IDA | RESEARCH NOTES


# CHALLENGES IN CYBERSPACE: THE HUMAN DIMENSION

5 Building the Cyber Warfare Force
10 DoD's Cyber Workforce Challenges
14 Staffing Cyberspace Operations
20 Identifying Enlisted Recruits with the Right Stuff to Perform Cyberspace Operations
26 Air National Guard Cyber Force
31 Modernizing Air Force Cybersecurity Test and Evaluation

November 2018

IDA is the Institute for Defense Analyses, a non-profit corporation operating in the public interest.

IDA's three Federally Funded Research and Development Centers provide objective analyses of national security issues and related national challenges, particularly those requiring extraordinary scientific, technical, and analytic expertise.

The summaries in this edition of IDA Research Notes were written under the auspices of IDA's Information Technology and Systems Division (ITSD). Please contact the division director, Dr. Margaret E. Myers (703.578.2782, mmyers@ida.org), for more information on any of these articles.

IDA

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, Virginia 22311
ida.org

# Challenges in Cyberspace: The Human Dimension

The first *IDA Research Notes* on *Challenges in Cyberspace* was published in 2011, not long after the Department of Defense recognized cyberspace as the fifth operating domain.

In the keynote article of that publication, retired **General Larry Welch** described ways to mature our understanding of cyberspace operations. Cyberspace is a domain, he wrote—a place, not a mission. As in the other domains—land, sea, air, and space—military superiority is derived from our freedom of action in, through, and from cyberspace, and from our ability to deny adversaries freedom of action at the times and places of our choosing. General Welch further recognized the need to move forward rapidly to build the needed cyber forces with the needed set of capabilities to produce the desired set of military effects across the spectrum of cyber operations.

Since 2011, the human dimension of cyberspace has been a common theme in IDA research. The articles in this issue of *IDA Research Notes* describe multiple aspects of our research related to the human dimension of challenges in cyberspace.

In the opening article here, **General Welch** again sets the stage by reviewing progress in building cyber forces in the United States Cyber Command and military departments. He notes that the significant cyber operations capability that exists today reflects the inherent limitations of embedding a combat force's mission in a structure dominated by the intelligence and information systems communities, and he advocates for intense attention to cyber warfare force organization, capabilities, policies, and authorities, consistent with the importance of the cyberspace domain to success in all domains.

In the next article, **Gregory Cox** summarizes an internal IDA research project that looked at seven "cyber workforce" projects over the past three years, all for various sponsors and with various perspectives. In lieu of finding common observations, he discovered that each sponsor started with a different understanding of "cyber" and "workforce." One of his conclusions is that the cyber workforce cannot scale proportionately to the growing challenges in cyberspace. The next four articles highlight research from some of the projects he examined.

**Thomas Barth** and **Stanley Horowitz** examine the total force mix for the military, civilian, and contractor personnel who make up the Cyber Mission Force (CMF). Their research includes an analysis of the CMF mission to determine which roles should be considered military essential, inherently governmental, or commercial activities.

The Army's challenges in identifying and training enlisted recruits for cyberspace operations roles are addressed in the article by **Thomas Barth** and **Elizabeth McDaniel**. They summarize continuing work to investigate the links between aptitude, knowledge and skill, maturity, personality

traits, and motivation and successful performance in cyber operations roles.

**Julia Warshafsky** describes several findings and recommendations from her IDA team's research on the Air National Guard (ANG) cyber force. She examines trends in cyber talent demand and military service propensity, ANG cyber personnel eligibility requirements, recruiting and retention efforts, and the evolving scope of the ANG's domestic cyber roles.

In the concluding article, **Walter Rhoads** provides an overview of research that developed a modernization roadmap for the Air Force cybersecurity test and evaluation workforce, infrastructure, and processes. The findings include near-, mid-, and far-term objectives to augment the cyber workforce capability.

# Building The Cyber Warfare Force

Larry Welch

**The Challenge: Cyberspace may well be the most contested operational domain and the domain in and from which operations produce the most far-reaching effects in the land, sea, air, and space domains. DoD needs dedicated cyber operational forces provided by the Services and employed by combatant commands with clear warfighting missions.**

**Eight years after establishing USCYBERCOM, there remains a need for a clear mission identity across DoD, more clarity in military department responsibilities for force building, and more rapid growth in capabilities.**

## The Central Issue

Organizing for effective cyber operations serving the needs of the Department of Defense (DoD) has proved to be challenging. A particularly visible current issue is the future organization of United States Cyber Command (USCYBERCOM). The President has made the decision to elevate the command to a full combatant command, which will remove it from United States Strategic Command's (USSTRATCOM) jurisdiction, where it was to be integrated with other global missions. The second decision, now resting with the Secretary of Defense, is on separating the roles of Commander, USCYBERCOM and Director of the National Security Agency (NSA). This issue calls for a deeper understanding of the relationship between the cyber operations role of USCYBERCOM and the signals intelligence mission of NSA and of the impact of that relationship on both missions. Regarding organizing for cyber operations, there is a need for increased clarity in the answer to the fundamental question: "Organize to do what?"

To respond rapidly to the clear need for effective cyber operations, DoD initially elected to build cyber forces largely in or closely associated with the existing intelligence and information systems structure. That approach has produced significant new cyber operations capabilities. Still, 8 years after establishing USCYBERCOM, there remains a need for a clear mission identity across DoD, more clarity in military department responsibilities for force building, and more rapid growth in capabilities. The answer to the question "To do what?" is to structure forces, policies, and authorities to conduct cyber warfare securing vital elements of cyberspace and delivering combat effects in and through cyberspace. *The fundamental need is for a Cyber Warfare Force to conduct offensive and defensive operations.*

## Some History

The initial motivation, advocated by the Director of NSA supported by the Director of National Intelligence, was the growing awareness of the need to protect information and systems from cyber intrusion and attack. DoD responded to the need by adding cyber operations to the mission responsibilities of USSTRATCOM. The Commander, USSTRATCOM's approach to this, and other missions added to the command's core strategic deterrence and space missions, was to form a set of Joint Functional Component Commands (JFCCs) and a Joint Task Force (JTF). This was to provide the command with access to needed expertise not available in the command.

The Intelligence Community's missions had long required intense focus on understanding information networks and exploiting access to information through networks. Forming JFCC-Network Warfare, with the Director of NSA dual-hatted as commander, was a logical organizing step in 2005. At the same time, Joint Task Force-Computer Network Defense (JTF-CND), created in 1998, was changed to Joint Task Force-Global Network Operations (JTF-GNO) charged with defense of the Global Information Grid (GIG). This separation of the offense and defense missions endured until the JTF-GNO was integrated into USCYBERCOM in 2010.

In 2008, the Deputy Secretary of Defense and the Vice Chairman, Joint Chiefs of Staff, asked IDA to provide recommendations on organizing for command and control (C2) of cyber operations. IDA formed a group of senior retired military officers and analysts who had relevant experience to address the issue. While providing options for approaches to cyber C2, IDA concluded and reported that DoD needed to put more emphasis on defining the cyber mission and building effective cyber forces than on C2 of forces not yet formed. Still the outbrief to the Joint Chiefs led to a decision by Secretary Gates to form a subunified command under USSTRATCOM, with the Director of NSA dual-hatted as commander.

The Commander, USSTRATCOM expressed the belief that the emphasis should be on clarifying mission expectations and on force building. He was concerned that building a new combatant command could be a distraction from needed clear direction to the military departments to deliver needed cyber forces. It soon became apparent that effective C2 has less to do with headquarters organization than with clarity of mission, authorities, force capabilities, and integration with operations in and from other domains. These essential elements are yet to be adequately defined and developed.

## Expectations and Outcomes

Both the Commander USSTRATCOM and the IDA panel were concerned with the direction and pace of cyber capability development in DoD. By 2007, the Department was beginning to treat cyberspace as an operating domain, and in 2011, cyberspace was officially recognized as a contested operating domain. Given that recognition, military objectives are essentially the same as for the other four operating domains: access and freedom of action to deliver desired

effects in and from the domain at times and places of our choosing. The corollary to that purpose is to deny the same to our adversaries. The logical expectation was mounting a concerted campaign to define and build a Cyber Warfare Force to meet the challenges to national security. These challenges have long been widely experienced with the sure prospect of becoming ever more consequential. Defining needs is a key joint community role in force-building for any domain—answering the "to do what?" question. The military departments then have the role of organizing, training, and equipping forces to meet those needs.

In the case of cyber operations, this role applies to each of the military departments. Unlike other domains, given the ubiquitous nature of cyber operations and the impact on operations in and from all domains, there is no dominant Service in this domain. This need not be an obstacle to the set of force providers (military departments) building an effective Cyber Warfare Force. As an example, while there is a dominant Service in the air domain, each of the Services has organized, trained, and equipped air domain capabilities, tailored to their dominant domain, to meet the demands of joint combat operations.

To build capabilities rapidly, the Army placed the cyber force-building responsibility in the Army Intelligence and Security Command (INSCOM). The Navy put the responsibility for operational control to execute cyber, electronic warfare, information operations, and signals intelligence in Tenth Fleet. The Air Force started with an intelligence wing and information warfare center, which was moved from the Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA) to a newly formed 24th Air Force in Air Force Space Command.

