CYBER BEACON 2014

Cyber Workforce Development, Education and Training Workshop

National Defense University
Fort Lesley J. McNair, Washington, DC
15-16 July 2014

Workshop Report

COL Jon Brickey, USA
Army Cyber Institute

CDR David Di Tallo, USN
NDU/iCollege

CYBER BEACON was inaugurated in July 2013 by National Defense University's Information Resources Management College (iCollege), bringing together senior cyber thought leaders from the Department of Defense (DoD) and around the world to discuss what then-Chancellor Robert Childs described as the "Cyber Beacon of Leadership."

For 2014, iCollege partnered with the Army Cyber Institute (ACI) at West Point to enjoin the private sector, DoD, academia, and the think-tank community to discuss cyber leader development, education, and training. CYBER BEACON 2014 began with two plenary session panels and concluded with a pair of workshops. All presentations and subsequent discussions were held on a not-for-attribution basis, to encourage frank and open dialogue. Therefore, this report summarizes the main thoughts and ideas expressed during the event, while not attributing them to specific individuals or organizations.

CYBER BEACON 2014 was made possible through the partnership and efforts of ICollege and ACI, with generous financial support from the NDU Foundation.

Executive Summary

The Army Cyber Institute and the National Defense University's (NDU's) iCollege co-sponsored a Cyber Workforce Development Education & Training Workshop at Fort McNair, 15-16 July. The goal was to bring together stakeholders for cyber education and training to provide situational awareness on current programs, identify gaps, and map out desired end states.

LTG Edward Cardon, Commander, U.S. Army Cyber Command, provided opening remarks and set the stage for the workshop, which consisted of four main sessions: 1) Strategic Requirements for the Cyber Workforce; 2) Operational Requirements for Cyber Leader Development, Training, and Education; 3) Breakout panels on Cyber Training and Education; and 4) a focus session on potential solutions.

Since competence rules in cyberspace, the Department of Defense (DoD) must normalize cyber competencies through thoughtful design of workforce development, education, and training. It must also move beyond rash personnel actions where training and education are not defined prior to an assignment in operational organizations. Finally, the essential education and training requirements must be known in advance to align the workforce with critical cyber positions.

The rapidly changing nature of technology makes cyber workforce development, education, and training difficult. Some specialty areas, like big data analytics, are extremely low-density fields that develop quickly and provide important capabilities, but create skill-set needs that are difficult to anticipate. Even major Internet companies, like Google, find it difficult to predict what cyberspace will look like in five years. Therefore, the cyber workforce has to be educated to deal with uncertainty and trained to deal with the most current tactics, techniques, and procedures in order to operate in the competitive cyber domain. Cyber warriors must periodically rotate between these three states: educate, train, and operate.

Workshop Takeaways

Overall, participant feedback indicated that the most valuable aspect of the workshop was the networking opportunity—there were over 40 representatives from all of the Services, Joint Staff, DoD agencies, academia and private industry.

Participants generally agreed that, while there may be adequate coordination and collaboration across the U.S. Cyber Command (CYBERCOM) and its Service *components*, there does not seem to be enough across the Service cyber *proponents* (e.g. U.S. Army Cyber Center of Excellence (CCOE), U.S. Fleet Cyber Command (FLTCYBERCOM, etc.). Many felt the Joint Staff to be the appropriate focal point to ensure consistent cyber workforce development, education, and training requirements for the Joint Force and overall coordination with the Services and DoD.

Most agreed that 80% of cyber workforce development, education, and training should be a joint or common endeavor. Further, in resource constrained environment, the Services should divide the requirements among them and then develop, educate, and train across the Services to satisfy the Joint Force's needs. Additionally, each Service still needs to provide its own unique cyber workforce development, education, and training to address inherent differences in service platforms, networks, and operations, which participants estimated would make up the final 20% of the total DoD effort.

Finally, many participants stressed the need for DoD to leverage the Reserve Component more in the cyber domain because reserve personnel are often already employed in civilian cyberspace-related industries, which are more agile and advanced in many ways than DoD. However, participants noted that there seems to be no single repository of this expertise, so concluded perhaps there should be a single

Service or DoD-wide office (point of contact) to track these human capital assets and leverage potential opportunities.

Joint Cyber Education and Training (JCET) Network (NET)

The Joint Cyber Education and Training (JCET) Network (NET) is composed of members from all Services, who are responsible for developing and delivering cyber workforce development, education, training, and orientation. The purpose JCET NET is to bring together all cyber education, training, and orientation courses under a collaborative, unifying strategy that enables the development and presentation of a seamless continuum of cyber education, training, and orientation for all ranks. For more information, visit: https://www.milsuite.mil/book/groups/jcetnet.

Table of Contents

Session 1:	**Strategic Requirements**	**Page 6**
Session 2:	**Operational Requirements**	**Page 8**
Session 3:	**Cyber Training and Education Focus Panels**	**Page 11**
Session 4:	**Workshop Discussions**	**Page 12**
Annex A:	**Cyber Training and Education Focus Panel Slides**	**Page 14**
Annex B:	**Workshop Discussion Slides**	**Page 22**
Annex C:	**Cyber Education & Training Career Progression**	**Page 32**
Annex D:	**Opportunities for Education & Training**	**Page 34**
Annex E:	**Additional Resources**	**Page 40**

Session 1: Strategic Requirements for the Cyber Workforce

Panelists:

- Mr. Anthony Packard, National Security Agency (ADET)
- Mr. David Still, Defense Information Systems Agency
- CAPT John Moore, USN, Joint Staff (J7)
- Maj Ben Leming, USMC, USCYBERCOM (J7)

Guiding Questions for Session One:

- Where are we now?
- Where do we want to be in the future?
- What department or agency specific needs do we have?

Discussion:

"We're going to need a bigger boat!" That modified quotation from the movie *Jaws* summed up the realization many participants felt, namely that DoD is facing a huge challenge and needs to quickly ramp-up the people, processes, and technology necessary to successfully operate in cyberspace. Since every organization needs more resources for growing the cyber workforce, participants agreed it was imperative to collaborate across departments, agencies, and Services to combine resources when possible. Moreover, they concluded that many cyber workforce initiatives need stable funding and a qualified staff to ensure success in the future.

While many participants noted there is no single executive authority for cyber workforce development, education, and training, they did observe that DoD was already on a good path to achieve commonality across the department, agencies, and Services. Participants estimated that 80% of the development, education, and training curricula are common, with the remaining 20% differentiated to meet unique needs. Many praised recent activities for cyber across DoD, including two examples: 1) the Deputy Secretary of Defense signed DoD's Cyber Workforce Strategy (CWFS) in December of 2013, and 2) there is a weekly telephone conference among principals that focuses on refining the various cyber work roles.

