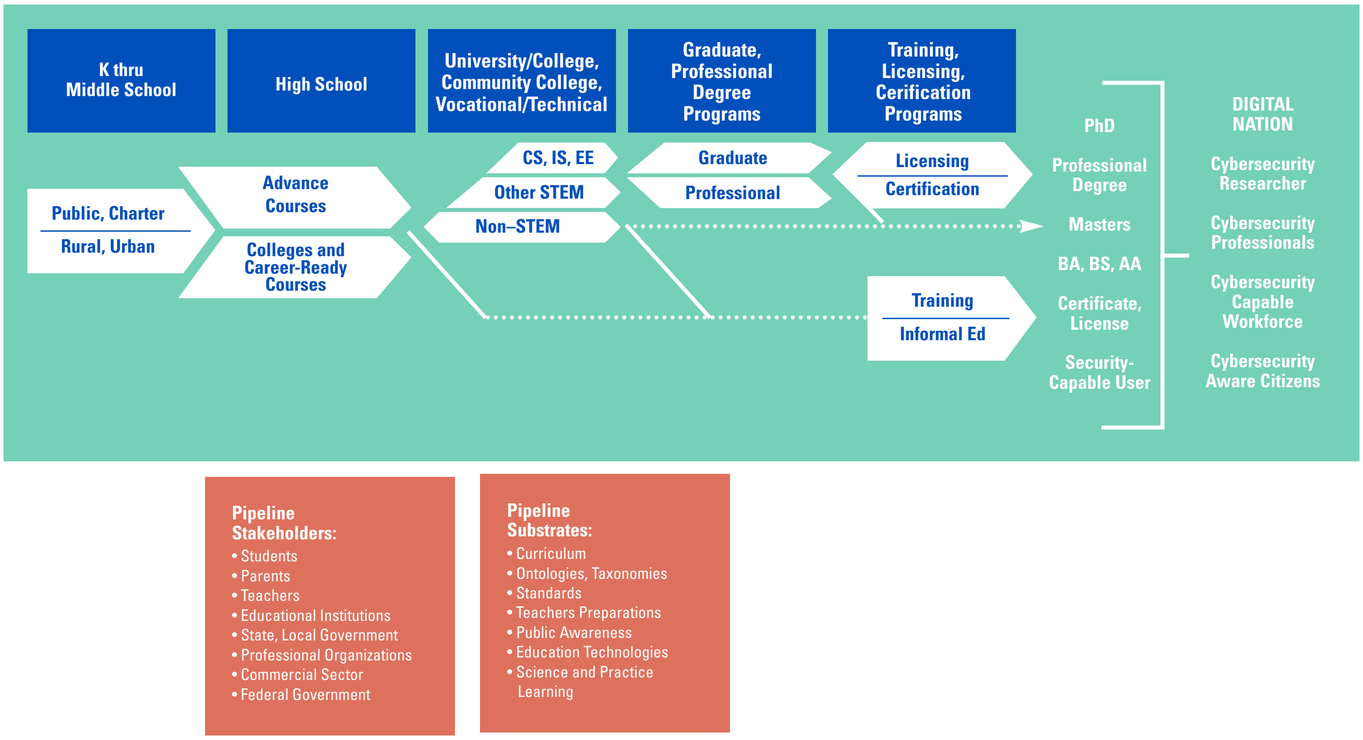

Figure 2. Cybersecurity Education and Training Pipline. (NIST NICE Strategic Plan, 2011)

Military Formal Schools

Military formal schools, such as the Marine Corps Communication Electronic School (MCCES) at Twentynine Palms, California teach our future military workforce. Much of the curricula taught at these formal schools closely matches the content that is presented to students in the civilian sector. It is well known that military formal schools typically trail chronologically relevant curriculum mainly due to the approval process. The approval process for formal military schools curricula is not an issue for Military Occupational Specialties (MOS) that are institutionalized within either the military or commercial sector, i.e. changes are relatively slow. The current cyber threat does not offer that luxury. The pace and dynamic nature of change relative to cyber threats mandates adjustment to curricula in formal schooling that is very problematic. That, coupled with the similarity of curricula and certification for the commercial sector, requires a new approach to educating and training the cyber workforce within the Services.