The necessary initial reliance on the NSA cryptologic platform for essential cyber operations further tied military cyber operations to Intelligence Community limitations and priorities. Operations on this platform are essential to effective intelligence operations. Important processes and qualifications are required to ensure continued effectiveness for intelligence collection and support to the broad range of operations that includes cyber operations. The overall result was that force-building direction, including operating unit structure, training requirements, and certification, migrated to the newly established combatant command and was strongly shaped by Intelligence Community practices and priorities.

This force-building approach has produced significant cyber operations capability, but it continued for almost a decade with the inherent limitations of embedding a combat forces mission in a structure dominated by the intelligence and information systems communities. The joint and Services intelligence and information systems activities serve vital purposes and meet a challenging set of mission demands. They are not combat operating forces that must interface and integrate with combat operations across multi-domains. Such forces need the clear identity and career field opportunities and expectations that characterize the recognized combat forces of the Services.

The Army began to treat cyber operations as combat arms with the establishment of MOS 17C, Cyber Operations Specialist, in 2015 and now treats cyber operations as a distinct branch of the Army. For the Air Force, cyber superiority is still not treated as a core mission, and career management leadership for specialty codes making up the Air Force cyber mission force rests with the intelligence directorate and the Chief Information Officer. The Navy continues to embed cyber operations in the signals intelligence structure.

## The Continuing Need

Effective cyber operations are increasingly essential to effectiveness in, from, and across all five domains. DoD is engaged every day in operations against aggressive adversaries in cyberspace. Cyber operations delivering effects in and from the contested cyber domain is a combat forces role. Meeting the operational challenge requires an operational organization with an operational orientation.

Intelligence and information systems skills and understanding are essential enablers of effective cyber operations. Intelligence officers and enlisted are essential members of combat operating teams—offense and defense. These skills are more essential for cyber operations than for other missions. Addressing cyber targets requires extensive intelligence preparation and continuous network analysis to navigate to the cyber target, penetrate defenses, create the desired effect, and assess the results. Further, unlike operations in other domains, cyber operations can change this man-made domain in hard-to-predict ways, requiring network analysis to be in real time.

These and other factors demand closely integrated, multi-discipline, experienced cyber combat crews in tailored units in the Cyber Warfare Force. The need is not to reduce the intelligence and information systems roles in cyber operations: the opposite is true.

The need is for a career force fed and sustained by communications, information, and intelligence career fields. But it cannot be a pick-up force of people temporarily diverted from other information systems and intelligence activity. Instead, it needs to be a Cyber Warfare Force treated as combat forces, managed and led as a career force. Like the approach to every other combat mission, the military departments need to deliver forces for cyber warfare operations conducted by combatant commands integrated with other forces to achieve warfighting effects.

The need is also for operating platforms and cyber weapons with capabilities and processes that are optimized for cyber operations. The operating platforms and cyber weapons need to provide for operations across the spectrum, from strategic to tactical. The rules of engagement and authorities need to be appropriate to the level of operations, just as is the case with operating platforms and weapons employed in and from other domains.

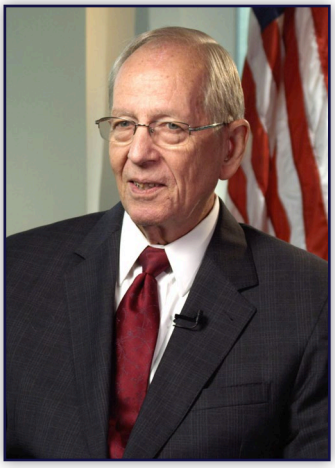
## Conclusion

Cyberspace may well be the most contested operational domain. It may also be the domain in and from which operations produce the most far-reaching effects in the land, sea, air, and space domains. To deal with these conditions and consequences, DoD needs dedicated operational forces provided by the Services and employed by a combatant command or commands with clear warfighting missions.

The force capabilities need to include intelligence and information systems experience and expertise, but they cannot be effective if they are subordinate to intelligence or information systems authorities and priorities. DoD has been successfully defining needs and organizing, training, and equipping warfare forces for decades in the land, sea, and air domains.

The Department is addressing the reality of warfare in the contested cyberspace domain with increased intensity. Despite the continuous ongoing conflict in cyberspace and the near certainty that such conflict will have an ever-larger role in warfare at all levels, the term *cyber warfare* continues to generate resistance in some quarters. Still, the importance of the cyberspace domain to success in all domains clearly warrants intense attention to Cyber Warfare Force organization, capabilities, policies, and authorities.

General Larry Welch is a Senior Fellow and former President of IDA. He holds a Master of Science in international relations from George Washington University.



# Department of Defense Cyber Workforce Challenges

Gregory Cox

**The Challenge: "Everybody" knows that the demand for skilled cyber workers exceeds the supply, but "nobody" knows how to solve this dilemma. There is no evidence that an approach based only on expanding the workforce pool will lead to a satisfactory solution. However, before viable solutions can be meaningfully explored, we need to understand the cyber landscape.**

**It has proven impossible to determine the size of DoD's cyber workforce because it depends on who is "in" and who is "out" of that workforce.**

## The Cyber Landscape Has Poor Resolution

There is a consensus that cyber threats pose serious and growing challenges, but that consensus begins to evaporate over the dimensions of those challenges. In part, this is because the full extent of the cyberspace domain landscape is still debated—what is included and what is not? While it is natural to desire a bounded and crisp description of the landscape, sometimes that desire can lead to a narrow interpretation of the challenges. For example, the Defense Science Board (DSB), expanding on the Department of Defense's (DoD) formal definition of the cyberspace domain, offered its fairly broad interpretation (DoD Defense Science Board January 2013), (DoD Defense Science Board February 2017).

> *The term "cyber" is broadly used to address all digital automation used by the Department and its industrial base.* ***This includes weapons systems and their platforms; command, control, and communications systems; intelligence, surveillance, and reconnaissance systems; logistics and human resource systems; and mobile as well as fixed-infrastructure systems.*** *"Cyber" applies to, but is not limited to, "IT" and the "backbone network," and it includes any software or applications resident on or operating within any DoD system environment.*

Likewise, the interpretation of DoD's cyber workforce might be narrow or broad. Under DoD Directive 8140.01 (Cyberspace Workforce Management), the cyberspace workforce comprises four endeavors: (i) cyberspace effects, (ii) cybersecurity, (iii) cyberspace information technology, and (iv) cyberspace-related intelligence. However, if we adopt the DSB's interpretation of cyber, workforce members must perform duties that might not be viewed as falling into these bins, such

as those to do with the cyber-related attributes associated with weapons systems and logistics systems.

This leads to an observation: it has proven impossible to determine the size of DoD's cyber workforce because it depends on who is "in" and who is "out" of that workforce. Despite this uncertainty, it is safe to say that DoD's cyber workforce size is currently over 100,000, and perhaps over 200,000.

## The Cyber Mission Force: An Experiment in Progress

If we accept the premise that the current DoD cyber workforce exceeds 100,000, it is apparent that the Cyber Mission Force (CMF), with its 6,187 authorized billets spread among 133 individual teams, is a small fraction of that workforce.[1] Nonetheless, the CMF tends to become the focus of discussions about DoD's cyber capabilities, with many of those discussions about which teams have reached initial operational capability (IOC) and which have reached full operational capability (FOC) (Department of Defense April 2015).

A casual reader might be excused for believing that once a CMF team has reached FOC, it will continue to have full capability. That is not the case, however, because constant personnel rotations change the teams' *readiness*. Fortunately, there is growing recognition that readiness, rather than IOC/FOC status, is a more-appropriate team attribute; unfortunately, however, readiness is still largely measured in terms of on-hand personnel, currency of personnel training, and equipment condition, which are essentially the same metrics used to establish IOC/FOC status.

Cyclical readiness is a fact of life for many military units (e.g., Army Brigade Combat Teams) as they undergo readiness ups and downs in their cyclical prepare-deploy-reset processes. However, IDA has found no evidence of plans to manage the inevitable cyclical readiness of the CMF, but rather an implicit assumption that all teams are ready all of the time. But unless there are sufficient redundancies to compensate for personnel turnover—a significant workforce impact—we should expect to see ups and downs in CMF team readiness.

## Workforce for the Entire Cyber Landscape, and Beyond

In his recent book, Bruce Schneier writes about computers in a broad sense. (Schneier 2015) Although his characterization is hyperbolic, it nonetheless speaks to a largely unappreciated facet:

> *Your phone is a computer that makes calls. Your car is a computer with wheels and an engine. Your oven is a computer that bakes lasagnas. Your camera is a computer that takes pictures.*

[1] The five types of CMF teams are Cyber Protection Teams (68), Combat Mission Teams (27), Combat Support Teams (17), National Mission Teams (13), and National Support Teams (8). Additional teams beyond these are currently being created from Army Reserve Units.

Schneier is not alone; Joshua Marcuse, Executive Director of the Defense Innovation Board, describes the F-35 this way (Marcuse n.d.).