Yet participants felt that DoD still lacks the authority to implement cyber workforce development, education, and training across the department in a holistic manner. For example, some noted there was a conceptual framework for a "Defense Cyber University," but it never materialized. Still others asked, "where is DoD's school for advanced cyber studies—to develop strategic leaders—and where are our weapons schools—to develop our 'Top Guns' in cyberspace?"

Participants generally agreed there are some gaps in cyber workforce development, education, and training across DoD. While there are a number of websites and catalogues, DoD does not have a single repository the workforce can reference. Some participants also observed that, while there are a great deal of cyber education and training resources in the private sector to leverage (which have the added benefit, in some cases, of offering formal certifications), there is a point at which DoD cannot outsource the curricula for specific mission requirements. Also, some felt it is important to offer education and training in the forms that match the learning styles of the workforce, whether face-to-face or online.

The Cyber Mission Force (CMF) pipeline is documented and understood, though it can be long. The current manning models are insufficient because for an individual's typical 4-year tour, units only get 2.5-years of operating time—the rest is needed for training and education (though mostly training).

With respect to the panel itself, participants learned a great deal about cyber workforce development, education, and training initiatives across a wide swath of DoD:

- CYBERCOM develops the Joint Cyberspace Training Standards (JCTS), a seminal work developed through rigorous methodology, that describes the cyber workforce and the cyber-related activities they perform and which serves as the cornerstone for the DoD 8140 manuals (which succeed the previous 8540 series). Defense Information Systems Agency (DISA) used the Knowledge, Skills, and Attributes (KSA's) from the JCTS to map to their work roles. As DISA performed this before the NICE Framework was in place, CYBERCOM is currently updating the KSAs and DISA will adjust once complete.

  Additionally, CYBERCOM provides cyber workforce training for its headquarters staff, subordinate commands, and others across DoD and the Services (resources permitting), through its Joint Advanced Cyber Warfare Course (JACWC) six times a year. PACOM has a similar course for its Area of Operations (AOR). CYBERCOM sees the need for the Services to develop and offer their own JACWC-like courses, perhaps geographically aligned with Joint Force Headquarters-Cyber in Texas and Georgia. Finally, CYBERCOM provides the Joint Qualification Records (JQRs) for the CMFs and supports three Tier 1 cyber exercises annually: CYBER FLAG, CYBER GUARD, and CYBER KNIFE.

- The Joint Staff maintains the Joint Cyber Range environment (architectures/infrastructures) to support the CMF's, COCOM's, Services, and DoD agencies. (OT&E runs the National Cyber Range.) There are approximately 80 nodes to the range and that number is growing. The Cyber Investment Management Board provides governance for the cyber range. We are probably 3-5 years out from being able to provide virtual environments on demand to support ranges.

- NSA's Associate Directorate for Education and Training (ADET) is expanding its Cyber Assessment and Recommended Training (CART) tool to identify training strengths and weaknesses and to develop individualized training programs. This could be extremely useful if combined with DISA's workforce training program and tools (found at "iase.disa.mil").

- DISA recently coded its entire workforce using a criterion similar to the NICE Framework and concluded that two-thirds, nearly 6,000 employees, are in cyber roles. The agency contends it is important to address training requirements for the entire workforce, not just the Service members. Further, there is a need to share requirements for work roles and not simply duplicate the DoD 8140 manuals. With respect to specific training, DISA provides in-house training opportunities for its employees and mission partners (e.g. COCOMs), but training for some of the low density work roles is outsourced. Moreover, anyone can access role-based online training at "iase.disa.mil" and request training syllabi from DISA.

Session 2: Operational Requirements for Cyber Workforce Development, Education, and Training

Panelists:

- Maj Ben Leming, USMC, USCYBERCOM (J7)
- COL Martha VanDriel, USA, Army Cyber Command (G7)
- LCDR Eduardo Salazar, USN, Fleet Cyber Command (N3)
- Lt. Col. David Canady, USAF, Air Force Staff
- Mr. Mark Bachrach, Marine Corps Cyber Command

Guiding Questions for Session Two

- Where are we now? Where do we want to be in the future?
- What service or command specific needs do we have?
- What should be common or joint?
- Are the strategic requirements right?

Discussion:

Panelists and participants generally agreed that the operations requirements for the cyber workforce vary on the roles the workforce plays. Three distinct roles were identified:

1. Cyber professionals;
2. Crossover professionals;
3. Others/non-cyber.

Cyber professionals

The cyber workforce accession and training pipeline is a fragile ecosystem. DoD has to properly assess cyber skills and minimize washout rates. This requires effective and efficient processes—interviews, tests, training, etc. DoD may wish to adopt a system similar to the Defense Language Institute in which staff identify individual learning styles and match with training programs. DoD is increasingly looking for individuals with a STEM background; however, there is also a need for non-STEM specialties. For example, the Air Force is increasing the number of cyber professionals with a STEM background from 50% to 70%. The Navy, however, mentioned the need to have Behavioral Scientists integrated into cyberspace operations.

Since the training timeline can often take 12 or more months and tens of thousands of dollars per individual, there is little room for slack/re-training. Participants identified the need for "bilingual operators"–those who understand offensive and defensive operations in cyberspace.

Crossover professionals

Some work roles require a broader understanding of cyberspace operations but without the detailed technical knowledge required by those who perform day-to-day network operations (i.e. "keyboard operators"). Some examples include operational cyber planners, attorneys, and intelligence officers.

Participants felt we currently lack operational planners with cyber knowledge because few understand how to incorporate cyberspace operations into COCOM plans. There are two ways to solve this problem: first, take current operational planners and make them "cyber planners", or, second, make cyber professionals operational planners. One impediment to the former may be security clearances, since

TS/SCI is often the minimum clearance level to work in the cyber domain due to links to intelligence platforms and processes. Also, it may be necessary for newly-minted "cyber planners" to have a basic understanding in signals intelligence (SIGINT) in order to follow some of the conversations in cyber plans and operations.

Others/non-cyber

Even those workforce members not directly involved in cyberspace operations require a certain level of education or training to succeed in the cyber arena. Some compare a standard desktop computer or laptop to a weapon system that requires training and certification. For example, every Soldier has to qualify on his or her personal weapon, while every driver has to complete driver's training. Therefore, why should we require less for an information system, especially given the risk? Taken one step further, all DoD employees should have increased cybersecurity awareness and practices that extend into their personal lives (this is an ideal goal for all computer users, not just those in the DoD.)

