SMALL WARS JOURNAL

# Cyber Talent for Unified Land Operations

*By **Rodney D. Harris** and **Jeffrey D. Morris***
Journal Article | *Jan 19 2016 - 12:53am*

**Cyber Talent for Unified Land Operations**

Rodney D. Harris and Jeffrey D. Morris

The Army is well on path to build their required portion of the US Cyber Command's Cyber Mission Force to meet strategic objectives. It's now time to address the impending need for cyber-enabled tactical operations and Service demands. Our strategy should be focused on the ways and means of creating an organization that allows the Army to lead in this domain while achieving the Combatant Commander's objectives, enabling Army operations across a full spectrum of combat in support of all levels of command. The strategy needs to push the boundaries of existing policies, procedures and organizations even to the point of breaking beyond existing structures.

People have always given our Nation and our Army the competitive advantage. In the Cyber Domain, the people continue to be the central factor to our success. Despite our zealous focus on technology, behind every E-mail, Tweet, #hashtag, and avatar—or better yet, behind every phishing scam, denial of service attack, Honey Pot, or Remote Action Tool in cyberspace—there is a person.

Outlined within this paper are observations and suggestions of what the Army can do moving forward to address the challenges attracting and retaining Soldiers and Civilians with the talent required to conduct cyberspace operations. Perspectives within this paper are based on engagements and observations across Army Cyber Command and 2nd Army with our Soldiers, Non-commissioned Officers, Officers, Warrant Officers and Civilians. Additionally, visits across the Special Operations Community, Federally Funded Research Facilities, academic institutions and many companies across the Technology Industry were helpful in shaping much of the suggestions outlined below.

**Cyber Domain Talent: A Warfighting Domain of Technologists**

A common concern affecting management of cyberspace operators is the general lack of institutional understanding regarding cyberspace as a warfighting domain. The central idea of Unified Land Operations is that Army units seize, retain, and exploit the initiative to gain and maintain a position of relative advantage in sustained land operations to create conditions for favorable conflict resolution.**[i]** Cyber is an intrinsic part of that idea as it now adds a domain we have historically not fought in, but one that increasingly is necessary to success on the ground, air, sea and space. Modern conflict is now an endless, ever evolving battle between many actors waged to a significant degree in the cyber domain. General Mark Milley**[ii]**, in the 2015 AUSA Green Book article**[iii]** noted "The technologies that have historically enabled our overmatch are becoming increasingly available to our adversaries." In a similar way, our adversaries increasingly have the technological means to thwart or interfere with those capabilities. Examples of this are: use of drones for reconnaissance and effects delivery, encryption of communications, recruiting and influence via social media, and miniaturized and less-detectable trigger

devices.

Changes this significant requires a new approach—not only in strategy and doctrine—but in how we manage to attract the right people, develop their talent, employ them in the right places and then keep them on our team. There is general consensus within the Department of Defense (DOD) we have a shortage of talent, but not many can describe the talent they require to fill the void. One attempt at defining the critical skills or the 'talent' required is grouped into two broad categories of technologists who directly impact organizational success in cyberspace operations.

The first category includes the truly gifted programmers (Tool Developers), and on-net operators and endpoint analysts. These are the top 2% of technologists or those who possess the cognitive ability to become a two percenter. Military, governmental, agency, and industry organizations are in a fierce competition to attract this top-tier talent.

The second category are the planners, intelligence analysts, targeting officers, network security analysts and others in the cyber operating force. That's not to imply all operators, developers, or end point analysts are necessarily two percenters but most who meet the initial qualifications are capable of becoming two percenters if led and developed properly. The other 98% of the workforce in the second category are critical to leading and supporting the two percenters. Failure to properly develop these leaders will drive the two percenters out of the organization. Without the two percenters, we can only expect to just meet the criteria for success defined by the current methodology and the Army will not likely lead the cyber domain as a Service.

The Army's HR and talent strategy should include three areas that directly impact cyber talent: First, understanding the characteristics and skills of our workforce; second, organizing our operational structure to effectively employ them; third, providing leadership.