> *The F-35 is not a plane with a supercomputer onboard; it is a supercomputer with wings.*

Indeed, we might go one step further and say that the F-35, with its multiple sophisticated sensors and requisite data fusion, is a *networked* supercomputer with wings. This implies that a prominent capability for the F-35 resides in the cyberspace domain and leverages the air domain, even though this clashes with the general characterization of this aircraft as operating in the air domain and leveraging the cyberspace domain. This observation is not unique to the F-35; we could talk about many (or most) modern weapon systems (e.g., Navy ships) or concepts this way. None of these weapon systems are immune to cyber threats, and thus there are cyber workforce implications for them.

Source:https://www.defense.gov/News/Article/Article/1218741/us-showcases-f-35-lightning-ii-aircraft-at-paris-air-show/,

This highlights a fundamental problem with the cyber workforce. The workforce will not—because it cannot—scale proportionately to the (growing) challenges. Although initiatives to enlarge and strengthen the workforce are important and helpful, DoD may not succeed in balancing workforce supply with demand by seeking more talent. It is time to start thinking outside the proverbial box.

First, a root cause of cyber vulnerabilities in weapon systems is that their relevant requirements were developed at a time (many years ago) when our understanding of the cyber landscape was less mature. (This assertion will also apply 10 years from now.) This demands a different mindset in the systems engineering process for weapon systems. In his book on security engineering, Ross Anderson observes that traditional system engineers deal only with error and mischance rather than malice. (Anderson 2008) Automobile manufacturers (who rely on profits) have come to accept responsibility for the "malice factor" after some highly publicized events, such as the *Jeep Cherokee* hack. (After Jeep Hack 2015) Why shouldn't major defense contractors (who also rely on profits) be held to similar standards?

Workforce solutions may also come from automation, which can help especially with challenges that are too fast, boring, or expensive for people to handle manually. As Dan Geer eloquently predicts: "The skills shortage in cyber security will not be solved. Governmental sectors will remain unable to retain those they have nurtured. The enterprises able to pay any price for talent will get all or most of that talent. Algorithms will therefore be deployed to do what we ourselves cannot do, which is to protect us from other algorithms." (Geer 2017)

However, as Geer is careful to articulate, caution is the watchword. There can be a steep (perhaps irreversible) downside to algorithmic automation as cyber challenges become more demanding in both scope and sophistication. Thus, we see potential use of pattern recognition and preprogrammed responses for cyber defense and intelligence as an aid to human operators, but we remain wary of visions with automation as "the workforce solution."

Finally, lest we think too narrowly about the many cyber workforce challenges, what about broader information operations and electronic warfare? There is some recognition that these are not cleanly separated from "cyber." In this sense, even the broad DSB interpretation of cyber may be too narrow. Indeed, with hindsight it may prove that DoD should have declared the "information domain" as the fifth warfighting domain instead of the cyberspace domain. But regardless of whether cyber and broader information elements are formally merged, they will compete for many of the same skilled workers. In an area where worker talent is in short supply, there is a compelling case for eliminating duplication and pooling workforce resources to the largest extent possible.

## References


2015. "After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix." *Wired*. https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

Anderson, Ross. 2008. *Security Engineering*. 2nd. Wiley Publishing Company.

Department of Defense. 2015. *The Department of Defense Cyber Strategy*. April.

Department of Defense Defense Defense Science Board. 2013. *Resilient Military Systems and the Advanced Cyber Threat*. January.

Department of Defense Defense Science Board. 2017. *Defense Science Board Task Force on Cyber Deterrence*. February.

Geer, Dan. 2017. *Keynote speech to SOURCE* ). Boston, April 27. http://geer.tinho.net/geer.source.27iv17.txt.

Marcuse, Joshua. n.d. https://www.youtube.com/watch?v=eatGvBU18MU.

Schneier, Bruce. 2015. *Data and Goliath*. W.W. Norton and Company.



Dr. Gregory Cox is a Research Staff Member in IDA's Information Technology and Systems Division. He holds a Doctor of Philosophy in mathematics from Auburn University.


# Staffing Cyberspace Operations

Thomas Barth, Stanley Horowitz

**The Challenge: Choosing the wrong total force mix for the Cyber Mission Force can put the mission at risk or create inefficiencies that consume scarce resources. This problem is compounded by the lack of a legal framework for identifying combatants in cyberspace operations.**

**Using military personnel for roles that are not truly military essential can be costly, both financially and manpower-wise.**

## Background

Building a Cyber Mission Force (CMF) capable of carrying out cyberspace operations is currently a major force planning effort in the Department of Defense (DoD). Determining the appropriate total force mix, defined as the choice between military, civilian, and contractor performance of DoD activities, is a key component in this planning effort. Choosing the wrong total force mix can put the mission at risk or result in inefficiencies that consume scarce defense resources. In the cyber arena, the problem is complicated by a lack of legal framework for determining which roles include direct participation in hostilities (DPH), and should, by law, be performed by military personnel. Faced with these challenges, DoD asked IDA to assess the current and projected total force mix for the CMF and, if possible, suggest alternative staffing plans.

## Process

In general, any manpower requirement can be classified into one of three categories:

- **Military Essential:** Military essentiality is governed by DoD Instruction (DoDI) 1100.22, which identifies five criteria for designating a requirement as military essential: (1) military-unique knowledge or skills are required; (2) military incumbency is required by law, Executive Order, treaty, or international agreement (e.g., DPH); (3) military performance is required for command and control, risk mitigation, or esprit de corps; (4) military manpower is needed to provide for overseas and sea-to-shore rotation, career development, or wartime assignment; and (5) unusual working conditions or costs are not conducive to civilian employment.
- **Inherently Governmental:** The definition of *inherently governmental* is found in the Office of Management and Budget's Office of Federal Procurement Policy Letter 11-01 and

is built around the well-established statutory definition in the Federal Activities Inventory Reform Act of 1998 as "a function so intimately related to the public interest as to require performance by Federal Government employees."

- **Non-Governmental Commercial Activity:** Activities that are not military essential or inherently governmental are considered commercial in nature.

Military essential requirements must be filled with military personnel. Any manpower requirement that does not meet these criteria shall be designated for *civilian performance* if the requirement is inherently governmental or subject to least-cost civilian or *contractor performance* if the requirement is a non-governmental commercial activity. There is room for interpretation in determining which roles should fall into which category. These determinations should not be made lightly. Using military personnel for roles that are not truly military essential can be costly, both financially (military personnel are generally more expensive than their civilian counterparts) and manpower-wise (military personnel performing non-military essential roles still count against the total authorized end-strength).

IDA's research focused on studying the CMF mission to determine which roles should be considered military essential, inherently governmental, or commercial activities open to the least costly performance type (civilian or contractor). To understand the CMF mission requirements, we studied existing DoD cyberspace strategies, doctrine, and current concepts of operation and employment for CMF.

A central element of IDA's methodology was to determine those positions that involve direct participation in cyber hostilities, which are deemed military essential. Criteria involving the intention to cause harm and the existence of a causal link between the actions of a billet holder and the infliction of damage were used. Upon this determination, the researcher team developed an alternative force mix that satisfied the staffing criteria as economically as possible. The researchers calculated the full costs of military, civilian, and contractor personnel for each Service's current force mix and an IDA-developed alternative.

## Findings

Staffing targets for CMF teams were put forth in the Chairman of the Joint Chiefs of Staff's Action Memorandum to the Secretary of Defense. (Chairman of the Joint Chiefs of Joint Staff 2012) Only the Army developed a staffing plan that strictly followed the workforce mix recommended in the memorandum. The other three Services viewed the recommended workforce mix as planning guidance. Their actual staffing plans reflected what they thought was the best force mix for their CMF teams.

The five CMF teams are (1) the National Mission Team, (2) the Combat Mission Team, (3) the National Support Team, (4) the Combat Support Team, and (5) the Cyber Protection

Team. The staffing mixes employed by each Service for the five teams are presented below along with the alternative staffing plan produced by the IDA analysis.[1] A description of the roles performed by each team can be found in our full-length report. (Barth, et al. August 2016)

Each Service's **National Mission Team** employs just under 60 personnel. While all four Services used a similar share of military officers, the use of enlisted military, civilians, and contractors varied. The Navy used the fewest civilians, while the Marine Corps (USMC) employed the most. IDA's alternative mix for the National Mission Team (shown in Figure 1) featured the fewest military personnel (primarily through reducing the number of enlisted) and more civilians.

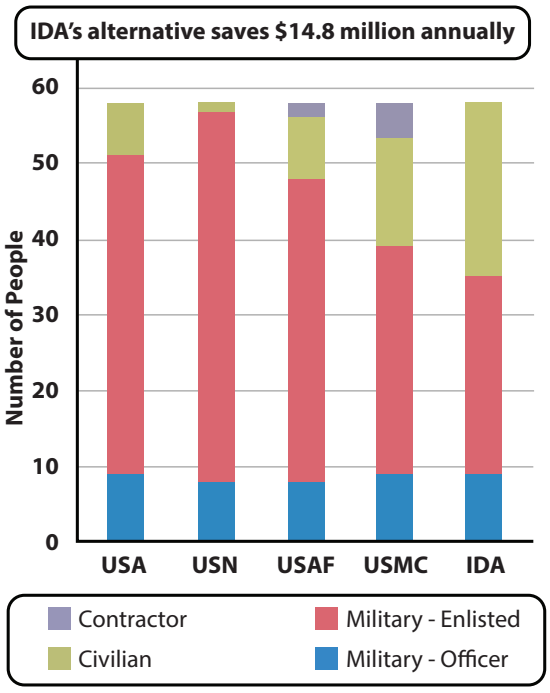



Figure 1. National Mission Team Composition

The **Combat Mission Teams** were also composed of approximately 60 personnel. As with the National Mission Teams, all four Services used a similar share of military officers. The use of enlisted military, civilians, and contractors varied (with the USMC again employing the most civilian-intensive mix). IDA's alternative mix for the Combat Mission Team (shown in Figure 2) featured the fewest military personnel (primarily through reducing the number of enlisted) and more civilians.