There was considerable discussion about how the Services have approached their Title 10 responsibilities for the cyber workforce. Some similarities/differences and service challenges include:

- The Navy does not have a cyber branch, though it has an Information Dominance Corps that includes several of the Intelligence and Information Technology specialties. The constant rotation between ship and shore duty causes tension in the training timeline and the ability to specialize.
- Signal and Intelligence specialties comprise the Army cyber workforce today. The Army does not currently have a cyber branch, though it may announce a new branch in October 2014.
- The Air Force has a cyberspace specialty—the 33 series—that consists of two communities: intelligence and communications. Some believe the Air Force prematurely fused the two communities together, despite clear differences in cultures and KSAs. (For more detail, see AFCEA article, "Failing of Air Force Cyber," http://www.afcea.org/content/?q=node/11855).
- The Air Force recently re-wrote the officer cyber branch system and is reviewing the enlisted structure. Now, they are focusing on civilian billets for the cyber workforce. They have dedicated cyber career managers for Airmen.
- The Air Force career field for cyberspace operator (1B4) has grown by 100% the past few years.
- The Marine Corps does not have a cyber branch.
- The Army and the Air Force are both wrestling with the challenge to integrate cyber expertise at the tactical echelon. (This goes back to the discussion of classification and the dependence on intelligence platforms/agencies.)
- There are some business processes across the DoD that rely on information systems; however, they are not operational processes. These may require different members of the cyber workforce.

Service	Operational Cyber HQ	Cyber Proponent HQ
Army	Army Cyber Command & Second Army	Cyber Center of Excellence, Training and Doctrine Command
Navy	U.S. TENTH Fleet	Fleet Cyber Command
Air Force	Air Force Cyber Command	24th Air Force
Marine	Marine Corps Cyber Command	Headquarters, U.S. Marine Corps

Several participants mentioned that the Service academic institutions seem to be doing great things for cyber education. That may be fine for the officers graduating from such institutions, but more needs to be done to leverage them for the benefit of the rest of the Services' personnel base. Participants wondered how do we leverage the Service academies for their expertise to inform cyberspace operations across DoD?

- The US Naval Academy offers a Cyber Operations major and two core courses for all midshipmen. The USNA has a new Center for Cyber Security Studies (http://www.usna.edu/Cyber/index.php)
- The US Military Academy is one of 13 academic institutions recognized by the NSA as a Center of Academic Excellence for Cyber Operations for the 2014-2019 academic years. It is home to the new Army Cyber Institute (http://www.westpoint.edu/acc/SitePages/Home.aspx)
- The Air Force Institute of Technology (AFIT) offers cyber training and education. The AF is currently revising its series of training courses: Cyber 200/300 (AFIT) and Cyber 400 (NDU). One of the challenges is delineating business and operational processes while fusing the CIO/A6 (Communications/Architectures) concerns with the A3 (Operations) focus.
- The Naval Postgraduate School has a number of cyber education programs, including a Master's degree focused on cyber systems and operations.

Panels 3A/B: Cyber Training (A) and Education (B) Focus Breakout Sessions

Panelists: N/A

(Note: attendees were split into two, roughly equal groups; some gave prepared remarks based on the guiding questions, while others presented their respective opinions or, informally, those of their unit.)

Guiding Questions for Panel 3

- What are the desired attributes of a cyber leader?
- What is a typical cyber leader career path?
- What career milestones require cyber training/education?
- What cyber training/education is currently available?
- What are sources of cyber training/education requirements?

Discussion:

Panels 3A (Cyber Training) and 3B (Cyber Education) were charged with answering key questions in the education and training of cyber leaders. Participants were asked to focus solely on either training or education to help bound the problem.

In both panels, some similarities were evident, namely the need for cyber leaders to first be leaders, in the traditional sense of the term. Just as in traditional career fields, participants generally agreed that cyber leaders will be expected to grow from being technically competent, to tactically proficient, and finally to being strategically focused. Therefore, the desired attributes of cyber leaders would be those of leaders in general, in addition to having the technical competency to lead cyber operations at the tactical, operational, and strategic levels or war.

When it came to a discussion of typical cyber career paths and the corresponding milestones requiring cyber training and education, participants indicated there was no definitive model as of yet. Most agreed that the education and training for junior cyber personnel (junior enlisted, junior commissioned officer, and junior civilian) was well established, at least at the early points, as it tended to focus on the technical and tactical aspects of their work. For them, the concern seemed to be about how to mix cyber and non-cyber assignments throughout a total career, which Service-specific milestones might affect.

At the highest levels of cyber leadership, participant also noted no typical career path, as the Services are, in some cases, appointing non-cyber leaders to key cyber positions. Indeed, in some cases, senior cyber leaders have grown up in completely unrelated fields. Participants felt that, in these cases, some level of "cyber awareness" or "cyber appreciation" was needed, but, as senior leaders, their true role was in strategic decision making.

Participants generally felt that as the cyber field itself matured, the corresponding career paths of its leaders would naturally flesh itself out. Until them, however, participants noted that the current mish mash of Service-specific and DoD-wide workforce guidance would continue.

See Appendix **A** for briefing slides each Panel presented in plenary session.

Session 4: Workshop Discussions

Panelists: N/A

(Note: attendees randomly split into two, roughly equal groups and addressed the guiding questions; prepared remarks were not solicited or given.)

Guiding Questions:

- What are the relevant strategic and operational education and training requirements?
- What gaps exist between those requirements and what is currently being done?
- What opportunities exist for reconciling them?
- How can we leverage industry and academia?
- How can we communicate better with cyber stakeholders?

Discussion:

During the workshop discussions, it was difficult to focus on any one piece of the cyber workforce development, education, and training "elephant." One participant suggested discerning the different audiences by career fields—"cyber" versus "non-cyber"—and comparing the current state with the expected or desired future state. Figure C-1 in Appendix C was one participant's attempt to show development, education, and training throughout a generic commissioned military officer career. Others noted the similarities between this and a proposed Cyber Branch milestone diagram developed by the Army Cyber Institute. (See page C3.)

Participants observed that service members with cyber-related skills—e.g. intelligence analysts or information system operators—transition from purely basic branch positions into newly designated cyber positions. At that point, they then focus on the unique cyber aspects of their job and (ideally) receive specialized training prior to cyber assignments. For those in senior ranks, some orientation courses and briefings are available to get up to speed. However, it is important to remember that they enter a cyber-related position from all walks of military life—artillery, infantry, engineer, etc.—though most come from an intelligence background. As participants found, there is no standard cyber workforce development, education, and training in existing career tracks, so, unless the newly-minted cyber professional has a personal or professional background in electronic warfare, information technology, or other cyber-related topics, they will likely have no knowledge of cyberspace operations.

Participants generally agreed that, in the future, every Service member must receive some standardized cyber workforce development, education and training at key milestones throughout their careers, from their entry level training through senior service college and into the general officer/flag officer/senior executive level. Some went further, expressing the need for a DoD-wide culture shift based on the Marine axiom "every Marine is a rifleman", extending this to cyber with "every service member is a cyber-defender." Along the same lines, there is the belief that DoD information systems are weapon systems, and as such, require rigorous qualification standards similar to those required for individual and crew weapons, e.g. machine guns, missile systems, tanks, and aircraft. Ultimately, this will require a culture shift across the entire Defense Department, from senior defense leaders on down, and must be injected in every learning, training, and education milestone.