**Finding the Talent**

One of the biggest challenges for the cyber mission force is finding the appropriate talent as the Army competes to attract the best and brightest. Here is where the challenge begins, as recruiting potential cyber personnel becomes difficult in the face of competition from industry and academia. Industry needs tens of thousands of new people every year and academia completes to fill classrooms. In many ways it is a vicious cycle as new talent needs training (industry) and knowledge (academia) but once they have it, they easily find employment outside of the military. Many leaders from these two fields comment that government-trained people are some of their best candidates.

With the large investment necessary to produce trained cyber personnel, it makes sense to identify those that have a talent for the field. While arguments rage about the proper way to identify cyber talent,**[iv]** they concentrate on identifying potential talent at the accession point into the military. This may find the best talent available at recruiting stations, but only out of a random population. We can to do better at finding the proper talent.

The identification process should be started as early as middle school age. This is no different than identifying athletic talent. Children with athletic talent start playing in general sports leagues, progressing through increasingly competitive programs that identify the best of the best. These individuals are rewarded for their talent and efforts through programs that pay for advanced education and monetary rewards. Cyber-talented individuals should be chased with the same fervor.

Many Science, Technology, Engineering and Math (STEM) programs start in middle school and provide a foundation for cyber education that exist through the various levels of US school systems. While not every

school has STEM-related programs, there is a national push to involve STEM at every level. Organizations exist to provide STEM education and syllabi to educators, such as the Dayton Regional STEM Center,[v] and should receive support from the US Army to increase the potential population of cyber talent.

Identifying cyber talent through competitive or educational programs would allow us to find the 'best of the best'. Cyber competitive programs such as the Cyber-Patriot: National Youth Cyber Education Program,[vi] created by the Air Force Association, is a prime example of encouraging STEM and cyber education while also identifying the cyber gifted. Thousands of youths participate every year, culminating at a national-level cyber competitions. These types of competitions extend into the high-school and college level as well. The Army should be supporting such programs as a pool of potential cyber talent as 'pre-selecting' potential cyber personnel increases the ability and talent of Army cyber forces. This focus extends to officer programs as well. The Reserve Officer Training Corps (ROTC) and the United States Military Academy (USMA) should be sending out recruiters to entice cyber talent to attend Army programs. Success for the Army is when USMA and ROTC have 'cyber talent' recruiters as well as athletic recruiters searching the country for the best candidates.

**Standards**

One prevalent opinion often discussed is that we should establish new standards or lower current standards that might be limiting our ability to grow the cyber force we desire. Having found no identifiable metric to support that argument, the Army should not nor needs to alter standards for service as a uniformed service member or Army civilian.

Soldiers and Army Civilians must adhere to fundamental Army values like integrity, loyalty and duty. The American people place a great deal of trust in our Army and we, who serve the Nation, are held to a higher standard than most. When service members are seen in uniform it's assumed the standards to succeed fighting the Nation's wars are met in regards to physical, moral, and ethical abilities and traits. These are the foundation of trust the American people and the world have in the U.S. Military. There is no distinction between a Cyber Soldier and a Soldier belonging to another branch.

While we need not lower our standards, we do need to better understand the distinctive difference in what motivates our cyber operators and adjust the approach to managing and developing them. As the demand for cyber talent continues to increase we should consider other options to meet the operational need without degrading our standards.

Any Soldier expected to deploy in support of US forces needs to meet Army physical and mental standards, but many in the potential cyber force population may have trouble meeting current physical standards.[vii] The United Kingdom's Royal Army addressed this challenge by creating a special reserve unit that will never deploy outside the UK and recruiting cyber industry people to fill its ranks. These technical specialists work in the cyber industry every day but can be called upon to defend Britain's cyber networks.[viii] The creation of this unit has caused consternation within Britain's military establishment by not applying the same standards to all military personnel. We aren't suggesting this model would work in the US military but similar models should be studied.

**Institutional Changes**

The Army has adjusted institutional processes to prevent losing some of our most talented people for reasons like the Qualitative Service Program (QSP) or programmed movements by Human Recourses Command (HRC) without regard to mission or individual skills.

