Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

PERSPECTIVES ON BUILDING A CYBER FORCE STRUCTURE

Stuart STARR[a,1], Daniel KUEHL[b,2], Terry PUDAS[c,3]

[a]*Center for Technology and National Security Policy (CTNSP), Washington, DC, USA*
[b]*iCollege of the NDU. Washington, DC, USA*
[c]*CTNSP, NDU, Washington, DC, USA*

Abstract: This paper explores the US's cyber force structure with special emphasis on the cyber workforce. To achieve that goal, this paper addresses several issues: it characterizes the nature of the cyber security problem; it draws on insights from senior decision-makers to identify cyber force structure needs; it characterizes current capabilities by summarizing the key initiatives that are being pursued by the US Services and key joint activities; and it identifies a spectrum of actions to mitigate shortfalls in the existing cyber forces structure (i.e. education; higher education and recruitment; certification, retention, professional development, and workforce management; exercises; and security clearance requirements). The paper concludes by identifying actions that NATO might pursue to improve its cyber force structure (e.g. conduct realistic, stressful exercises) and by identifying residual issues to address (e.g. career progression; value of employing "patriotic hackers").

Keywords: cyber workforce; cyber needs; cyber capabilities; residual cyber issues.

Disclaimer: The views expressed in this article are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U. S. Government. All information and sources for this paper were drawn from unclassified material.

1 Fort Lesley J. McNair, Washington, DC, USA; email: StarrS@ndu.edu.
2 Fort Lesley J. McNair, Washington, DC, USA; email: KuehlD@ndu.edu.
3 Fort Lesley J. McNair, Washington, DC, USA; email: PudasT@ndu.edu.

INTRODUCTION

The goal of this paper is to explore the US's cyber force structure with special emphasis on the cyber workforce. To achieve that goal, this paper addresses five objectives. First, it characterizes the nature of the cyber security problem. Second, it draws on insights from senior decision-makers to identify cyber force structure needs. Third, it characterizes current capabilities by summarizing the key initiatives that are being pursued by the US Services and key joint activities. Fourth, it identifies a spectrum of actions to mitigate shortfalls in the existing cyber forces structure. The paper concludes by identifying actions that NATO might pursue to improve its cyber force structure and by identifying residual issues to address.

In order to realize that goal and the subordinate objectives, this paper has employed several key sources. One of the primary sources was the conference on Cyber Force Structure that was convened at the National Defense University (NDU) in the fall of 2009. That source is complemented by White House initiatives on cyber security, testimony that was presented to the US Congress, and the results of several studies that addressed key cyber security and cyber force issues.

1. NATURE OF THE PROBLEM

Recently, ADM Dennis Blair (USN, ret.), Director of National Intelligence, presented the "Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence" (Blair 2010). In that testimony, ADM Blair cited the "far-reaching impact of the cyber threat" as the primary threat facing the US. In support of that statement, ADM Blair made the following observations. He noted that "Neither the US Government nor the private sector can fully control or protect the country's information infrastructure." In particular, he noted that the "The cyber criminal sector in particular has displayed remarkable technical innovation with an agility presently exceeding the response capability of network defenders." He further observed that "Criminals are developing new, difficult-to-counter tools." and that in 2009, "we saw the development of self-modifying malware…". He concluded that "We cannot protect cyberspace without a coordinated and collaborative effort that incorporates both the US private sector and our international partners."

To support those observations, ADM Blair cited two global trends that are exacerbating the problem: network convergence and channel consolidation. Network convergence refers to the merging of distinct voice and data technologies to a point where all communications are transported over a common network structure. Channel consolidation refers to the concentration of data captured on individual users by service providers. He concluded that "… these trends pose potential threats to the

confidentiality, integrity and availability of critical infrastructures and of secure credentialing and identification technologies."

Similarly, FBI Director Robert S. Mueller III warned that the cyber terrorism threat is "real and ⋯ rapidly expanding" (Nakashima 2010a). In his remarks he recommended strongly that companies should tell the US government when their computer systems have been attacked.

2. KEY NEEDS

As a foundation for characterizing the cyber force structure, it is important to characterize the key needs that drive the cyber force. Unfortunately, that foundation does not yet exist. However, to contribute to that discussion, the following section draws on several key products to help build that foundation.