Going back to Figure C-1, professionals in cyber career fields will get a full dose of cyber-specific education and/or training upon their accession, and, throughout their careers they will receive additional workforce development, education, and special training as they conduct actual cyberspace operations.

Participants agreed this would be a constantly repeating cycle--educate, train, operate--with a focus on training and operating.

See **Appendix B** for briefing slides that each Workshop presented in the final plenary session.

Appendix A
Cyber Training and Education Focus Session Slides

UNCLASSIFIED

NATIONAL DEFENSE UNIVERSITY

CYBER BEACON 2014

Panel 3A: Cyber Training Focus

Panel 3B: Cyber Education Focus

15 July 2014

Imagine, Create, and Secure a Stronger Peace...

UNCLASSIFIED

UNCLASSIFIED

CYBER BEACON 2014

Discussion Points

- What are the desired attributes of a cyber leader?
- What is a typical cyber leader career path?
- What career milestones require cyber training/education?
- What cyber training/education is currently available?
- What are sources of cyber training/education requirements?

Imagine, Create, and Secure a Stronger Peace... 1

UNCLASSIFIED

UNCLASSIFIED

CYBER BEACON 2014

What are the desired attributes of a cyber leader?

- Competent, understands and speaks the cyber language.
- Cyber-Domain in the maneuver space, we want our senior leaders to come from a technical background. We don't want to take an Army General and put him/her in an Air Force leadership role, we don't want to do the same with our Cyber-Generals.
- Would we only select those people who went through the Cyber Milestones?
- "Integrational" effects need to be understood.
- Below the field grade level you could take those who understand planning and integrate them into the Cyber-domain.
- Not to just be able to think strategically, but to be able to effectively communicate across channels. Cyber-speak.
- For the Navy at the E-7 Level and above, yes, professionals are technically proficient. Looking forward, do we want our Cyber-Generals to be technically proficient?

UNCLASSIFIED

UNCLASSIFIED

CYBER BEACON 2014

What are the desired attributes of a cyber leader?

- Strategic level focused (iCollege) (Chairman's DLA – instruments of national power)
- CIO is a cyber leader
- AF Cyber 400 course designed to know the culture and the issues facing – leaders need to know how to think to drive the organization…
- Getting people to conduct the mission and understanding threats, mitigating risk
- Educating on different aspects of Cyber (information, communication, technology) – understanding specific definitions
- Focusing on the Conduct of operations
  - Attack and exploit
  - Offense and Defense (JP 3-12)
  - Warfighting functions

UNCLASSIFIED

CYBER BEACON 2014

What are the desired attributes of a cyber leader?

- Respond immediately based upon threat and must understand all across government
  - Understand authorities
  - Understand the big picture and when to apply particular operations to actively defend
  - Understand the players, stakeholders, relationships
- Understand human element
  - Individual user (and how to communicate)
- Clear understanding of what a cyber leader really is
- Chess master

CYBER BEACON 2014

What is a typical cyber leader career path?

- Combat leader
  - AWC with cyber integration
- Apprentice, Journeyman, Master (military perspective – Army)
  - Tactical, operational to Strategic
  - Providing services
  - Security efforts
- No particular path (many with different backgrounds)
  - All use technology that drives mission
  - Business skill, planning, risk management, budget
- Successful leader first with cyber skills added
- Growing leaders within the cyber domain – so they have broadening experiences

CYBER BEACON 2014

What is a typical cyber leader career path?

- Depends on community and what service we are talking about.
- Cyber-Leaders will need the same attributes of leadership as any other community.
- Timeframe? There is a deficit of Cyber-leaders who have not had the career path yet. Future Cyber-leaders will be **us** in the future. How do we get a grunt or aviator leader to get smart on being a new Cyber-leader? Not too much technical things that they need to understand. They need to get smart on their new cyber world in order to understand the language.
- 22 or 23 year old Cyber-Gurus may not be developed enough to be key leaders yet? The army has to come to grips that they may not be able to have both. Perhaps a cultural difference. Will you always be a leader wherever you go? Possibility of not being promoted to 1-Star because you are a cyber-guru. I MEF can be commanded by a grunt or aviator, could it be commanded by an officer with a Cyber career path?
- There is always leadership and experience that everyone brings to the table. Very technically and tactically proficient people who have pre-requisite knowledge that make them good leaders.

UNCLASSIFIED

CYBER BEACON 2014

What is a typical cyber leader career path?

- Army has their vision or perhaps a draft of what leadership will look like. What will projected career path in Cyber look like? The other 3 Services have not created a niche in Cyber yet. Different paradigm for Army, forcing people into a specific career path. This is something new.
- Air Force has a career path with some operational squadrons. Cyber Operations groups = O-6 billets. There are no real senior level billets for Cyber-operators.
- Hope there is a sharing of development of Cyber operators between the services.
- Argument that Cyber-operators should stay in Cyber Ops in order to maintain proficiency. Highly perishable skill.

CYBER BEACON 2014

What is a typical cyber leader career path?

- Concern that LTs will spend so much time doing Cyber Ops; that they will miss opportunities to develop leadership skills. May already be going away from that in the Army. Army is trying to split the difference. Small LT population will come in with specialized skills. Those officers who have a STEM degree who decide to go Infantry or Armor, will have a warfighting understanding, and will have a propensity for understanding leadership.

CYBER BEACON 2014

What career milestones require cyber training?

Panel 3A: Cyber Training Focus

- Anybody on the Cyber-Mission teams. In the different services, can you be on the CPT as an O-1 or O-2? If you want to develop leaders, do you put them into a technical job or give them more leadership responsibilities? Most Lt's are out in the Fleet. Most Team Leads are SIGINT or COMMS. First go out to the fleet and work operationally.
- What would be designation for the position? Command? Brigade command? What do our Brigades do in Cyber? Across the force, not just the Cyber-Force. All units should have some sort of Cyber training.
- Senior Service College report. War colleges are really bad when it comes to Cyber education. Cyber training could/should be part of the core. Not enough and not quality enough when it comes to Cyber at the Senior Service level.
- We are essentially now Cyber-dependent and not just Cyber-enabled in today's military.

CYBER BEACON 2014

What career milestones require cyber training?

Panel 3A: Cyber Training Focus

- War colleges have all been in touch with the J-7.
- Navy Information Warfare community, personnel that have done tactical SIGNIT, and become Cyber Team Leads maybe.
- Enlisted are the technical personnel, Officers will need to understand their jobs but not know about all technical aspects.
- Enlisted and Warrant Officers on leadership training. CPT leads?

CYBER BEACON 2014

What career milestones require cyber training and education?