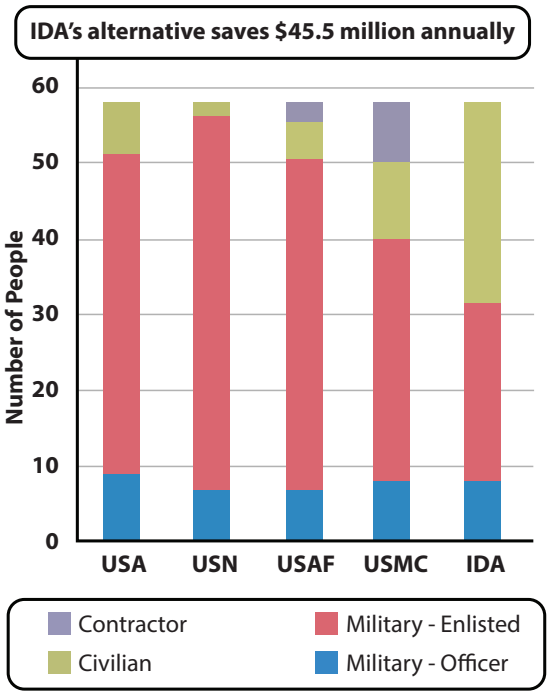
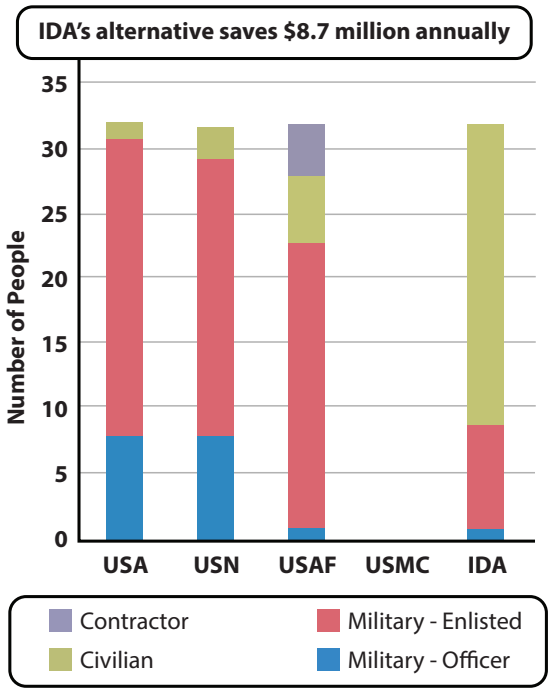



Figure 2. Combat Mission Team Composition

The **National Support Teams** were smaller in size (just over 30 personnel). The Air Force used significantly fewer military personnel when compared to the Army and Navy (the USMC had no

[1] While IDA did determine certain roles were non-governmental commercial activities, contractors are not featured in the IDA alternative CMF team force mixes, as they were found to be more costly than government civilians.

team). The IDA alternative (shown in Figure 3) maintained a military officer mix similar to that of the Air Force, but greatly reduced enlisted personnel in favor of civilians.




**Note: The USMC does not have an NST.**

Figure 3. National Support Team Composition

The **Combat Support Teams** were made up of approximately 35 personnel. The force mix employed by each Service varied greatly. The Army and Navy teams were primarily military (although they varied in their officer/enlisted mix, with the Navy employing a much higher share of officers). The Air Force and USMC teams included a higher share of civilians and contractors, while the IDA alternative (shown in Figure 4) employed the fewest military personnel.

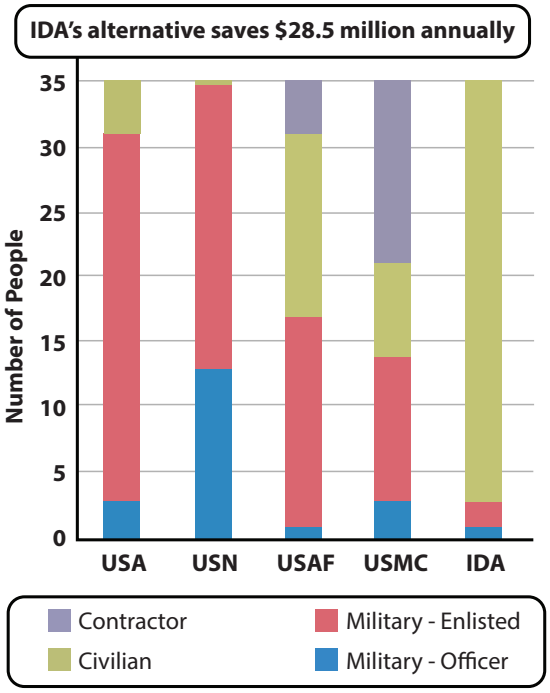



Figure 4. Combat Support Team Composition

The makeup of the **Cyber Protection Teams** also varied by Service. The Army and Navy again had a more military-intensive mix than the Air Force or USMC, and the IDA mix (shown in Figure 5) featured the highest civilian share.

To understand the budgetary implications of the various force mixes, we calculated the full cost of manpower for each Cyber Team using the total force mix employed by the Services (all Services combined) and the IDA alternative force mix (replacing each Service's current mix with the IDA alternative). The costing was performed in accordance with guidance and cost elements laid out in DoDI 7041.04. (DoD Instruction 7041.04 July 3, 2013)

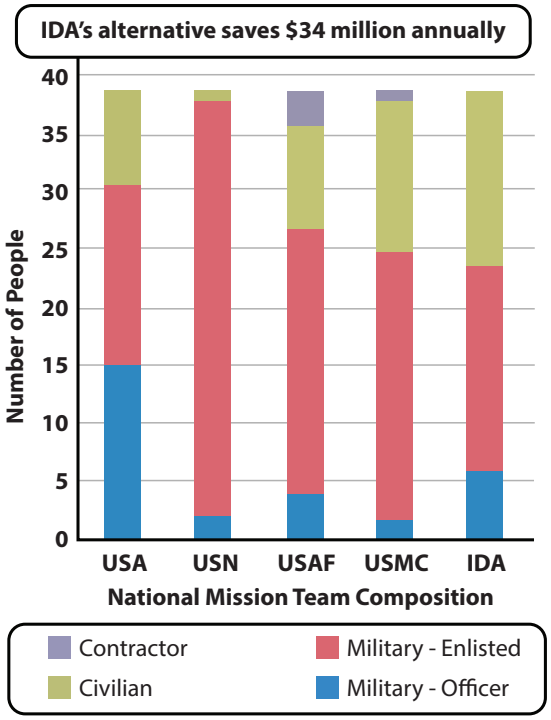



Figure 5. Cyber Protection Team Composition

## Conclusions and Recommendations

The IDA CMF staffing analysis concluded that a more civilian-intensive force mix could save the DoD approximately $130 million annually while maintaining compliance with DoDI 1100.22. Below we discuss some potential caveats to this analysis and make two recommendations for improving DoD's ability to assess the optimal total force mix.

### Develop a Legal Framework for Determining Combatants in Cyberspace Operations

As part of this analysis, the IDA team developed a protocol based on DPH to guide its determination of what billets require military personnel. This analysis was required because DoD currently lacks a legal framework for determining CMF work roles that are direct participants in *cyberspace* hostilities. It would be prudent for DoD/U.S. Cyber Command (USCYBERCOM) to develop such a legal framework, informed by any existing Government legal opinions on the topic of DPH.[2]

Additionally, a closer comparison of the position descriptions with the actual work to be performed would result in better factual information on the nature of the positions. This would provide Service manpower planners with a better framework to guide cyberspace operations workforce mix assessments, much like they now have for considering kinetic combat operations.

### Evaluate CMF Team Effectiveness

During the research period, the Services had just started standing up their initial teams in the CMF. In the future, performance data will be essential for evaluating the levels of expertise, experience, and continuity needed in a team's work roles for the team to accomplish its mission. This information would inform decisions about civilian and military mix.

[2] We did not have access to such U.S. government legal positions for DPH or other legal matters relating to this research. This would most certainly be an area for detailed research and analysis.

## References


Barth, Thomas H., Jerome J. Burke, Mark F. Kaye, Drew Miller, Linda Wu, and Stanley A. Horowitz. August 2016. *Staffing for Cyberspace Operations.* IDA Paper P-5217, Institute for Defense Analyses, Alexandria, VA.

Chairman of the Joint Chiefs of Joint Staff. 2012. Action Memorandum to the Secretary of Defense, "JCS Tank on CYBERCOM Mission Manpower." 30 November 2012. Washington, D.C.: Joint Staff, December 5.