Army Cyber Command has justified the need for higher re-enlistment bonuses and special pays like Assignment Incentive Pay (AIP) and Special Duty Assignment Pay (SDAP) but much more will be required. If we fail to attract and retain the people capable of developing these skills because we don't understand them, we'll have to rely more heavily on contractors.

Our contract partners are overwhelmingly great Americans who are committed to the defense of our Nation. However, we only require they have the skill we cannot produce internally and qualify for the security clearance necessary to work. We have no real process of ensuring their values and motives are in line with the Nation or the Army. The result of that missing process could result in more Snowden-type events.

To better develop this workforce, the Army should considering the following points and suggestions:

- The Army should recognize that some of our people will not be driven to lead units like companies, battalions, and brigades but will excel as truly gifted technologists and we shouldn't penalize their promotion potential if they want to continue behind the keyboard rather than be forced by the Army broader career progression model.
- Half of our operators, developers, and most advanced analysts should be Warrant Officers; WO1-CWO4. If you are talented enough to reach a Journeyman or advanced status, you automatically assess into the Cyber Warrant Officer program.
- Any junior Soldier who becomes an Apprentice operator should automatically be promoted to SGT, much like the Ranger Regiment does when an E4 graduates Ranger School. Any Soldier who desires to try and qualify for training in these work roles should be afforded the opportunity, much like Master Gunners or Rangers in the conventional maneuver force.
- At some point, even the most skilled technologist can reach burn out and want to seek other opportunities across industry. We should not only accept this, but help them find a position within industry where we have strong partnerships through the Career Intermission Program (CIP).**[ix]** **[x]** If done properly they will be an advocate for our program and help us attract new talent. When they want to come back, we should let them without penalizing their rank nor time in grade while on active duty.
- We should facilitate seamless moves across Components: Active, Guard and Reserves. It's important that we take a Total Army approach to our training and hold firm to one standard.
- When an enlisted Soldier completes their initial eight year enlistment, they should be allowed to continue to serve without regard to re-enlistment and transfer to an indefinite status. In this career field, the number one incentive we can offer is constant access to the most technological training available as the rate of technology continues to accelerate. When we send an enlisted Soldier to a significant educational opportunity, we can require an additional duty service obligation (ADSO), as we do with commissioned officers.
- If we fail to maintain a culture and environment that meets their goals then they will resign. This will be even more important once the new retirement program becomes available and service members are allowed to take their 401K-type benefit with them. We may be able to provide 'kickers' to 401K benefits as an enticement to stay in the military, as was once done in the Veterans Educational Assistance Program (VEAP).**[xi]** The Soldier deposited money into an education fund account the program created, with the Army matching deposits on a 2-1 basis.
- Our civilian workforce should be allowed the STEM skill allowance that currently exists for GG-series Civilians in the National Security Agency (NSA) and other organizations. Civilian team members who are doing the same job with the same qualifications and skills on the same platform and mission as an NSA employee should be compensated the same way and amount. If not, then they may leave to work for the organization that values their service the most.
- The Fiscal Year 16 National Defense Authorization Act allows us to establish qualified work roles within our cyber civilian workforce as excepted service positions. Because cyber qualifications

cannot be judged as well as in other fields, this change is necessary to offer better pay scales and benefits to attract highly specialized professionals. This position change should include Army Cyber Command, JFHQ-C, and the Cyber Center of Excellence civilians.

- Excepted service cyber employees should be allowed to transfer to the competitive civilian service without undergoing additional hiring examination, as is the case now.
- The CMF should be exempt from the strenuous limitations on the use of over-time, ensuring civilian employees are not disadvantaged in comparison to NSA employees who are given more flexible options for over-time opportunities.
- We should allow more morale-building hours to ensure our civilian workforce are able to participate in all organizational activities and approved fitness programs without losing leave days in order to build a cohesive team.
- The DOD should create a new Cyber Career Program for civilians that allows for rapid advancement through a focused path for progression within the Cyber Mission Force. Many current civilian employees are in situations where they cannot advance due to a mismatch between job descriptions and actual job requirements.
- Finally, I believe that we should have complete transparency in regard to how we manage and develop the workforce. We can do that through an application for the CMF that allows all our people to see available opportunities like Training With Industry (TWI),**[xii]** Advanced Civil Schooling (ACS), and current position vacancies and opportunities both inside the Cyber Mission Force and beyond such as with Training and Doctrine Command (TRADOC), Asymmetric Warfare Group (AWG), United States Special Operations Command (SOCOM), and the Army Cyber Institute (ACI) to list a few. Individuals that meet the published requirements and Knowledge-Skills-Abilities (KSAs) would be allowed to submit their resume for consideration. This would also flatten communications allowing leader blogs and chats groups that will more likely resonate and connect with our distributed and highly technical workforce.