- Continuous/refresher: should be ingrained within military courses at the most basic level just as maintenance of a vehicle
- Existing career courses should include cyber (in progress but needs to be expedited) (Army and Air Force)
- -- Where do we need to add the cyber-training? IDC? Cyber Center of Excellence? Mapping out the MOS's to the training. Air Force, undergraduate Cyber-Training. Cyber 200, 300, 400 will help those leaders get to the next level of understanding.
- Assignment to unit with cyber missions; education/orientation prior to assignment to COCOMs with additional relevant training/orientation at the unit

CYBER BEACON 2014

What cyber training is currently available? Where?

1. ADET (Primary source of Information)
2. Professional Education Center (National Guard)
3. Vermont Regional Training Institute
4. USCYBERCOM
5. 39th IOS (Hurlburt Field)
6. DISA IASE (List of Training Repositories) – DL via Website
7. FED Virtual Training Environment (DOS) – DL via Website
8. 229th IOS (Vermont)
9. 1st IO Command
10. UMBC
11. NDU iCollege
12. Ft. McCoy USAR
13. AFWIC (Nellis)
14. Cyber COE
15. DCITA (Defense Cyber Investigation Training Academy)
16. Skillport
17. National Intelligence University (NIU)

UNCLASSIFIED

CYBER BEACON 2014

What cyber education is currently available? Where?

- Civilian Universities, especially at NSA (Centers of Academic Excellence)
- NDU's iCollege – MS and education in context
- DAU: Cyber security with focus on acquisition
- Carnegie Mellon – offer technical education
- Information Assurance, cyber security tailored in a doctorate (BS, MS, PhD) – Capitol College
- U.S. Cyber – JACWC (orientation)
- 1st IO Command – courses for GS14 and above
- NPS, NSA, DHS, AFIT (MS, PhD – enlisted to officers, and WO)
- AWC – 3 hour course, elective program, distance education more robust
- PEC – University of Arkansas at Little Rock

CYBER BEACON 2014

What are sources of cyber training requirements?

Panel 3A: Cyber Training Focus

- NDU:
  - Clinger-Cohen Act
  - DOD CIO
  - CIO Council
  - FISMA 2002
- Services:
  - Cyber Center of Excellence:
    - Operational Force
    - Doctrine
    - Laws/Executive Orders
    - Service Chief
  - ADET:
    - COMUSCYBERCOM
    - NSA Director

CYBER BEACON 2014

What are sources of cyber education requirements?

Panel 3B: Cyber Education Focus

- Joint Staff (iCollege)
- CIO/CFO (iCollege)
- NDU-P (iCollege)
- Faculty led (iCollege – capabilities)
- Students' feedback (iCollege) (Capabilities)

Appendix B
Workshop Slides

UNCLASSIFIED

NATIONAL DEFENSE UNIVERSITY

CYBER BEACON 2014

Workshop 1
Workshop 2

July 16, 2014

UNCLASSIFIED

Discussion Questions

- What are the relevant strategic and operational education and training requirements?
- What gaps exist between those requirements and what is currently being done?
- What opportunities exist for reconciling them?
- How can we leverage industry and academia?
- How can we communicate better with cyber stakeholders?

CYBER BEACON 2014

What are the relevant strategic and operational education and training requirements?

Workshop 1

- Education
  - Master's or equivalent opportunities expected. (Cyberspace, CS, IT)
  - Collection of courses (Framework)
  - Brilliant Young/Brilliant Old People
  - Basic Fundamentals Awareness
  - General Users versus Technical Specialists
  - Leadership versus technical skill?
  - Appropriate Value – Timing,
  - Gap in leaders understanding of Cyberspace

CYBER BEACON 2014

What are the relevant strategic and operational education and training requirements?

Workshop 1 (continued)

- Training
  - SCADA
  - 8570 Requirements
  - NICE/JCTCS
- Operational Impacts
  - Pilot Analogy / Doctor Analogy
  - Special Ops Analogy
  - Enlisted versus Officer
  - Culture differences
  - Policy/rules versus operational impact

UNCLASSIFIED

CYBER BEACON 2014

What are the relevant strategic and operational education and training requirements?

Workshop 2 (continued)

- What are the operational requirements vs other requirements, i.e. personnel
  - Role based training requirements (training and personnel development)
  - Requirement of billet vs. what a person really must do
  - Work roles match ASIs
  - Work roles must specifically identify skill set
  - Math, science, social sciences skill set may be the base of what we need to build upon
  - What we don't have - Standardized set of courses for leaders who have no background in cyber who will lead in a cyber position
- All domains must understand impacts of cyber domain

UNCLASSIFIED

UNCLASSIFIED

CYBER BEACON 2014

What are the relevant strategic and operational education and training requirements?

Workshop 2

- (3 levels) Professionals, decision makers, practitioners
- Uniformity within competencies
- Orientation within leadership (mid to senior) and identifying gaps
- Non-supervisor, supervisor, management, senior-management, executive (5 levels)
- Identify mission set (end product) at various levels (K,S,As for groups)
- Understand different services' requirements for cyber leadership

UNCLASSIFIED

UNCLASSIFIED

CYBER BEACON 2014

What are the relevant strategic and operational education and training requirements?

Workshop 2 (continued)

- How do we employ the skills sets at the tactical, operational, and strategic level?
- How do these leaders employ teams (who understand effects) at the operational level?
- How do we make our leaders "cyber smart"
- Information Operations (IO) Officers must have knowledge of non-kinetic tools and be able to inform senior leaders of cyber operations
  - No uniformity across the services of what the IO does
  - USAF has cyber expert within operation cell to advise operations officer (part of MDMP)
  - Army developing CEMA (similar to what the AF has)
- Able to deal with the unknown so must have the ability to adapt, have flexibility

UNCLASSIFIED

UNCLASSIFIED

CYBER BEACON 2014

What gaps exist between those requirements and what is currently being done?

Workshop 1

- Vague
- Gap? No funding? Lack of perspective? Unified Command?
- Laws and policies
- A lot being offered, but not managed or organized.
- Training – we are figuring it out, for Education requirements – still unclear.
- How do we teach them the value of Cyberspace?
- Training vs Education
- Make the examples in the current training more realistic and relevant; make the training more operationally oriented
- 1 and 0's translated to the physical world.
- Goal oriented training
- Rewards?
- Cost Benefit Analysis/Risk?
- Continual/Sustained Education vs only annual requirements – Proactive vs Reactive

UNCLASSIFIED

CYBER BEACON 2014

What gaps exist between those requirements and what is currently being done?

Workshop 2

- Recommendation - A study (military and private) what works well and what doesn't (knowledge, capabilities) – are they relevant to what we are trying to build
- Speed education lifecycle – to maintain relevancy, time dependency
- Technical field that requires social sciences (social sciences is part of this technological field)
- Cyber immigrants are in charge of decision making and must have cyber knowledge
- Gaps in requirements themselves – system isn't designed to identify those needs as we need them, more ad-hoc

UNCLASSIFIED

CYBER BEACON 2014

What gaps exist between those requirements and what is currently being done?