DoDI Instruction 1100.22. April 12, 2010. *Policy and Procedures for Determining Workforce Mix.*

DoDI Instruction 7041.04. July 3, 2013. *Estimating and Comparing the Full Costs of Civilian and Active Duty Military Manpower and Contract Support.*



Mr. Thomas Barth (left) is a Research Staff Member in IDA's Information Technology and Systems Division. He holds a Master of Arts in strategic studies from the U.S. Army War College and a Master of Arts in military art and science from the School of Advanced Military Studies, U.S. Command and General Staff College.

Mr. Stanley Horowitz (right) is an Assistant Director in IDA's Cost Analysis and Research Division. He holds a Master of Arts in economics from the University of Chicago.


# Identifying Enlisted Recruits With the Right Stuff to Perform Cyberspace Operations

Thomas Barth, Elizabeth McDaniel

**The Challenge: Identifying enlisted personnel for the cyberspace effects workforce is challenged by a shallow pool of candidates and steep qualifying and performance requirements. If the Army can identify recruits with the right attributes and potential, it can increase the number who pass lengthy and expensive advanced training.**

**There are only so many people with cyber skills to begin with. It may take ten years to grow the pool to a sufficient number of qualified candidates.**

According to the Department of Defense (DoD) Strategy for Operating in Cyberspace, "The development and retention of an exceptional cyberspace workforce is central to DoD's strategic success." (DoD Strategy for Operating in Cyberspace January 2011) The supply and demand imbalance has been well documented:

> *There are only so many people with cyber skills to begin with. It may take ten years to grow the pool to a sufficient number of qualified candidates. The pool for the DoD is especially shallow due to the requirements for U.S. citizenship, clean credit, and the ability to obtain a clearance. (Private sector security executive n.d.)*

DoD's cyberspace workforce comprises personnel assigned to the areas of cyberspace effects, cybersecurity, cyberspace IT, and portions of the Intelligence workforces. (DoD Directive 8140.01) Developing the cyberspace effects workforce, the "personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in and through cyberspace," (DoD Directive 8140.01) presents a particularly difficult set of challenges. To meet its requirements for the Cyber Mission Force (CMF) teams, a component of the cyber effects workforce, the Army is recruiting individuals to serve as cyber operations specialists, classified as military occupation specialty (MOS) 17C. Cyber operations specialists execute defensive and offensive cyberspace operations. Their duties include performing cyber-attacks and defenses; performing cyber intelligence, surveillance, and reconnaissance actions on specified systems and networks; conducting network terrain audits, penetration testing, basic digital forensics data analysis, and software threat analysis; reacting to cyberspace events; employing cyberspace defense

infrastructure capabilities; collecting basic digital forensics data; providing incident response impact assessments; and producing network security posture assessments. The training process for cyber operations specialists requires the successful completion of 10 weeks of Basic Combat Training and two phases of Advanced Individual Training (AIT), plus an additional 45 weeks of intense technical cyber training. (U.S. Army 2017)

The funnel below illustrates the challenge facing the Army in identifying and recruiting a pool of enlisted personnel who can complete successfully the intensive training process and join its cyber mission teams as qualified cyber operations specialists.

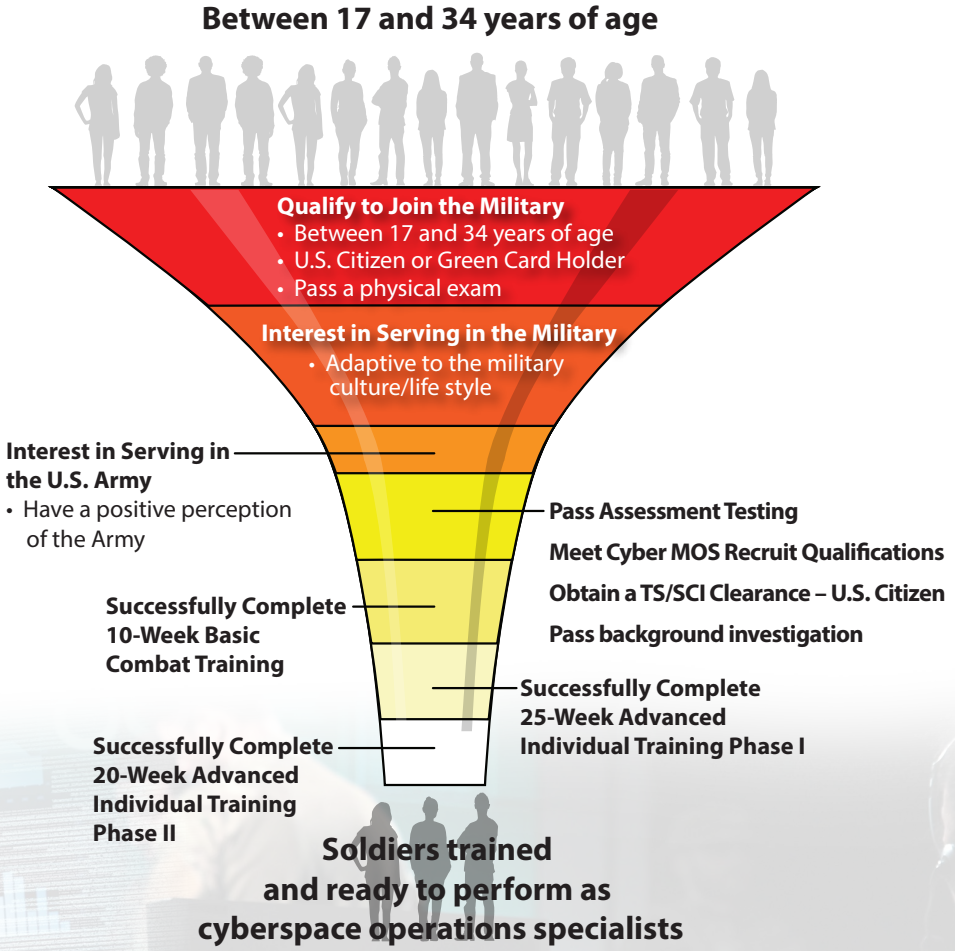
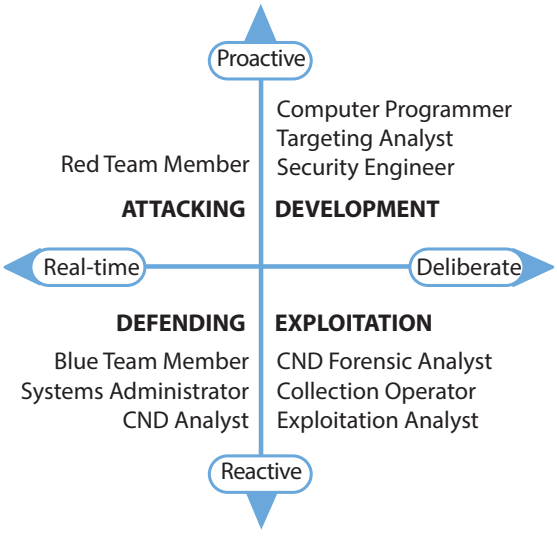



Figure 1. A Notional Funnel to Illustrate the Army's Challenge in Identifying and Training the Enlisted Recruits for Cyberspace Operations Roles.

## Efforts to Assess the Aptitudes of Recruits for the Cyber Workforce

Since the 1940s, the U.S. Armed Services have explored the use of personality variables as predictors of performance. At a Military Entrance Processing Station (MEPS), a prospective recruit currently takes a battery of tests to assess his or her general and specific knowledge and aptitude for a variety of MOSs. The Armed Services Vocational Aptitude Battery (ASVAB) qualifies applicants to enlist in the military and assigns them to particular jobs and fields. Its tests measure aptitudes in four domains: verbal, math, science and technical, and spatial. OCCU-Find, an inventory of work-related interests, is part of the ASVAB Career Exploration Program for recruits.

Since the 1950s, the Services have explored the relationships among work interest and preferences, motivation, identity, meaningfulness, sense of belonging, and work-related behavior. (Campbell, O'Rourke and Bunting 2015) The Cyber Test (CT), originally called the Information and Communication Technology Literacy (ICTL) Test, has been administered as an operational test to Service applicants since 2014. The intent of the CT is to assist DoD stakeholders in selecting and classifying enlisted personnel likely to be successful in training for a range of entry-level technology-related occupations. The CT is administered at MEPS on the ASVAB platform to Service applicants who wish to pursue select information technology (IT)/ cyber careers. The CT is modeled after an ASVAB information test (e.g., Electronics Information) and assesses basic computer literacy via knowledge-based multiple-choice questions in four fundamental areas: computer operations, networks, security and compliance, and software programming. The CT has demonstrated potential to improve the quality of applicants and reduce academic turnover in technical training for these demanding occupations. (Correspondence with Michael Ingerick 2017) The Cyber Aptitude and Talent Assessment (CATA), developed by the University of Maryland's Center for Advanced Study of Language (CASL), focuses on attributes with predictive value for cyber tasks. As illustrated in Figure 2, the roles are segmented to match the demands of particular tasks along two dimensions: proactive to responsive, and real-time to deliberate. (Campbell, O'Rourke and Bunting 2015)




CND = Computer Network Defense

Source: Campbell, O'Rourke and Bunting 2015

Figure 2. Cyber Roles Differ along Two Dimensions.