Community Colleges

There is a community college proximate to every Base, Station, Fort, and Camp within the continental United States (CONUS). The Woodbridge, Virginia campus of the Northern Virginia Community College ("NOVA") is essentially equidistant between Fort Belvoir and Marine Corps Base Quantico. This is important for many reasons but for the purpose of this paper it is especially relevant. NOVA was recently designated a Center of Academic Excellence Two-Year (CAE2Y) for Information Assurance Education by the National Security Agency (NSA) and Department of Homeland Security (DHS).

MOS to Degree

During 2012, a collaboration among NOVA, MCCES, and Headquarters Marine Corps (HQMC) Directorate for Command, Control, Communications, and Computers (C4) evaluated the concept of "mapping" the formal education and training of MOS 06XX Marines to credit based curricula offered by NOVA. The initial effort consisted of an evaluation of the Information Technology (IT) Essentials course taught at MCCES to approximately 2800 Marines annually. The result was promising in that the Course Description Document (CDD) for IT Essentials closely correlated with two courses taught by NOVA: ITN 106 – Microcomputer Operating Systems; and, ITN 107 – Personal Computer Hardware Troubleshooting. The concept was validated and students who have attended MCCES and completed the IT Essentials course are eligible for six advanced standing credits at NOVA. The next step was further correlation by MCCES of IT curricula offered by NOVA to Marine MOS' and the associated CDD's. Subsequent to MCCES relating MOS' to NOVA IT curricula, NOVA proceeded to correlate the CDD's with NOVA curricula, learning objective to learning objective. This rigorous process of correlation and approval at NOVA lasted roughly five months and was completed in December 2012. NOVA leadership, including the President of NOVA, debriefed this effort at the MCNOSC on December 11, 2012 to the Commanding Officer of the MCNOSC and senior leadership from HQMC C4. Also in attendance was an Executive Vice President from the University of Maryland University College (UMUC), a key partner in this endeavor for both delivery of curricula and transfer from NOVA to a four-year baccalaureate degree granting institution that is also recognized as a CAE IA Education.

The "MOS to Degree" effort resulted in defining pathways to the Associate of Applied Science (AAS) degree in Information Systems Technology (IST). This pathway to an AAS IST degree was defined for Marines having the following MOS' along with their eligibility for advanced standing credit based on the MOS as well as military education/training:

- 0612 – Telephone Systems Installers Maintainers; 23 credits
- 0619 – Telecommunications Systems Chief; eight credits
- 0621 – Field Radio Operator; 23 credits
- 0629 – Radio Chief; eight credits
- 0651 – Cyber Network Specialist; 17 credits
- 0659 – NCO Cyber Systems Chief; eight credits
- 0689 – Cyber Security Chief; eight credits
- 0699 – Communications Chief; 20 credits

The collaboration between NOVA and HQMC demonstrated the extreme value for the Cyber Workforce through simple communication of needs and continuous dialogue. The results for the Marines are potentially profound in that the immediate effect is that approximately 14,000 Marines in 2012 are eligible for this program. Table 1 below depicts fiscal year (FY) 2012 on hand manpower as well as FY2013-2014 manpower projections for the MOS' currently mapped along with MOS 2651 which is currently in process.

Table 1 – Manpower Projections for Fiscal Years 2012-2014. (Marine Corps Manpower and Reserve Affairs Enlisted Personnel Availability Digest, 2010)

MOS	0612	0619	0621	0629	0651	0659	0689	0699	2651
FY12OH	2356	349	6070	1020	3158	615	199	346	689
FY13Rqmt	1943	337	5442	999	3026	628	215	339	582
FY14Rqmt	1881	326	5317	975	2986	627	204	333	619