Workshop 2 (continued)

- Framework is already in place for education and training of officers
- Cyber piece is injected within each education milestone to provide familiarization throughout a career or maneuver specialists through cyber specific education throughout their entire career (cyber smart vs. cyber expert)
  - Must be done in the school house
  - At senior level – target what GO's wish they knew or want to know
  - Must know authorities, policies
- Everyone is a cyber security warrior just as they are a rifleman
  - Know your technology device as you know your M16

CYBER BEACON 2014

What gaps exist between those requirements and what is currently being done?

Workshop 2 (continued)

- Need operational focus as well as intelligence focus for cyber leader education
- AF provides one year program through AFIT (PME O-4 level) that places officers into the cyber field
- Too many schools providing cyber curriculum instead of partnering to ensure uniformity or specialization where needed
- Cyber operations (how to employ cyber teams) should be in each education milestone for all services
  - In order to get to this point – all cyber education should be accredited
  - Should be mandated

CYBER BEACON 2014

What opportunities exist for reconciling them?

Workshop 1

- Look at what everyone is doing (both training and education)
- Leverage existing opportunities
- Structure future opportunities so that they are efficient
- To inform senior leadership of the challenges
  - Joint Staff J-7
  - Service Cyber Leaders
  - DoD/OSD

CYBER BEACON 2014

What opportunities exist for reconciling them?

Workshop 2

CYBER BEACON 2014

How can we leverage industry and academia?

Workshop 1

- Competition for talent
- Academia
  - Inform academia what kind of education we need
  - Inform research communities of our problems
  - Use public/private partnerships
- Industry is the leader
  - Tell industry what are requirements are
  - Use public/private partnerships
- Reserves may not be leveraged enough
  - Already have people working in Industry
- Information Sharing and Analysis Centers (ISAC's)

CYBER BEACON 2014

How can we leverage industry and academia?

Workshop 2

- Provide education and credit to the military community
- Robust Training with Industry (TWI) opportunity for cyber career
- Fellowship programs
- Invite private industry into our DoD education system
- Understand limitations exist in regards to classifications as you get deeper into cyber operations
- Private and public partnerships
- Classification programs

CYBER BEACON 2014

How can we leverage industry and academia?

Workshop 2 (continued)

- AFIT, NPS, NDU – have academia and classification worked out
- Partner with interagency
- Partner with SANS, ISAC, etc. (foundational) and other industry such as Google (machine industry), electric, FFRDC (help in source selection)
- SCADA education partnered with DHS (up to one week course)
- What are we going to teach vs. how we are going to teach through research and development, tap into cyber exercises (i.e. Capture the Flag)
- Involve internationals (private and government)
  - State partnership programs exist

CYBER BEACON 2014

How can we communicate better with cyber stakeholders?

Workshop 1

- Methods
  - Forums/Seminars/Beacons/Collaborations/Conferences
- Who does the communicating to senior cyber leaders? How?
  - Various channels
  - Depends on who has money
  - Army example: focus is being put into the Army Cyber Center of Excellence
  - Cyber awareness probably should not be service specific
  - Is there a need for a "Joint Cyber Center of Excellence"?

CYBER BEACON 2014

How can we communicate better with cyber stakeholders?

Workshop 2

- Stakeholders must have a sense of ownership – build a network of professionals
- Identify cyber stakeholders and key cyber stakeholders
- Identify shortcomings and how to fix them
- Talk the right language
- Know your audience and speak their language (for any key leader)
- Develop reporting channels and triggers
- USCC Cyber exercises is a vehicle for better communication between stakeholders

CYBER BEACON 2014

How can we communicate better with cyber stakeholders?

Workshop 2 (continued)

- Linkage between commerce, justice, and homeland security (minimum)
- Solve the classification issue (over-classification?)
  - Understand difference between classification and authorities
  - Educate on classification and what they are
  - Where is the information (what system is it on) and how to de-classify

Appendix C

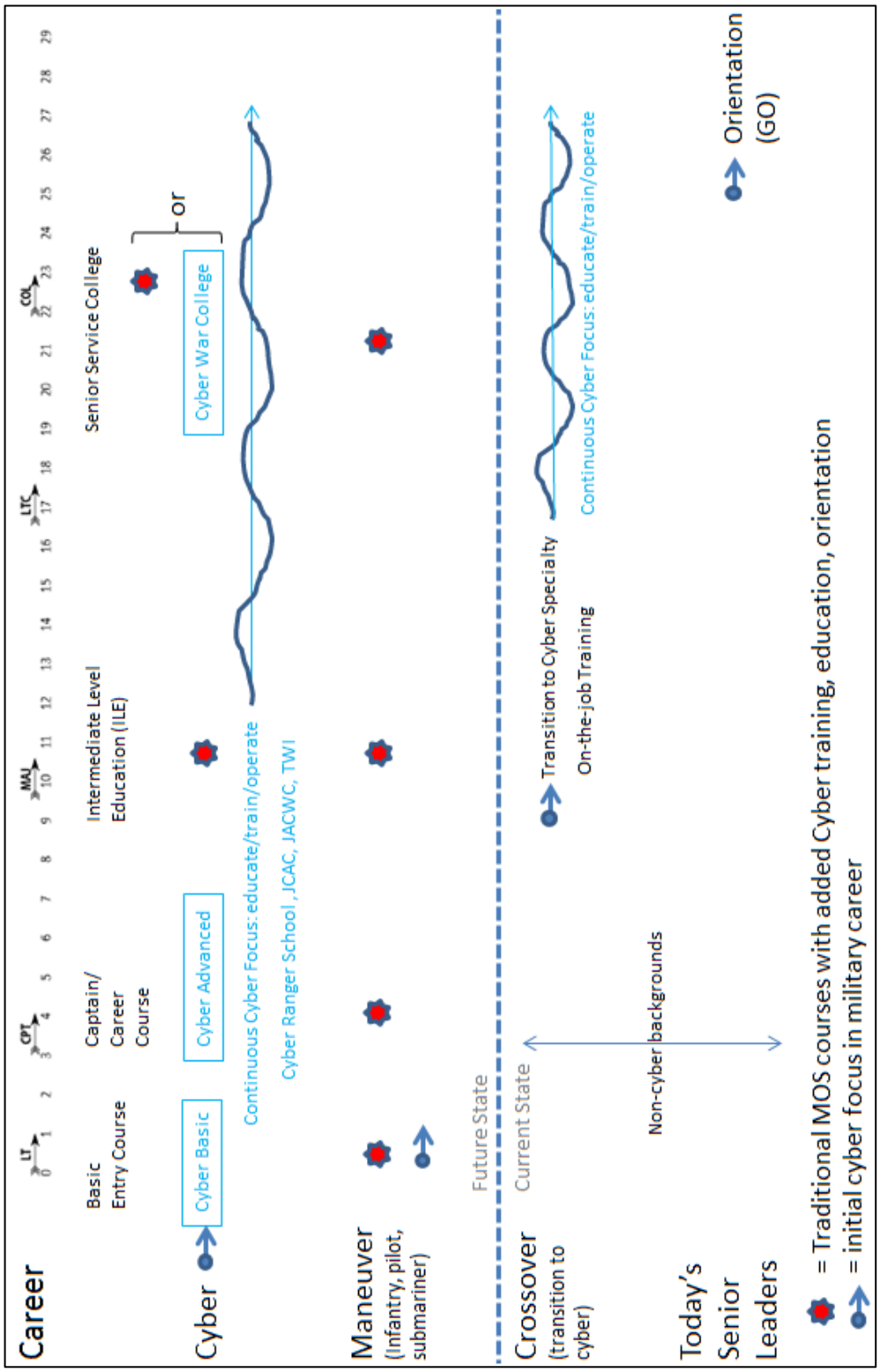

Figure C-1: Notional Cyber Development, Education and Training Milestones for Commissioned Military Officers