In 2016, CASL partnered with the Air Force to develop the AF-CATA, which focuses on critical thinking and other foundational abilities for success in cyber warfare operator training, including working memory and spatial visualization, as well as traits that predict operational job performance, like speed and vigilance. (Campbell, Identifying Untapped Talent 2017) The Canadian Armed Forces and the UK Ministry of Defence are currently using the Defence Cyber Aptitude Test developed by IBM to identify personnel with natural talent and the right skills for specific cyber positions. (Davies 2017)

Research continues on the predictive value of other assessments on attributes related to cyber roles. One is the Tailored Adaptive Personality Assessment System (TAPAS), which the Army has been administering at MEPS since 2009. Also, the U.S. Army Research Institute for the Behavioral and Social Sciences is developing the Common Cyber Capabilities Test, to measure the five to seven capabilities determined to be important to cyber work, and the Systems Thinking Assessment. (Wind 2017)

## Characteristics of Personnel Who Might Fill Cyber Roles

### Hackers, Red Teamers, and Pen Testers

In the media, the term "hacker" is used to describe a cybercriminal; however, the Army focuses on the ethical kind. Possessing exceptional talents, passions, and proclivities for highly specialized cyber roles, these skilled professionals know how to look for weaknesses in networks and/or computer systems. They are needed to maintain national security and protect our nation's critical infrastructure. They are characterized by high intelligence, consuming curiosity, and facility with intellectual pursuits. (Department of the Navy 2017)

Hackers called *Red Teamers*, or intrusion or pen (penetration) testers, conduct vulnerability probes of an organization's computer networks (with the organization's consent) to discover vulnerabilities and provide remedial solutions to make the networks and systems more secure and safe.

Ethical hackers are cyber security/effects professionals who demonstrate their skills as Red Team members or penetration testers in support of the mission of the organization. The Certified Ethical Hacker (CEH) certification can be earned through assessment of one's knowledge of the security of computer systems using penetration testing techniques. (EC-Council 2017)

### Cyber Warriors

Cyber warriors use cyber weapons, strategies, and technologies for nonmilitary ends such as cyber espionage. They tend to be well trained and educated, with approximately one half possessing at least a bachelor's degree. (Beard 2016) The Offensive Security Certified Professional (OSCP) is available only to those who conduct offensive operations and have passed specific training and a 24-hour online examination. (Offensive Security

2017) According to one private sector cyber executive, the OSCP is essential for acceptance as a colleague by some critical cyber operations teams.

Cyber warriors often demonstrate skills such as network traffic sniffing, packet analysis, network and system mapping, forensics, reverse engineering, binary analysis, and other such capabilities. (Andress and Winterfield 2014) In their capacity as warriors, their age and physical fitness are less critical than in traditional combat roles; however, they must be able to sit for long periods of time in front of computers. Mental factors such as maturity, intelligence, problem-solving skills, and creativity are highly valued, but among this population resistance to rules and authority figures may be common. They are intensely curious about how things work and can be made to fail. Cyber warriors, serving in critical roles, must demonstrate such qualities as self-control, empathy for the noncombatant population, temperance against the temptation to do what is expedient rather that what is right, discretion and discernment regarding privacy, and honor, among other attributes. (Beard 2016)

According to the authors of *The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce*, a key to force structure is finding educated people with a proclivity toward hacking. Interest and competence in science, technology, engineering, and mathematics (STEM) fields does not necessarily mean an individual might be a good cyber operator. Higher education is critical for success in performing some cyber warfare roles due to their reliance on theoretical as well as practical education. Graduate work develops the minds of individuals with technical aptitude to apply their knowledge of cyberspace to research, design, develop, test, and evaluate hardware, software, and firmware for the purpose of exploiting, defending, and attacking cyber and cyber physical systems. Training without education proved insufficient to assure mathematically complex, information-centric systems. If the Air Force identifies a candidate for a certain cyber operations role who has high aptitude or proclivity who lacks the required degree, such as a bachelor's degree in computer science, the Air Force might make an exception until the degree is earned. (Yannakgeorgos and Geis 2016)

## Continuing Efforts

The Army continues to investigate the link between aptitude, knowledge and skill, maturity, personality traits, and motivation with successful performance in cyber operations roles of new recruits and enlisted personnel already in the force. Further research is needed to link attributes identified by CT and CATA and the performance of personnel in cyber operations roles in the Army and other Military Services, as well as the predictive value of CT and performance in the Joint Cyber Analysis Course (JCAC) and the Army Research Institute's development of new instruments.

## References


Andress, J., and S. Winterfield. 2014. *Cyber Warfare, Second Edition: Techniques, Tactics, and Tools for Security Practitioners*. Waltham, MA: Elsevier.

Beard, M. 2016. "Beyond Tallinn: The Code of the Cyberwarrior?" In *Binary Bullets: The Ethics of Cyberwarfare*, edited by F. Allhof, A. Henschke and B. J. Strawser. New York: Oxford University Press.

Campbell, Susan G. 2017. "Identifying Untapped Talent for Cyber Warfare Operations Using a Cyber Aptitude and Talent Assessment," *NICE 2017 Spring eNewsletter*." https://www.nist.gov/itl/applied-cybersecurity/nice/nice-2017-spring-enewsletter#Featured.

Campbell, Susan G., Polly O'Rourke, and Michael F. Bunting. 2015. "Identifying Dimensions of Cyber Aptitude: The Design of the Cyber Aptitude and Talent Assessment." *Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting*.

2017. Correspondence with Michael Ingerick (The Human Resources Research Organization). September 5.

Davies, N. 2017. "Davies, N., "Cyber Aptitude in the Military," *Frontline Defence* 14 (3). http://defence.frontline.online/article/2017/3/7065-Cyber-Aptitude-in-the-Military.

Department of the Navy. 2017. "Credentialing Opportunities Online (COOL)." April 3. https://www.cool.navy.mil/

Department of Defense. 2017. "DoD Directive 8140.01, Cyberspace Workforce Management." July 31.

Department of Defense. 2011. "DoD Strategy for Operating in Cyberspace." January.

EC-Council. 2017. "Certified Ethical Hacking Certification." https://www.eccouncil.org/Certification/certified-ethical-hacker.

Offensive Security. 2017. "Offensive Security Certified Professional." https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/.

Private sector security executive, interview by IDA. n.d.

U.S. Army. 2017. "Careers & Jobs: Cyber Operations Specialist (17C)." August 22. https://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/computers-and-technology/cyber-operations-specialist.html.

Interview with Dr. Alexander P. Wind, Army Research Institute for Behavioral and Social Sciences. 21 January 2016.

Yannakogeorgos, P. A., and J. P. Geis. 2016. *The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce*. Maxwell Air Force Base, Alabama: Air University Press: Air Force Research Institute.



Mr. Thomas Barth is a Research Staff Member in IDA's Information Technology and Systems Division. He holds a Master of Arts in strategic studies from the U.S. Army War College and a Master of Arts in military art and science from the School of Advanced Military Studies, U.S. Command and General Staff College.

Dr. Elizabeth McDaniel is an Adjunct Research Staff Member in IDA's Information Technology and Systems Division. She holds a Doctor of Philosophy in education from the University of Miami.


# Air National Guard Cyber Force

Julia Warshafsky

**The Challenge: The Air National Guard has a capable foundational cyber force, but it still faces challenges to manning and sustaining its cyber career fields. Additionally, the scope of this force's roles for and authorized activities in domestic cyber efforts is not yet well-defined.**

**While working to man its cyber squadrons and ensure readiness for mobilizations to the Cyber Mission Force, the ANG has also been exploring ways to provide greater cyber support to state, local, tribal, and territorial entities.**

In late 2014, the Air National Guard (ANG) began efforts to stand up 15 new cyberspace squadrons to support the Air Force component of the Cyber Mission Force (CMF) under U.S. Cyber Command. While working to man its cyber squadrons and ensure readiness for mobilizations to the CMF, the ANG has also been exploring ways to provide greater cyber support to state, local, tribal, and territorial (SLTT) entities. However, continuing shortages of cyber talent, declining propensity and eligibility for U.S. military service, stringent CMF and ANG cyber personnel eligibility requirements, and ANG Recruiting's limited resources prompt ANG concern about its ability to sustain a skilled cyber force that continually meets the CMF's and the nation's demands in cyberspace. Moreover, laws and policies guiding ANG cyber support within SLTT communities are still evolving, and the ANG's roles and responsibilities for domestic cyber activities have not yet been clearly defined.

IDA identified challenges and opportunities for the ANG cyber force and provided recommendations to the ANG and National Guard Bureau (NGB) based on analysis of national cyber professional employment trends; ANG cyber career fields, missions, and recruiting and retention; and the force's potential to assist in various domestic cyber efforts.

## National Demand for Cyber Talent

Existing literature on cyber professional employment confirms that the nationwide demand for cyber talent is high and outstrips available supply, and that it will continue to do so as the need for cyber personnel continues to grow. This situation creates a shortage of qualified cyber professionals that the ANG can recruit. Some sources conclude that the difficulty of finding qualified cyber professionals will eventually subside, predicting that the supply of cyber talent will increase and adoption of automation technologies will reduce demand for human professionals, but these sources still agree that this stabilization

will not occur any time soon. (Libicki, Senty and Pollack 2014) (Vizard 2016)

We investigated the people who could potentially be *trained* to become ANG cyber personnel. Bureau of Labor Statistics data show that more than 5.6 million people, not including military members, federal employees outside the executive branch, or recent degree- or certificate-holders, are employed in computer, math, and engineering jobs nationwide. While there may be well more than 5 million people whose education and experience indicate that they could possibly be trained to become part-time cyber personnel to fill 1,065 ANG CMF positions, the potential supply pool quickly begins to shrink when the requirements for military service and, specifically, for military service in ANG cyber positions are taken into account.