During the period from 3 to 14 December 2012, NOVA conducted a pilot class at Camp Lejeune, NC during normal working hours to twenty Marines. The classroom was their appointed place of duty for this two week "training" evolution. Upon completion, this On Duty Education provided the twenty Marines who attended enrollment in NOVA and three credits toward the AAS IST degree. This training course, paid for with unit funds, was delivered by NOVA adjunct professors. To quote LtCol Randy Pugh, 2d Radio Battalion Commanding Officer: "The evolution of the Marine Corps' missions in the past decade and the convergence of civilian and military technologies (e.g., computer networking) has opened new opportunities to also converge military and civilian education/training." The On Duty Education evolution at 2RadBn demonstrated the relevance of this convergence as well as a methodology for future education/training, particularly in areas where military technologies are essentially the same as those being employed in the civilian/commercial sector. It is more than cost effective, it's critical.

MOS to Degree Program Benefits

The following benefits of the MOS to Degree program are the result of collaborative discussion among representatives of NOVA, HQMC C4, and 2nd Radio Battalion:

- Benefit to the Service
  - Fungible Funding Methodology
  - Efficient MOS Related Training
  - Dual Track MOS Oriented Education
  - Better Qualified/Prepared Personnel for Operations and Transition
- Benefit to the Individual
  - Advanced MOS Related Education/Training
  - Credit Based Training
  - Pathway to Associate Degree
  - Articulation Pathways to Baccalaureate Degree
- Benefit to the Unit
  - "On Duty" Option for Education/Training
  - Enhanced Operational Readiness
  - Improved Morale

Universities

A critical issue for development of the Cyber Workforce is a clear transfer pathway from the community colleges to four-year degree granting institutions. Although not imperative, it is preferred that the four-year institution be a recognized CAE for IA Education such as UMUC. UMUC is important and relevant due to its global reach and historic relationship with the DoD. There will be many other options available to the overall Cyber Workforce as this initiative develops and evolves.

For students attending NOVA, there are many articulation/transfer options for those who complete the AAS IST degree. In addition to UMUC, these options include: George Mason University (GMU), Fairfax, VA; George Washington University (GWU), Washington, DC; University of Mary Washington (UMW), Fredericksburg, VA; and, Old Dominion University (ODU), Norfolk, VA. Similar arrangements could be developed nationwide.

National CyberWatch Center

The National CyberWatch Center ("CyberWatch") was originally one of four Advanced Technology Education (ATE) institutions funded by the National Science Foundation that were focused on cyber security. Today, the lead institution for CyberWatch is Prince George's Community College, located in Maryland proximate to NSA which reflects the appropriate level of engagement necessary for a national strategy to address the development of a Cyber Workforce. CyberWatch member institutions now consist of over 100 Community Colleges and Universities as well as more than 45 Public/Private Supporters including U.S. Cyber Command and Microsoft. In addition to its advocacy of community college cyber security programs, the mission of CyberWatch is to increase quality and quantity of cyber security technicians in the workplace. CyberWatch is doing this through developing college curricula, sponsoring cyber security competitions, and engaging federal agencies and industry in discussions regarding the value of the community college student to the cyber security workplace.

Training

Department of Defense Directive 8570.01

Department of Defense (DoD) Directive 8570.01 establishes policy and assigns responsibilities for DoD Information Assurance Training, Certification, and Workforce Management and authorizes the publication of DoD 8570.01-M that outlines the Information Assurance Workforce Improvement Program. DoD 8570.01-M provides guidance for the identification and categorization of positions and certification of personnel conducting IA functions within the DoD workforce supporting the DoD Global Information Grid (GIG). The DoD IA Workforce includes all individuals performing any of the IA functions described within DoD 8570.01-M. This DoD IA Workforce includes DoD personnel in the 2210 job series (as designated by the Office of Personnel Management), all military personnel required to perform IA functions, and contractor personnel performing IA functions. Basically, DoD 8570.01-M stipulates that all of the DoD IA Workforce should be trained to the same standards.