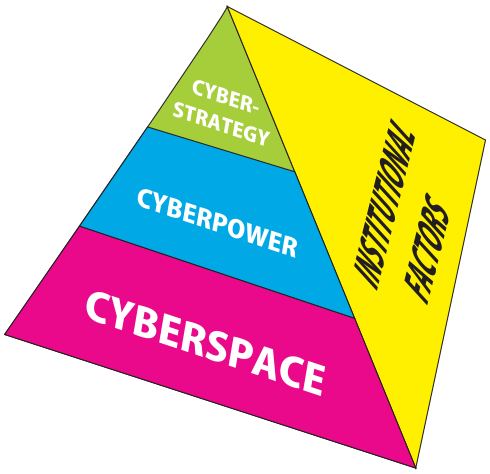

Figure 1. A Cyber Model

As an initial step, this section introduces a conceptual model that was presented in the NDU book, "Cyberpower and National Security" (Kramer, et. al., 2009). We characterize that model and identify the intellectual capital that is needed to implement that model. Second, we introduce the twelve initiatives that are subsumed within the White House's Comprehensive National Cybersecurity Initiative (CNCI) (available at www.whitehouse.gov/cyber security/comprehensive-national-cyber security-initiative). We then map those initiatives onto NDU's conceptual model to characterize the cyber force implications of those initiatives. Third, there is interest in the needs associated with a cyber attack capability. To address that issue, we

refer to the recent report that was issued by the National Research Council (NRC) on that issue (Owens, et. al., 2009). Finally, we anecdotally address the size of the cyber force by citing recent Department of Homeland Security (DHS) initiatives to hire cyber experts.

In analyzing the cyber domain, four key areas emerge (see Figure 1). These include the cyber-infrastructure ("cyberspace"), the levers of national power (i.e. diplomacy, information, military, economic, or "cyber power"), the degree to which key entities are empowered by changes in cyberspace ("cyber strategy"), and the institutional factors that affect the cyber domain (e.g. legal, governance, organization). For the purposes of this paper, this framework will be employed to decompose the problem.

Although the definitions of many of these terms are still contentious, this paper will use the following definitions for key terms. For the purposes of this theory, this white paper has adopted the formal definition of cyberspace that the Deputy Secretary of Defense formulated: "…the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries". (Deputy Secretary of Defense 2008). This definition does not explicitly deal with the information and cognitive dimensions of the problem. To deal with those aspects explicitly, we have introduced two complementary terms: cyber power and cyber strategy.

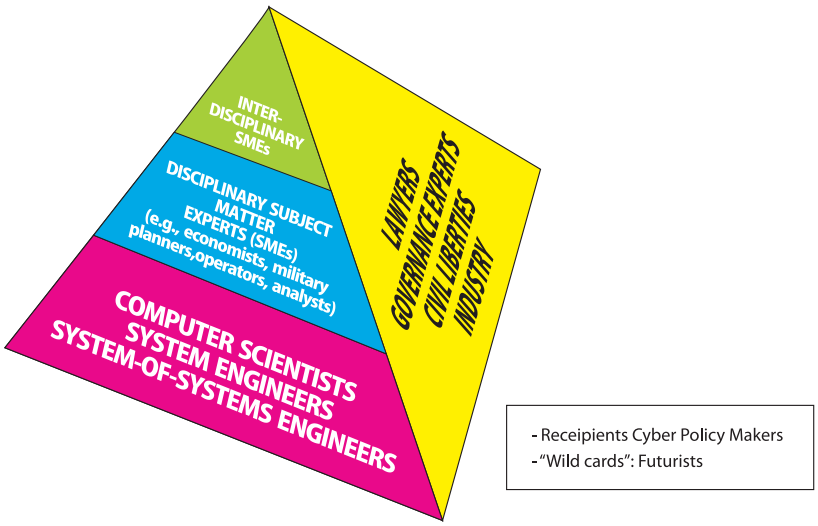

Figure 2. Required Intellectual Capital

This white paper has adopted the following definition for the term "cyber power". It is "the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power." In this context, the instruments of power include the elements of the Political/Diplomatic, Informational, Military, Economic (P/DIME paradigm).

Similarly, the term "cyber strategy" is defined as "the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power." Thus, one of the key issues associated with cyber strategy deals with the challenge of devising "tailored deterrence" to affect the behavior of the key entities empowered by developments in cyberspace.

Finally, the other facet of the pyramid considers a spectrum of related institutional factors. These include factors such as governance, legal, organizational, and public-private relationships.

Consistent with that framework, we make the following comments about the intellectual capital that is required for each of these layers (Figure 2).

In the area of cyberspace, we are interested in the intellectual capital that is required to deal with components of cyberspace through the interdependent networks of information technology. To meet that need, there is a requirement for highly capable, *inter alia,* computer scientists, system engineers, system administrators, and system-of-system engineers. It should be emphasized that these positions cannot be filled with recent graduates or novices. There is a need for a security cleared, highly trained, and competent cadre of cyber security professionals.