These challenges with talent management are shared across the Services as the DOD struggles to operationalize this new domain. The Army, having created the new Cyber Branch and 17-series MOS, is in the best position to lead the DOD if we are willing to make significant change.

**Organizing Operational Structures**

How we currently organize and employ cyberspace operators is itself a barrier to talent management and development. Organizational structure and design in cyberspace operations, to a large degree, has been developed by USCYBERCOM. CYBERCOM's focus is at the strategic level and does not adequately address the Army's cyber requirements at the operational and tactical level. Cyber's value to the Army at these levels is not well understood, but ongoing efforts are exploring the tactical-operational edges.**[xiii]** **[xiv]** The design of our teams, infrastructure, tools, and command and control may not be applicable to tactical units and have been created and developed in a way which stifles innovation and allows little room for initiative.

Our adversaries are most likely not restricted by rigid organizational structures and self-imposed barriers. A quick study of the current Russian operations in the Ukraine and elsewhere offers insight into some of the most visible flaws with our current operating concepts.**[xv]** Russia has learned to artfully converge and weaponize information operations, electronic warfare, and network warfare in both digital and physical operations, while we debate what actions are military operations versus intelligence activities and struggle with traditional concepts of Offense, Defense and Exploitation, Operational Preparation of the Environment, and Intelligence Surveillance Reconnaissance.**[xvi]**

Many cybersecurity experts argue that offensive and defensive cyber tools are often the same, the difference lies in the intent of their use. Regardless of the purpose of the code, the skill required enabling

network or platform operations to deny, destroy, degrade or disrupt are not unlike the skill required to operate within our own network or platforms to hunt, identify, prevent and remove adversaries. A great example of this argument is the impact of adding malicious software to the Wassenaar Arrangement that limits the transfer of dual use technologies.**[xvii]**

Today we have teams organized and structured for offense, other teams for defense, and still others for analysis and exploitation. Our current structure has created stove pipes that become barriers to intelligence and information sharing while limiting our ability to synchronize cyberspace operations.

The reasoning for legal authorities and proven processes enabling success at the strategic level should always remain a primary factor in our planning assumptions. The Army now has the opportunity to lead in this space by creating cyber operation forces structured as maneuver forces to conduct full-spectrum combat operations. These operations can be based on Mission, Enemy, Terrain and weather, Troops and support available, Time available and Civilian considerations (METT-TC), instead of just saying that "we maneuver in cyberspace."

To facilitate information sharing and synchronize cyberspace operations, the Army cyber force should mirror the structure of maneuver forces to conduct a full spectrum of combat actions. Commanders can then task-organize within their formations to accomplish the mission and allow them to assess risk based on desired effects. If a team is required to enable an effect that does not involve action above the subnet level, should it take the Commander-in-Chief to approve their operation? Many of the required technologies and capabilities are no longer held as a national secrets and are used in homes today by children who don't ask for Presidential approval.

Current policy, structure and organizational models designed around existing legal authorities not only limits the innovation and capabilities of our people but also prevents any deterrence that could be gained by more aggressive responses to attacks. They limit our ability to share lessons learned from Unconventional Warfare operations as we do in every other domain. The Army should be moving faster to employ teams in support of tactical operations while reducing the standards for intelligence gain/loss decisions. Investing in this capability and demonstrating it without regard for attribution will foster buy-in from our maneuver forces and also serve to deter actions by our adversaries.