Academic Exercises

Capstone graduation activities out of academia that align with the needs of the operational IA community, i.e. government and industry, are essential for ensuring that the IA workforce is qualified. One significant change to DoD 8570.01-M, reflected in Change 3 dated January 24, 2012, replaces the word "certified" with "qualified." This change essentially mandates that a qualification process be developed to ensure that the Cyber Workforce pipeline delivers personnel to the operational IA community who are capable of *sitting the position* on day one. Cyber exercises that stimulate interest in IA and evaluate practical capabilities are an important element of the qualification process. Below are a few examples of such cyber exercise related activities.

Cyber Patriot

Cyber Patriot is the premier national high school cyber defense competition that is designed to give hands on exposure to the foundations of cyber security. Cyber Patriot is not a hacking competition. Cyber Patriot's goal is to excite students about Science, Technology, Engineering, and Mathematics (STEM) education.

Cyber Aces

The Cyber Aces foundation achieves its mission by offering challenging and realistic cyber security competitions, training camps, and educational initiatives through which high school, college students, and young professionals develop the practical skills needed to excel as cyber security practitioners and to become highly valued citizen-technologists.

Collegiate Cyber Defense Competition

The largest of these exercises is the Collegiate Cyber Defense Competition (CCDC). CCDC is a three day event and the first competition that specifically focuses on the operational aspect of managing and protecting an existing commercial network infrastructure. CCDC provides a unique opportunity for students and industry professionals to interact and discuss many of the security and operational challenges the students will soon face as they enter the job market. CCDC not only benefits the students involved but also the corporations as these graduates will be bringing a more experienced skill set to their jobs upon beginning their employment. CCDC also provides direct feedback for schools to exercise, reinforce, and examine their security and information technology curriculum.

Readiness

Operational readiness is the primary theme behind this discussion of an ecosystem and the DoD IA Range. The DoD IA range can leverage and build upon already existing relationships within the DoD that include extending connectivity to operational units such as the Radio and Communications Battalions, emulating components of the Marine Corps Enterprise Network (MCEN) for training purposes. In addition, readiness can be enhanced by collaboration with academia for curriculum and research as well as industry for tools and training, especially regarding industry standard certifications.

Certification

Certifications are critical qualifying criteria for the Cyber Workforce. In order to professionalize the Cyber Workforce, particularly the 2210 population of which there are approximately 7700 within Department of the Navy (DON), academia must collaborate with government and industry in order to maximize allowable advanced standing credit for commercial certifications such as those awarded by organizations such as Microsoft, CISCO, CompTIA, (ISC)2, and Global Information Assurance Certification (GIAC). As an example, the MCNOSC employs 162 2210's and the list of requisite certifications across that workforce includes most of the industry standard certifications. Close and continuous communication among the MCNOSC, NOVA, and the IA Range will ensure that the Cyber Workforce for the MCNOSC remains on the leading edge of available education, training, and readiness.

The Ecosystem For Cyber Workforce Education, Training & Readiness

The Cyber Workforce Ecosystem must consider all elements within the community of interest (COI). Evaluating this ecosystem is somewhat analogous to observing the socio-economic dynamics in any particular region. In fact, it is very similar and demonstrates the multi and cross disciplinary nature of developing a truly capable cyber workforce. Let's take the Quantico, Virginia region as an example in the sections that follow with respect to developing and sustaining a qualified cyber workforce that complies with the spirit and intent of DoD 8570.01-M. Figure 3 depicts the flow of candidates through academia into both government (MCNOSC and Marine Corps Intelligence Activity (MCIA)) and industry. In this instance, candidates flow through the community college (NOVA) and/or four year universities (GMU or UMUC). NOVA has transfer agreements with both GMU and UMUC.