## Downward Trend in Military Service Propensity and Eligibility

The population of individuals who are both interested in and eligible for U.S. military service has been declining over the last two decades. Some of the factors for this are the declining veteran population (knowing someone who has been in the military is highly correlated with accession), false perceptions of the military, increasing propensity of high schoolers to attend college, and increasing disqualification for more than one reason (such as obesity, drug use, criminal activity, financial problems, certain tattoos and piercings, physical and medical conditions, and low scoring on the Armed Forces Qualification Test). At the same time that the pool of prospective recruits to the military is shrinking, the Services' need for greater numbers of specialized, technical talent has grown with the stand-up of the CMF and diversifying global cyber threats.

## ANG Cyber Personnel Eligibility Requirements

Specific eligibility requirements for personnel to join an ANG cyber squadron further reduce the already limited pool of potential ANG recruits. ANG cyber personnel must complete basic military training if they have not previously served in the military, obtain a TS/SCI security clearance, and typically reside within a 50-mile radius of a squadron location. This last requirement poses additional challenges to sustaining a first-rate ANG cyber force, as some of the ANG's 15 new cyberspace squadrons, shown in Figure 1, are located in areas that do not appear to have large technical or cyber talent markets.

Depending on their specialty, assigned squadron, and whether they have prior cyber experience in an active component, ANG cyber personnel must complete anywhere from 17 to 100 weeks of technical training. Although all ANG members must be willing to commit at least one weekend per month and two weeks per year to the ANG on top of their full-time civilian employment, ANG cyber personnel must commit to an additional 6-month mobilization every three years to support the CMF.

## ANG Recruiting

In this competitive cyber talent market, the ANG has no recruiters dedicated to hiring cyber personnel,

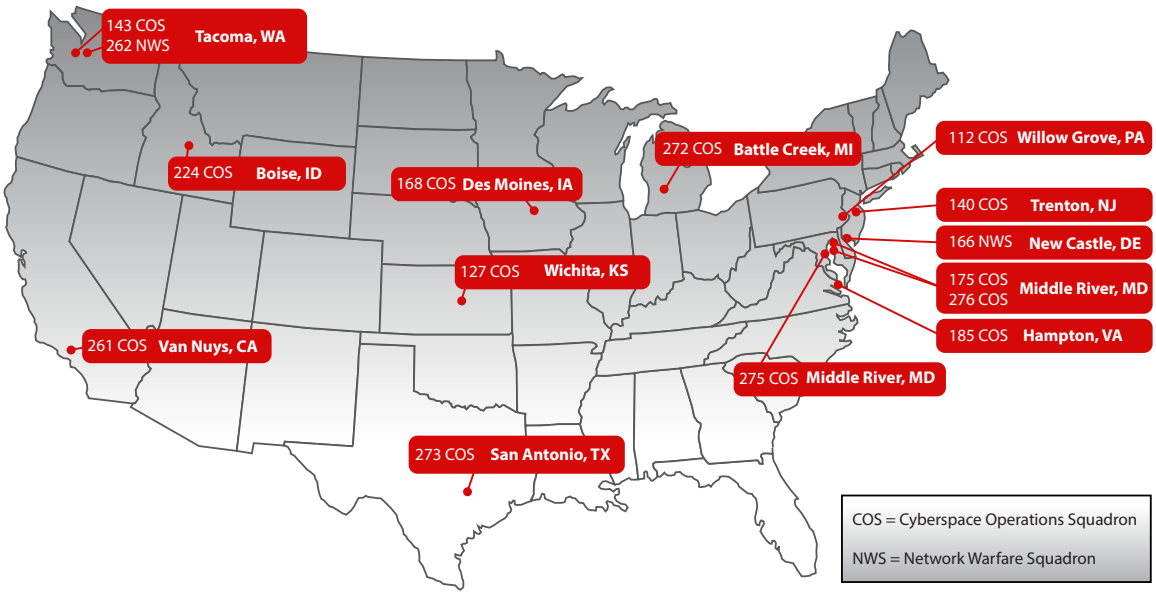



Figure 1. New Air National Guard Cyberspace Squadrons.

and ANG recruiters and staff lack adequate tools, technology, and resources to recruit specifically for cyber career fields, collect recruitment and retention data, and perform analyses of cyber workforce recruitment and retention. Because of the difficulty in finding non-prior service (NPS) personnel who can and are willing to meet the rigorous ANG cyber requirements, and the considerable time and cost involved in training NPS cyber recruits, the ANG fills its cyber positions largely by retraining current ANG members in other career fields or by recruiting personnel transferring from active duty who have had some level of cyber training. The active components are currently conducting pilot programs for the direct commissioning of recruits to cyber positions; however, similar pilot programs have not been authorized for the National Guard and Reserves.

## Developing the ANG Domestic Cyber Roles

While originally developed to support Title 10 CMF missions, the ANG's cyber squadrons have also been working with their respective state governors, adjutants general, emergency management agencies, and public utilities to address state and local cybersecurity challenges. In the past few years, ANG cyber personnel have assisted in a number of state responses to domestic cyber incidents—such as those coinciding with the civil unrest in 2014 in Ferguson, Missouri, and in 2015 in Baltimore, Maryland—and have provided cyber protection capabilities such as vulnerability assessments to several state entities. Various reports over the last few years have called for the government to increase use of the National Guard for such efforts, citing the Guard's

expanding cyber capabilities; ability to leverage private sector talent; tradition in building international, federal, and SLTT partnerships; and ability to operate under both state and federal authorities in three different duty statuses: State Active Duty, Title 32, and Title 10. However, laws and policies guiding ANG domestic cyber activities, in particular, are still evolving.

### Cyber Incident Response

To date, the government has focused primarily on outlining the National Guard's role in cyber incident response, specifically in support of civil authorities during or after a cyber event, consistent with the National Guard's historical role in disaster response. National Guard capabilities for cyber incident response are being incorporated into DoD's policies for Defense Support of Civil Authorities and the National Cyber Incident Response Plan developed by the Department of Homeland Security. Directive-Type Memorandum 17-007, *Interim Policy and Guidance for Defense Support to Cyber Incident Response* (DSCIR), released in June 2017, is the latest guidance on responsibilities and use of the National Guard and other DoD Components for DSCIR activities.

### Ongoing Cyber Protection

Less national-level focus has been devoted to how the National Guard could be used in an ongoing domestic cyber protection role. The May 2016 Deputy Secretary of Defense Policy Memorandum 16-002 offers the latest guidance on the National Guard's ability to coordinate with, train, advise, and assist mission partners in preventing, defending against, and recovering from cyber incidents. Although the memo is a step forward, it does not clearly establish the scope of the National Guard's authorized roles in advance of a domestic cyber incident or the specific actions the National Guard can undertake in cyberspace in Title 32 or State Active Duty status.

## Recommendations

IDA recommends that the NGB and ANG focus on acquiring improved tools for workforce data collection and analysis and on examining the impact of both traditional and new incentives on the recruitment and retention of cyber personnel. We also recommend that the NGB and ANG create plans for National Guard engagement in accomplishing governors' cybersecurity goals, collaborate with stakeholders to implement command and control constructs in response to domestic cyber incidents, and conduct pilot projects to enhance National Guard domestic cyber protection efforts.

The National Guard and its stakeholders should determine the national-level vision for the Guard's future roles and responsibilities in cyberspace. Today, the National Guard has limited capacity for domestic cyber activities. If it is to be increasingly called upon for domestic cyber support, a construct allowing it to balance domestic efforts and CMF mobilizations will need to be developed.

## References


115th Congress. 2017. Department of Defense Emergency Response Capabilities Database Enhancement Act of 2017, S. 307 and H.R. 1049.

Booz Allen Hamilton. 2015. *Cyber In-Security II: Closing the Federal Talent Gap.*

Burning Glass Technologies. 2015. "Job Market Intelligence: Cybersecurity Jobs, 2015."

Center for Strategic and International Studies. January 2017. *From Awareness to Action: A Cybersecurity Agenda for the 45th President.*

Commission on Enhancing National Cybersecurity. December 2016. "Report on Securing and Growing the Digital Economy." National Institute of Standards and Technology.

Council of Governors, Department of Homeland Security, and Department of Defense. 2014. "Joint Action Plan for State-Federal Unity of Effort on Cybersecurity." July.

Department of Defense. 2016. Deputy Secretary of Defense Policy Memorandum 16-002. "Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information Networks, Software, and Hardware for State Cyberspace Activities." May.

Evans, Karen, and Franklin Reeder. 2010. *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters,* CSIS Commission on Cybersecurity for the 44th Presidency, November 2010. Center for Strategic and International Studies.

Department of Defense. 2017. Directive-Type Memorandum 17-007. "Interim Policy and Guidance for Defense Support to Cyber Incident Response (DSCIR)." June.