Many debates on cyber-enabled tactical operations focus on lawful authorities, access, infrastructure, and tools. Because the Army is required to focus on the land and human elements of cyberspace, we should be leading the effort to establish a new authority that bridges Titles 50, 40, 44, 32, and others. As long as we continue to ask for authorities that belong to other organizations, the resulting decisions may not be based on missions but instead on the possibilities of losing resources. If I give you my authorities, then I am really giving you my resources required to administer those authorities. Until then, authorities should not prevent us from properly training. Failing to allow our cyber forces to train in developing the tools, access, and infrastructure required to employ effects at the tactical level restricts innovation and ultimately contributes to the loss of our most talented operators.

**Leading the Cyber Professional**

The final challenge and arguably the most important is leading Cyberspace Talent. Talent management and effectively employing cyberspace operators ultimately depends on leadership. Only after spending considerable time learning the technical aspects of cyber operations can leaders have meaningful conversations and begin to affect organizational culture barriers, fix issues with pay, promotions, leader development and talent management. Leaders who do not understand the field will have a hard time understanding the needs of their cyber Soldiers.

Regarding the “two percenters,” those technologist that every organization within the government and industry are looking to find and keep, these are those who our organization must learn to lead if we want to attract and retain them. Obviously all developers and operators are not two percenters but the 98% who are gifted with the cognitive ability to work in high technology roles and even understand the environment are the ones who are able to lead the two percenters.

Now that we have a new Cyber Branch, we can start to build our initial cadre of future cyber leaders who will have both a technologist’s understanding of the cyber domain and broad knowledge of Army and joint operations. In the future, cyber leaders with computer science degrees and qualifications as software developers and on-net operations will have a better understanding of cyberspace operations and the needs of cyber operators. They will also have inherent creditability that our leaders don’t always have today. I often compare this to an infantry platoon leader in the 82nd Airborne Division—trying to lead without a Ranger Tab. Recently, an article written by Army and industry leaders suggested creating a cyber leader course modeled after the Army Ranger School. These technologists advocate training cyber leaders to the standards expected of Ranger graduates: tough, comprehensive, and stressful. Such leaders would have a deep understanding of their chosen domain, but also gain experience in creating and leading teams to operate in full-spectrum cyber operations.**[xviii]**

The USMA is currently graduating a handful of cyber-trained lieutenants every year, many who participated in the Cyber Leader Development Program (CLDP). This optional program allows cadets additional computer science and cyber technology opportunities and those who complete over 800 hours additional training can be recognized in their official training records.**[xix]** This small core of leaders, along with equal numbers of cyber-trained ROTC graduates, will grow into the cyber leaders of tomorrow. But for now, the Army must look among existing Army leaders to choose those to lead the new CMF.

**Conclusions**

The Army leads the Department of Defense in developing organizational structure, institutional programs and facilities to meet the Combatant Commands requirements. We are leaning forward to meet the emerging demand for Cyber capabilities as traditional weapon platforms, rather than operations to keep our ability to communicate. The idea of an “Improvised Cyber Device” used to destroy and or disable war-fighting platforms is no longer a fictional concept but a reality we must begin to consider. The investment being made for structural facilities and institutional development will be of little value if we fail to make the necessary changes in how we conduct Talent Management of the Cyber Mission Force…regardless of the domain, our people remain the critical center of gravity.

*The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Military Academy, Army Cyber Command, the Department of the Army, US Cyber Command, the Department of Defense, or the US Government*.

**End Notes**

**[i]** HQDA, ADP 3-0 *Unified Land Operations*, Oct 2011;

**[ii]** Chief of Staff, US Army; http://www.army.mil/leaders/csa/

**[iii]** AUSA 2015 Green Book;
https://www.ausa.org/publications/digital/Documents/greenbook2015/index.html

**[iv]** *Cyber Aptitude Assessment: Finding the Next Generation of Enlisted Cyber Soldiers,* http://cyberdefensereview.org

**[v]** http://daytonregionalstemcenter.org/

**[vi]** https://www.uscyberpatriot.org/

**[vii]** Army recruit command boss: Overweight youth a growing problem; 29 Aug 2014; http://www.usatoday.com/story/news/nation-now/2014/08/29/army-recruiting-obesity/14798757/