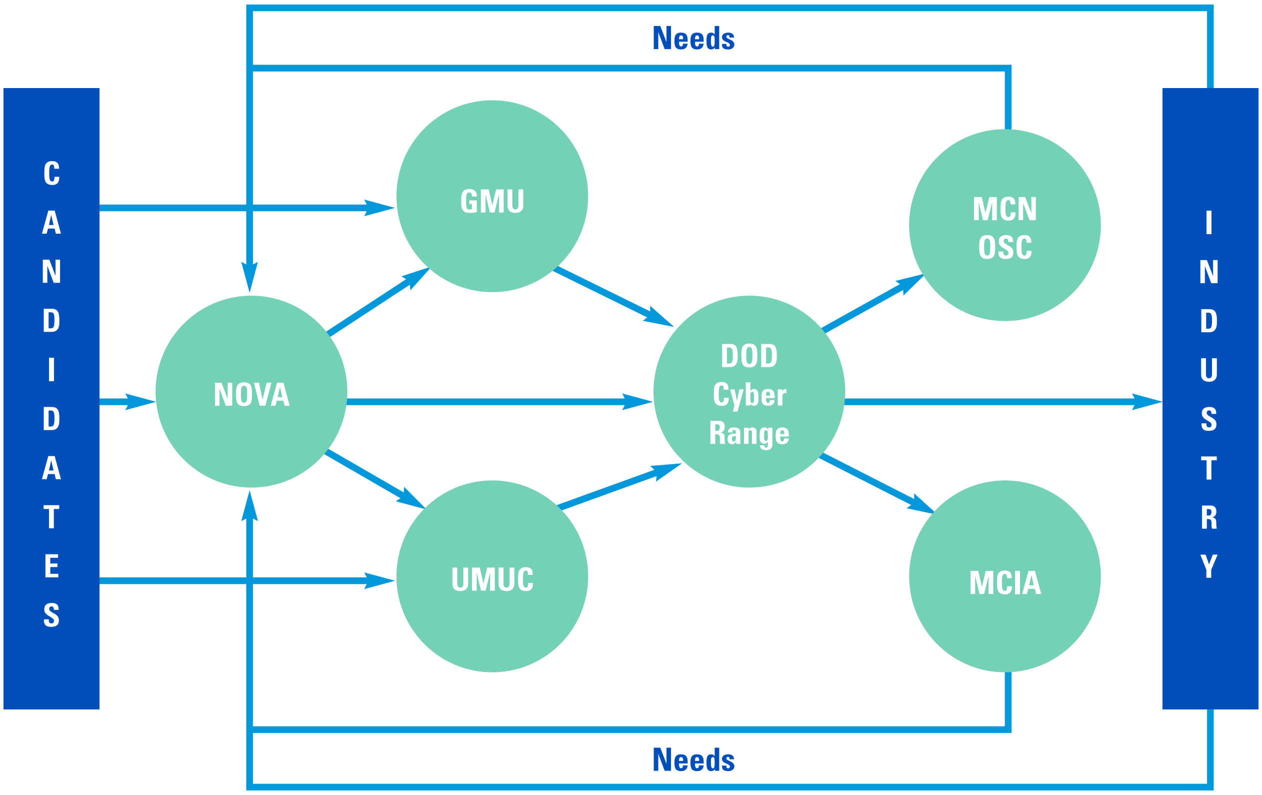

Figure 3. The Ecosystem for Cyber Workforce Education, Training, and Readiness.

Candidates

Candidates for the Cyber Workforce span a very wide spectrum indeed inclusive of all who have any interest for consideration over the long term to include veterans. In the short term, we can focus on the pipeline of Service members graduating from military formal schools during FY2013, the government civilian population having the designator of 2210, and contractor personnel. For the Marine Corps, the number of Marines expected to complete the IT Essentials course at MCCES during FY2013 is 2,683. Based on the work already accomplished by NOVA, each of these Marines will be eligible for six advanced standing credits toward an Associate of Applied Science (AAS) Degree in Information Systems Technology (IST). Although all of the courses are available online, the five Marines who reported into the MCNOSC in January 2013 also have the opportunity to enroll in NOVA and attend class at one of the six campuses located in northern Virginia.