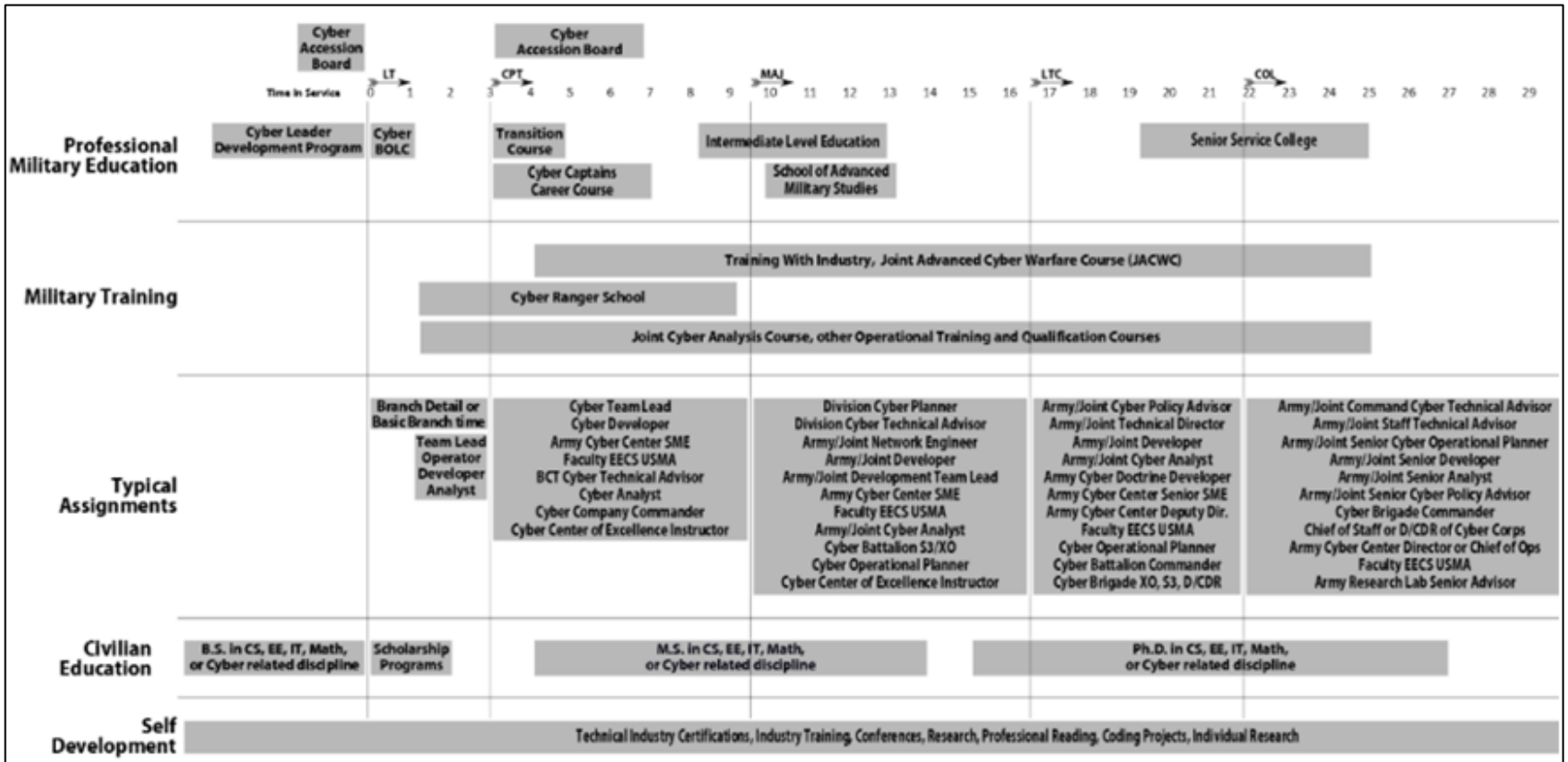

Figure 4: The Cyber Corps officer career progression timeline, from pre-commissioning through colonel.

Proposed Army Cyber Branch Career Model, from "Professionalizing the Army's Cyber Officer Force, T. Arnold, R. Harrison, and G. Conti, 2013, Vol 1337, No 2, pp. 24, http://www.westpoint.edu/acc/SiteCollectionDocuments/FULL%20PACOF.pdf

Figure C-2: Proposed Army Cyber Branch Career Model

Appendix D
Organization Snapshots

Army Cyber Institute

I. Courses (only open to USMA cadets)

- Core: 1) Python programming (intro to cyber)
  2) networking, databases, and cyber security
- Electives: Forensics; Cyber Operations (Strategy, Policy & Technology), and many others

II. Programs (USMA cadets)

- BS in Electrical Eng, Comp Sci, and IT (A; cadets)
- Cyber minor (A; cadets)
- Summer internships, 3 weeks long, 60 cadets (A), potential for ROTC cadets (U)
- NSA Center of Academic Excellence for Cyber Operations for the 2014-2019 academic years

III. Centers

- Cyber Research Center
  - Education, Research; focus on cadets
- Army Cyber Institute
  - Outreach, Advise, Research, Education

http://www.westpoint.edu/acc/SitePages/Home.aspx

IV. POCs

Ms. Clare Blackmon
-clare.blackmon@usma.edu
- 845-938-3392

Ms. Khadijah Bellamy
-khadijah.bellamy@usma.edu
- 845-938-3481

1st IO COMMAND

I. Courses (Open to military (E6 and above) and civilians) with a TS/SCI clearance

- •E, EL: Army Cyberspace Operations Planners Course
- •E,EL: Executive Cyberspace Operations Planners Seminar

II. Programs ()

- • NA

III. Centers (or other)

- • ACOPC awards ASI N9 (Cyberspace Operations Planner) to Army Officers and Warrant Officers.
- •ACOPC is listed in the National Cryptologic School Catalog as CYEC 3000.