**[viii]** Fitness tests waived for MoD's new reservist cyber warriors, 21 Jan 2015; http://www.telegraph.co.uk/news/uknews/defence/11360976/Fitness-tests-waived-for-MoDs-new-reservist-cyber-warriors.html

**[ix]** Enlisted Career Intermission Pilot Program CIPP; 20 Nov 2015; https://www.hrc.army.mil/Enlisted/Enlisted%20Career%20Intermission%20Pilot%20Program%20CIPP

**[x]** Take three years off: Army extends sabbatical program; 06 Jul 2015; http://www.armytimes.com/story/military/careers/army/2015/07/06/career-intermission-pilot-program-2015/28471175/

**[xi]** Veterans Educational Assistance Program; http://www.benefits.va.gov/gibill/veap.asp

**[xii]** Broadening Opportunity Programs https://www.hrc.army.mil/OPMD/Broadening%20Opportunity%20Programs%20Building%20a%20cohort%20of%20leader

**[xiii]** Army experiments now underway that integrate cyber and land operations; 10 Jul 2015; http://www.c4isrnet.com/story/military-tech/cyber/2015/07/10/army-testing-cyber-integration-in-land-operations/29976545/

**[xiv]** Phreaker, Maker, Hacker, Ranger: One Vision for Cyber Support to Corps and Below in 2025; 11 Aug 2015; http://smallwarsjournal.com/printpdf/26664

**[xv]** Russia's Winning the Electronic War; 21 Oct 2015; http://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/

**[xvi]** The Ukrainian crisis – a cyber warfare battlefield; 05 Apr 2014; http://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html

**[xvii]** The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies; http://www.wassenaar.org/

**[xviii]** Towards a Cyber Leader Course Modeled on Army Ranger School; 18 Apr 2014; http://smallwarsjournal.com/printpdf/15584

**[xix]** Towards a Cyber Leader Course Modeled on Army Ranger School; 18 Apr 2014;

## About the Authors


### Rodney D. Harris

Command Sgt. Maj. Rodney D. Harris, USA, recently retired from active duty. His final assignment was the Senior Enlisted Leader to the U.S. Army Cyber Command and 2nd Army. He holds a B.S. from Trident University International.


### Jeffrey D. Morris

Master Sergeant Jeffrey D. Morris is a Cyber Senior Non-commissioned Officer and Sergeant Major of the Army Cyber Institute at West Point. He holds a Ph.D. in System Engineering from the Air Force Institute of Technology, a M.S. in Information Systems from Nova Southeastern University, a M.S. in Strategic Intelligence from the National Intelligence University and a B.S. from Excelsior College. He holds the Certified Incident Handler certification and teaches information technology and systems engineering courses at West Point. He conducts research on quantum computing and cyber talent.



**Links:**
{1} http://smallwarsjournal.com/author/rodney-d-harris
{2} http://smallwarsjournal.com/author/jeffrey-d-morris
{3} http://www.army.mil/leaders/csa/
{4} https://www.ausa.org/publications/digital/Documents/greenbook2015/index.html
{5} http://cyberdefensereview.org
{6} http://daytonregionalstemcenter.org/
{7} https://www.uscyberpatriot.org/
{8} http://www.telegraph.co.uk/news/uknews/defence/11360976/Fitness-tests-waived-for-MoDs-new-reservist-cyber-warriors.html
{9} https://www.hrc.army.mil/Enlisted/Enlisted%20Career%20Intermission%20Pilot%20Program%20CIPP
{10} http://www.benefits.va.gov/gibill/veap.asp
{11} https://www.hrc.army.mil/OPMD/Broadening%20Opportunity%20Programs%20Building%20a%20cohort%20of%20leader
{12} http://www.c4isrnet.com/story/military-tech/cyber/2015/07/10/army-testing-cyber-integration-in-land-operations/29976545/
{13} http://smallwarsjournal.com/printpdf/26664
{14} http://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/
{15} http://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html
{16} http://www.wassenaar.org/