The MCNOSC is a critical element in the ecosystem since it employs personnel representing all three sectors of the Cyber Workforce: Service personnel; government civilians; and, contractors. The mapping exercise accomplished by NOVA that defined a pathway to an AAS Degree dependent on a cyber MOS provides an opportunity for the MCNOSC to also define a similar career strategy for the 2210's and stipulate the labor category descriptions for contractor personnel. In time, this close collaboration with academia engaged with NSA regarding cyber security related curricula will provide the opportunity for organizations such as the MCNOSC to baseline their Cyber Workforce.

Needs

The most critical component of, and issue within, this ecosystem is maintenance of the relevancy of the curriculum. The effort to date has relied significantly on the communication between Headquarters Marine Corps and NOVA as well as with Department of the Navy Chief Information Officer (CIO) and Center for Information Dominance (CID). It is imperative that the needs for cyber workforce education and training be continually articulated by the headquarters advocates and, more importantly, the tactical entities responsible for cyber operations.

The need for personnel qualification can be met by leveraging the existence of the DoD IA Range. At this point in time, the DoD IA Range is utilized for aperiodic exercise activities for evaluation of cyber security competencies. It can be much more. In fact, the DoD IA Range can and should be utilized for training and formal readiness assessment of cyber security personnel. It should provision services such as emulated architectures representative of real world scenarios as well as quantitative assessment of performance. There is no such methodology in place today. Operational entities such as the MCNOSC have the need for such a capability so that they can be assured of receiving qualified personnel without impact on mission effectiveness. The essential ingredients of an Ecosystem for Cyber Workforce Education, Training, and Readiness exist proximate to Marine Corps Base, Quantico, VA.

The Department of Defense Information Assurance Range

The DoD IA Range is an existing cyber range environment funded through various initiatives within the DoD and provides, among its various missions, a safe but realistic environment for service members in the IA, or cyber, community to learn and practice their trade. The IA Range accomplishes its mission by physically and virtually representing primarily the Tier 1 architecture and services provided by the Defense Information Systems Agency (DISA). The Tier 1 network is the backbone of the Global Information Grid (GIG) and carries most DoD traffic across the globe. In some cases, lower levels of the DoD network, to include representations of Service level networks, are also represented. By replicating these networks and their associated services, the IA Range offers computer network defense (CND) operators an opportunity to get exposed to and become familiar with the tools they can expect to encounter in their respective units. The virtualized nature of the IA Range introduces many possibilities for educating the Cyber Workforce. While the following examples discuss only the DoD, the same concept applies across the whole of government, industry, and academia. Provided in the traditional crawl-walk-run format, these examples highlight two additional potential uses for the IA Range.

Crawl. The IA Range, in its current state, represents the crawl phase of training and education. In this capacity, it accurately represents a production network but is meant to be a relatively benign environment in order to allow students the opportunity to learn the basics of what threats and defenses look like. Additionally, the IA Range allows students to test their skills and expand their experiences. The use of the IA Range at this stage is the culmination of a student's formal training and from the IA Range, students are transferred out or returned to operational units where they are expected to put their newly developed skills to use. On the job training and continued education is expected at this point, but that becomes difficult because operational units do not have the resources to build and maintain training networks dedicated to cyber training and commanders rarely allow cyber training on their tactical networks for fear of impacting real world operations. This problem can be solved, however, with minimal investment by extending Point of Presence (POP) nodes to the operational units. This would allow them to connect back to both the architecture and services offered by the IA Range. Once the units have remote access to the IA Range, cyber Marines can move to the walk phase of training. The need for a continuous cyber warfare training environment at the tactical edge was articulated by 2d Radio Battalion in March 2013. Connectivity from operational units such as 2d Radio Battalion to the IA Range would enable this level of training.