IV. POCs

Mr. David Painter
- david.l.painter.civ@mail.mil
- 703-428-4357 (DSN 328)

Mr. John Mense
-john.l.mense.civ@mail.mil
- 703-428-4351 (DSN 328)

Mr. Amit Daniel
-amit.p.daniel.civ@mail.mil
- 703-428-4974 (DSN 328)

Air Force Institute of Technology

www.afit.edu/ccr

I. Short Courses

- Cyber 200. E; E5-E6, O3 & Civ Equiv – 3 weeks
- Cyber 300. E; E7-E9, O4-O5 & Civ Equiv – 2 weeks
- Adv Cyber Education. E; ROTC summer prog – 8 weeks

II. Grad Programs (Mil, Gov't, Def Ctr) – All active programs

- MS – Cyber Ops, Comp Eng, Comp Sci, Electrical Eng, Software Eng
- PhD – Comp Eng, Comp Sci, Electrical Eng
- IA Certificates: NSTISSI # 4011, 4012, 4016
- Research focus in all grad programs

III. Centers (or other)

- Center for Cyberspace Research (CCR) / Air Force Cyberspace Technical Center of Excellence (CyTCoE)
  - Research – DoD & National Security Focus; basic & applied, unclassified & classified (up to TS/SCI)
  - NSA/DHS Center of Academic Excellence in IA Research
  - NSA/DHS Center of Academic Excellence in IA Education
  - NSA National Center of Academic Excellence in Cyber Operations

IV. POCs

Dr. Bob Mills, CCR Director
-robert.mills@afit.edu
-937-255-3636 x4527
-(DSN 785)

US Naval Academy

I. Courses (only open to USNA students)

- SY110: Intro to Cyber Security
- SY201: E, C: Cyber Fundamentals (python programming)
- SY202: E, C: Cyber Systems Engineering
- SY204: E, C: Cyber Systems Programing (C programming)
- SY301: E, C: Data Base Structures and Cyber Operations
- SY303: E, C: Cyber System Architecture and Cyber Operations
- SY304: E, C: Hacktivism and Social Engineering
- (Note: Multiple other courses under development)
- Two Core Cyber Courses (2,000+ students per year, Si110/EC310))

II. Programs (USNA and Exchange Students)

- BS in Cyber Ops, Computer Eng, Comp Sci, IT (A)
- Information Warfare Club (A)
- Forum on Emerging and Irregular Warfare (affiliated)
- NSA Distinguished Visiting Professors (A)
- Research and Journal (focus on midn/faculty) (A)
- Cyber Fellows (interdisciplinary) (planned)

III. Centers (programs offered, see above)

- USNA Center for Cyber Security Studies

IV. POCs

CAPT Paul Tortora
Director, Cyber Center
- tortora@usna.edu
- 410.293.0933
Dr. Mark Hagerott
Deputy Director
-hagerott@usna.edu
- 410.293.0937

DISA

I. Courses:

- **Classroom – 64 courses in catalogue FY14 (46 instructed)**
- **Online Web Based Training (https://iase.disa.mil) – 35 courses**
- **DISA Enterprise Tools courses (https://iase.disa.mil) – 29**
- **Virtual Training (FedVTE) – 65 https://www.fedvte-fsi.gov/**
- **Role-Based courses – 2 (Server Admin & Network infrastructure)**
- **Cyber Protection Team (CPT) courses – 6 courses covering 32 CPT tools**

II. Programs:

- **DISA Certification and Assessments Program in development**
- **Intent to expand Cyber Workforce training to include assessments and certificates/certifications for aprox 55 Cyber roles at DISA**
- **New repository of courseware, procedure guides, and training checklists available to the DoD Services and Agencies at https://powhatan.iiie.disa.mil/specialty_courses/index.html**
- **DISA workforce coded to align personnel to roles**
- **Near term – Level 1 Certificate program for 11 roles by Dec 2014**

POC: David Still
Senior Policy Analyst: Cyber Workforce
Defense Information Systems Agency // Mission Assurance Directorate
Desk: 301-225-8391 or DSN: 312-375-8391
david.j.still.civ@mail.mil , david.j.still.civ@mail.smil.mil , david.still@disa.ic.gov

I. Courses (USAWC students, all education)

- TSC-08 Cyberspace Domain (Core)

Electives

- WF2235: Cyber Operations--What Senior Leaders Need to Know
- WF2234b: Cyber Space Theory and Strategic Security Implications
- CL2231b Cyber Warfare
- CL2237b: Cyber Planning
- CL2238: Futures Seminar

Distance Education (Distance Ed Students)

- Cyber Warfare

II. Programs (Students and outside organizations)

- (A) Cyber Wargame Series
- (A) Cyber Workshops
- (A) C/JFLCC Education
- (A) FA-59 (BSAP) Education
- (A) Senior Leader Seminar Education

III. Centers

- Center for Strategic Leadership and Development
- Strategic Studies Institute

IV. POCs

Mr. Bill Waddell
Director MCCD
717 245-4222
William.o.waddell4.civ@mail.mil

Prof Brian Gouker
NSA Visiting Professor
717 245-4727
Brian.a.gouker.civ@mail.mil

Appendix E
Additional Resources

Title	Organization/Publisher	Location
DoD Cyber Workforce Strategy	DoD CIO	http://dodcio.defense.gov/initiative/Cybersecurity/CS.aspx
Cyber Force Concept of Operations and Employment (CFCOE)	USCYBERCOM	Base document is classified; Annex C (Training) is unclassified.
Information Assurance Support Environment	DISA	http://iase.disa.mil/
Cyber Domain Security and Operations	DOD	http://www.defense.gov/home/features/2013/0713_cyberdomain/
The National Initiative for Cybersecurity Education (NICE)	NIST	http://csrc.nist.gov/nice/
Professionalizing the Army's Cyber Officer Force	Army Cyber Institute	http://www.westpoint.edu/acc/SiteCollectionDocuments/FULL%20PACOF.pdf
Joint Cyber Education and Training Network	milBook; unaffiliated	https://milsuite.mil/book/groups/jcetnet
Self-development for Cyber Warriors	Small Wars Journal	http://smallwarsjournal.com/jrnl/art/self-development-for-cyber-warriors
Information Operations Newsletter	US Army Space and Missile Defense Command	http://www.phibetaiota.net/category/journal/information-operations-io/io-newsletter/
State of Cyber Workforce Development	Software Engineering Institute	http://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_83508.pdf
Air University Cyberspace & Information Operations Study Center	Air University	http://www.au.af.mil/info-ops/cyberspace.htm

Cybersecurity Conference Listing	IEEE	http://www.ieee-security.org/Calendar/cipher-hypercalendar.html
Military Cyber Professionals Association Facebook Group	MCPA Private Facebook Group, LinkedIn Group, and various chapter sites	https://www.facebook.com/groups/milcyber