Kosiak, Steven M. 2008. *Military Manpower for the Long Haul.* Center for Strategic and Budgetary Assessments.

Libicki, Martin C., David Senty, and Julia Pollack. 2014. *hacker5 Wanted: An Examination of the Cybersecurity Labor Market*. RAND Corporation.

Office of the Under Secretary of Defense, Personnel and Readiness. 2015. *Population Representation in the Military Services: Fiscal Year 2015 Summary Report.*

Orvis, Bruce R., Narayan Sastry, and Laurie L. McDonald. 1996. *Military Recruiting Outlook: Recent Trends in Enlistment Propensity and Conversion of Potential Enlisted Supply*. RAND.

Runey, Michael, and Charles Allen. 2015. "An All-Volunteer Force for Long-Term Success." *Military Review.*

Segal, David R., Jerald G. Bachman, Peter Freedman-Doan, and Patrick M. O'Malley. 1999. "Propensity to Serve in the U.S. Military: Temporal Trends and Subgroup Differences," *Armed Forces & Society.*

Soifer, Don, and Dan Goure. August 2016. "Six Principles for the National Guard's Cybersecurity Role Protecting the Grid." *In The National Interest.*

Vizard, Michael. 2016. "How Automation Will Affect Cybersecurity Jobs." *Dice Insights.*

Woodruff, Todd , Ryan Kelty, and David R. Segal. 2006. "Propensity to Serve and Motivation to Enlist among American Combat Soldiers." *Armed Forces & Society.*



Ms. Julia Warfshafsky is a Research Associate in IDA's Information Technology and Systems Division. She holds a Bachelor of Arts in political science and Spanish from the Pennsylvania State University, Schreyer Honors College.


# Modernizing Air Force Cybersecurity Test and Evaluation

Walter Rhoads

**The Challenge: The current U.S. Air Force workforce cannot support its current cybersecurity test and evaluation requirements. Yet those requirements are expected to increase as the demand for cybersecurity test and evaluation continues to grow.**

**The USAF should first seek to augment its workforce capability to support cybersecurity evaluations of systems either in or entering production.**

The United States Air Force (USAF) 46th Test Squadron (46 TS) asked IDA to structure a roadmap for workforce, infrastructure, and process cybersecurity test and evaluation (CSTE) modernization efforts. The effort provided a time-phased, cybersecurity test investment roadmap based on priority, cost, and technology maturity levels to support future airborne platform; weapons; and command, control, communications, computers, intelligence, surveillance, reconnaissance (C4ISR) cyber acquisition programs.

To assess the workforce requirements for CSTE modernization, IDA applied three methods using available data, empirical rules of thumb, and simple projections based on historical and planning data. The first method, which was the most rigorous, used a standard workforce planning model that assumed the data for each parameter in the formula was available, directly measured, and collected at the same time. The second method quantified expected demand and likely supply needs based on acquisition parameters and estimated life-cycle costs; this method relied on subject matter experts and planners who employed rules of thumb when developing concepts and rough order of magnitude cost estimates. The third method examined existing staffing levels, how the workforce was deployed and employed, and the 46th/DET's known portfolio of acquisitions and programs.

Each method was used to produce a demand forecast and supply forecast from which an assessment of workforce gaps was made. The detailed labor data for select individual events provided insight into the substantial number hours spent on travel, planning, and dry-run activities. For example, penetration activities for the Air Force Distributed Common Ground System (AF DCGS) comprised less than 20% of the 2,000 hours spent on this program; dry runs and reconnaissance accounted for 36%, and planning and travel accounted for 40%.

We found that the current USAF workforce has insufficient size and depth to support current or potential future CSTE requirements. The USAF CSTE workforce is currently structured to support Risk Management Framework (RMF) control

compliance evaluation for fielded systems and acquisition programs. These shortfalls are particularly acute for CSTE intended to support production and fielding decisions.

IDA recommends that the USAF pursue a spiral improvement program to augment, broaden, and deepen its CSTE workforce. These improvements should be phased to accomplish near-, mid-, and far-term objectives.

The USAF should first seek to augment its workforce capability to support cybersecurity evaluations of systems either in or entering production. This first step would involve (1) ensuring that the USAF CSTE workforce has professional certifications in all relevant disciplines and has all necessary clearances; (2) expanding the existing National Security Agency (NSA)-certified threat portrayal team capabilities; and (3) integrating system subject matter experts in Aircraft and Weapons (A&W) and C4ISR systems, including industrial control systems.

To develop an augmented, robust threat portrayal capability in a low-cost, expedited manner, IDA recommends that the USAF develop teaming arrangements among the Threat System Management Office (TSMO), the 57 Information Aggressor Squadron (IAS), the 177 IAS, and the 46 TS. A teaming arrangement will substantially reduce the USAF costs because TSMO reports that establishing an NSA-certified threat portrayal team can take 4 to 5 years, cost $3 million, and involve annual maintenance costs of $2 million. Furthermore, they report that developing appropriately trained government leads may require at least 18 months.

To meet mid- and long-term objectives, IDA recommends that the USAF expand its civilian workforce with dedicated subject matter expertise in threats, weapon systems, and operational environments. Consistent with this recommendation, the USAF should establish a comprehensive workforce solution that is designed to build domain expertise through training, outreach, and direct experience.

We further recommend that the USAF develop a joint community of interest among the following organizations: 92 Information Operations Squadron (IOS), 57 IAS, 177 IAS, the Army Research Laboratory's Survivability and Lethality Analysis Directorate, and the Naval Systems Command Cyber Warfare Directorate.

Implicit in the foregoing recommendation is a need to retain a skilled workforce through development, training, and financial compensation incentives.

The 46 TS is now implementing IDA's recommendations.

Mr. Walter Rhoads in an Adjunct Research Staff member in IDA's Information Technology and Systems Division. He holds a Master of Science in systems analysis and management from the University of Southern California.

# Past Issues

## Multidisciplinary Research for Securing the Homeland – IDA and DHS: Beyond 15

- Countering Terrorism One Technology at a Time
- Does Imposing Consequences Deter Attempted Illegal Entry into the United States?
- Improving Shared Understanding of National Security and Emergency Preparedness Communications
- Foreign Counter-Unmanned Aerial Systems: Developments in the International Arms Market
- Operationalizing Cyber Security Risk Assessments for the Dams Sector
- Understanding the Juvenile Migrant Surge from Central America
- Implementing a Roadmap for Critical Infrastructure Security and Resilience
- Baselining: Application of Qualitative Methodology for Quantitative Assessment of Emergency Management Capabilities
- Analysis, Analysis Practices, and Implications for Modeling and Simulation
- Test and Evaluation for Reliability

## Acquisition, Part 2: Executing and Managing Programs

- Cost Growth, Acquisition Policy, and Budget Climate
- Improving Predictive Value of Poor Performance
- Root Cause Analysis of VTUAV Fire Scout's Nunn-McCurdy Breach
- Evaluating Solid Rocket Motor Industrial Base Consolidation Scenarios
- Managing Supply Chain Cyber Risks To DoD Systems and Networks
- Looking Back at PortOpt: An Acquisition Portfolio Optimization Tool
- Predicting the Effect of Schedule on Cost
- Recent Developments in the Joint Strike Fighter Durability Testing

## Test and Evaluation: Statistical Methods for Better System Assessments

- Assessing Submarine Sonar Performance Using Statistically Designed Tests
- Applying Advanced Statistical Analysis to Helicopter Missile Targeting Systems
- Tackling Complex Problems: IDA's Analyses of the AN/TPQ-53 Counterfire Radar
- Improving Reliability Estimates with Bayesian Hierarchical Models
- Managing Risks: Statistically Principled Approaches to Combat Helmet Testing
- Validating the Probability of Raid Annihilation Test Bed Using a Statistical Approach

## Technological Innovation for National Security

- Acquisition in a Global Technology Environment
- Lessons on Defense R&D Management
- Commercial Industry R&D Best Practices
- Strengthening Department of Defense Laboratories
- Policies of Federal Security Laboratories
- The Civilian Science and Engineering Workforce in Defense Laboratories
- Technology Transfer: DoD Practices

## Acquisition, Part 1: Starting Viable Programs

- Defining Acquisition Trade Space Through "DERIVE"
- Supporting Acquisition Decisions in Air Mobility
- Assessing Reliability with Limited Flight Testing
- Promise and Limitations of Software Defined Radios
- Implications of Contractor Working Capital on Contract Pricing and Financing
- The Mechanisms and Value of Competition
- Early Management of Acquisition Programs

## Security in Africa

- Trends in Africa Provide Reasons for Optimism
- China's Soft Power Strategy in Africa
- Sudan on a Precipice
- A New Threat: Radicalized Somali-American Youth
- Chinese Arms Sales to Africa

## Challenges in Cyberspace

- Cyberspace – The Fifth and Dominant Operational Domain
- Transitioning to Secure Web-Based Standards
- Information Assurance Assessments for Fielded Systems During Combat Command Exercises
- Supplier-Supply Chain Risk Management
- Internet-Derived Targeting: Trends and Technology Forecasting
- Training the DoD Cybersecurity Workforce

IDA | RESEARCH NOTES



4850 Mark Center Drive • Alexandria, VA 22311-1882
ida.org

@IDA_org