Walk. More advanced than the crawl phase, the walk phase of training introduces increased complexity, realism, and consequences into the training environment. This capability, like the original IA Range, would be built as a limited network, but instead of representing the entirety of the GIG, it would only represent the actual equipment the Marines would use to create the tactical networks that the cyber Marines would be responsible for defending in real-world situations. Cyber Marines would be afforded the opportunity to understand the vulnerabilities associated with specific models of routers, switches, firewalls, and operating systems that are currently in use. Being a virtual representation of the network, there is no risk to an operational environment while still providing the opportunity to actively defend a representative version of a tactical network. To add another level of challenge to the walk phase, network attackers (for example Radio Battalion Marines) could be allowed to practice on the same network at the same time. Aside from allowing two communities (attackers and defenders) to train at the same time, this would allow each community to practice their trade against human adversaries. If a defender was required to figure out how to stop a human network attacker from gaining access to the network and if an attacker had to adjust his or her attack in response to random, human generated (vice fixed or scripted tools) defensive measures, the value of the training would increase for both sides and leads to a qualification methodology, i.e. the run phase.

Run. The run phase of training is the capstone type event for the Cyber Workforce and represents a paradigm shift for large scale exercises and operational forces operating on them. Leveraging the IA Range as the backbone of an exercise network, operational and cyber training objectives can be exercised simultaneously on a single network. Cyber effects can be experienced on the virtual version of the operational network (the exercise network), offering realistic cause and effect scenarios. For example, if an adversary successfully takes down a chat server – a common Command and Control (C2) tool – using the IA Range, that tool could truly be brought down, removing that capability from the operational picture until it can successfully be restored. This is different, and much more realistic, than the current method of announcing that the chat server is down and relying on the honor system to ensure that no one uses it. And, there are no long-term consequences to disabling the chat server because it is a virtual appliance that can be easily reset to a previous (working) state. Operators benefit from this because they get realistic indicators of an attack as well as accurate depiction of the effects of a cyber attack.

There are benefits for academia and industry as well. With access to the IA Range at all levels or phases, knowledge can be shared across the government, industry and academia. There is little doubt that one sector knows all possible attack vectors or defensive measures. Academia might by exposing a previously unknown security flaw in a networking standard or product and can test against representative networks offering real-time visibility to government operators and industry vendors. Industry, on the other hand, could benefit from seeing not only how their equipment is deployed but also how it is attacked and defended. Industry may also contribute to the defense of the network by providing information on their equipment that may only show a vulnerability when used in a certain configuration or equipment string. The IA Range provides a non-threatening way for industry, academia and government to share information beneficial to all.

Student Throughput

The essential ingredient of the process for meeting the Cyber Workforce needs is sufficient flow of candidates into the education, training, and qualification process. The Cyber Workforce is truly a community of interest (COI) comprised of active duty military Service members, government civilians, and contractor personnel. Many of those in the civilian sector are veterans. For example, the DON CIO estimates that approximately 75% of the civilian IA workforce are veterans. Due to attrition from one entity to another within this COI, it is mission critical for operational entities such as the MCNOSC to address this manpower challenge, holistically.

It is well recognized by the leadership at MCNOSC that a highly qualified cyber warrior can command a high salary in industry. As these folks are educated and trained they become even more valuable to the commercial sector, i.e. as contractors. Some will stay within the government workforce but many will not. Therefore, the Cyber Workforce Ecosystem must produce a significantly higher number of qualified personnel as the flow into the pipeline, much like the recruiting methodology, in order to maintain mission readiness and effectiveness. An engagement strategy into the middle and high schools will be very important for attracting the numbers of people that will be necessary for the Cyber Workforce. Therefore, a STEM component is a critical element within the Cyber Workforce Ecosystem and there are many leverage opportunities such as Cyber Aces and Cyber Patriot, as noted earlier in this paper.

Qualification

As was noted previously, the January 2012 revision to the DoD Directive 8570.01-M replaced the term “certification” with the term “qualification.” This fundamental change from certification to qualification should ensure that Cyber Workforce personnel are actually capable of performing the job required of them. It is incumbent upon the supporting establishment to ensure that the qualification of personnel is accomplished before they are assigned to defend our networks. Those charged with ensuring the security of operational networks should not also be required to ensure that the personnel are qualified, especially when the supporting establishment and ecosystem already exists to provide that function. Qualification needs to be the culmination of an education and training process. A network architecture emulation methodology must be instantiated so that those personnel who are educated and trained are also deemed to be qualified by rigorous assessment of their abilities. It is critical that this emulation methodology be closely linked with real world operational architectures much like simulators are used to evaluate a pilot’s ability to return to the cockpit.

Summary

The Ecosystem for Cyber Workforce Education, Training, and Readiness proximate to Marine Corps Base Quantico is representative. It can and should be replicated in such places as Augusta, Georgia and San Antonio, Texas and other locations where there is significant potential for collaboration among government, academia, and industry. It is also critical that this methodology be considered nationally in order to scale the capacity necessary to build the Cyber Workforce that this nation needs. Collaboration with Centers of Academic Excellence in Information Assurance Education, as designated by NSA, and industry leaders in cyber security training such as CompTIA and (ISC)2 will ensure that the Cyber Workforce is as prepared as possible to accomplish the mission. In addition, leveraging the existence and capabilities of such activities as the DoD IA/Cyber Range will facilitate the qualification of the Cyber Workforce. Open and continuous dialogue will ensure that the Ecosystem for Cyber Workforce Education, Training, and Readiness remains relevant to meeting the needs of government and industry.

Acknowledgements

The author would like to sincerely thank his associates and colleagues from within the triad of government, academia, and industry with whom he has collaborated over the past two years on this project. Specifically, I want to thank Mr. David Green, Lieutenant Colonel Randolph Pugh, Major Paul Keener, Ms. Paula Worthington, Dr. Margaret Leary, Mr. Brian DeMuth, and Mr. Joel Scharlat.

References

Air Force Association's Cyber Patriot National High School Cyber Defense Competition. (n.d.). *About.* Retrieved May 28, 2013 from **http://www.uscyberpatriot.org/about/Pages/default.aspx**

Cyber Aces. (n.d.). *About Us.* Retrieved May 28, 2013 from **http://www.cyberaces.org/aboutus.html**

Cyber Watch. (n.d.). *About Cyber Watch.* Retrieved April 14, 2013 from **http://www.cyberwatchcenter.com/index.php?option=com_content&view=article&id=50&Itemid=29**

DeMuth, B. and Scharlat, J. (June 2013). Modeling and Simulation of Cyber Effects in a Degraded Environment. *International Test and Evaluation Association Journal,* (pp. 164-167).

Department of Defense Directive 8570.01. (2007). *Information Assurance Training, Certification, and Workforce Management.* Washington, DC.

Department of Defense Manual 8570.01-M. (2012). *Information Assurance Workforce Improvement Program.* Washington, DC.

Hinckley, G. (January 2013). *Cyber Workforce Education Initiative.* ABET Inc., Stafford, VA.

Marine Corps Communications-Electronics School. (2009). *MOS Roadmap: 0651-0659-0699; Data Network Specialist; Data Chief; Communications Chief.* Twentynine Palms, CA.

Marine Corps Order 5311.1D. (2010). *Manpower and Reserve Affairs Personnel Availability Digest.* Washington, DC.

National Collegiate Cyber Defense Competition. (n.d.). *About.* Retrieved June 23, 2013 from **http://www.nationalccdc.org/index.php?option=com_content&view=article&id=46&Itemid=27**

National Institute of Standards and Technology. (August 2011). National Initiative for Cybersecurity Education Strategic Plan. Washington, DC. Retrieved April 14, 2013 from **http://csrc.nist.gov/nice/documents/nicestratplan/Draft_NICE-Strategic-Plan_Aug2011.pdf**

Pugh, R. (December 2012). *"On Duty" Education Information Paper.* 2d Radio Battalion, Camp Lejeune, NC.

Pugh, R. (March 2013). *Continuous Cyber/Electronic Warfare Training Environment at the Tactical Edge (C2T2).* 2d Radio Battalion, Camp Lejeune, NC.

Secretary of the Navy Instruction 1543.2. (2012). *Cyberspace/Information Technology Workforce Continuous Learning*. Washington, DC.

Worthington, P. (2012, October). *Advanced Standing between Northern Virginia Community College and United States Marine Corps*. Northern Virginia Community College, Annandale, VA.