In the area of cyber power, there is a need for disciplinary subject matter experts (SMEs) that are able to assess the impact of the rapid changes in cyberspace on the factors of diplomacy, information, military, and economics. For example, military planners and operational analysts have employed live, virtual, and constructive models and simulations to establish that the addition of a digital link to airborne interceptors (AIs) from an AWACS aircraft will enhance the AIs Loss Exchange Ratios by a factor of 2.5 (Gonzales, et. al., 2005). Similarly, we need SMEs to determine the functional relationships between improvements in cyberspace and the other levers of power.

In the area of cyber strategy, we need SMEs who are conversant with the empowerment of key entities (e.g. terrorists, criminals, near-peers) that emerges from improvements in cyberspace. For example, (Kramer, et. al., 2009) observes that terrorists are being empowered by cyberspace in their ability to perform a variety of key, inter-related functions (e.g. recruit, raise resources, plan and command and control

operations, conduct influence operations, and educate and train). Key features of this empowerment include low cost of entry, world-wide reach, sanctuary, and the potential to link with transnational criminals. Of particular interest is the challenge in developing a theory of cyber deterrence. To further that debate, the NRC is conducting a competition to address fifty-one questions associated with cyber deterrence (NRC 2010).

Finally, in the area of institutional factors, we need a broad set of legal, governance, and private sector experts. These include, *inter alia*, lawyers (who are conversant with cyberwar and proportional responses, differences in international versus sovereign law), governance experts (who can assess the impact of the new contract with Internet Corporation for Assigned Names and Numbers (ICANN)), and the private sector (which controls on the order of 85% of the elements of critical infrastructure).

Overall, there is a need for cyber policymakers who can synthesize these insights into coherent, meaningful policy positions. As an aside, policymakers have found it useful to have futurists who can speculate meaningfully about future directions in each level of the pyramid.

Over the last few years, the White House has aggressively supported the CNCI (Reference 5). These initiatives were begun in the administration of President George W. Bush and re-evaluated by President Barak Obama. The key features of these initiatives are summarized briefly in Table 1.

#	Initiative
1	Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections (TICs)
2	Deploy an intrusion detection system of sensors across the Federal enterprise
3	Pursue deployment of intrusion prevention systems across the Federal enterprise
4	Coordinate and redirect R&D efforts
5	Connect current cyber ops centers to enhance situational awareness
6	Develop and implement a government-wide cyber counterintelligence plan
7	Increase the security of our classified networks
8	Expand cyber education
9	Define and develop enduring “leap-ahead” technology, strategies, and programs
10	Define and develop enduring deterrence strategies and programs
11	Develop a multi-pronged approach for global supply chain risk management
12	Define the Federal role for extending cybersecurity into critical infrastructure domains

Table 1. Comprehensive National Cyber Security Initiatives

To understand the key needs associated with these initiatives, these initiatives have been mapped into the cyber “pyramid”, cited above (Table 2).

As can been seen in Table 2, we have postulated that the bulk of the CNCI initiatives are associated with cyberspace. In addition, two of the issues are associated with cyber strategy (i.e. develop a Counter Intelligence plan; develop deterrence strategies) and one is associated with institutional factors (e.g. extend cyber security into critical infrastructures domains). We have noted that initiative 8, expand cyber education, is germane to all four areas of interest. Initiative 8 identifies two key challenges. First, there are not enough cyber security experts within the Federal Government or the private sector. Second, it notes that there is not an adequately established Federal cyber security career field. To deal with those challenges, the CNCI has identified two key needs. First, there is a need to develop a technologically skilled and cyber-savvy workforce. In addition, it calls for the creation of an effective pipeline of future employees. Ultimately, there is a requirement for a national strategy on the issue.

Area	CNCI
Cyberspace*	• (#1) Manage Federal Enterprise Network as a single network enterprise • (#2) Develop intrusion detection system • (#3) Develop intrusion prevention system • (#4) Redirect Research & Development • (#5) Connect cyber centers for situational awareness • (#7) Increase security of classified networks • (#9) Develop "leap ahead" technologies • (#11) Manage global supply chain risk
Cyberpower*	
Cyberstrategy*	• (#6) Develop Counter Intelligence plan • (#10) Develop deterrence strategies
Institutional Factors*	• (#12) Extend cybersecurity into critical infrastructure domains

* (#8) Expand cyber education

Table 2. Mapping the CNCI onto the Cyber Model

In addition, the NRC (Owens, et. al., 2009) recently issued a paper that focused on the cyber force needs associated with cyber attack. Cyber attack refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks.

They formulated several key needs to foster a national debate on cyber attack. They concluded the following: "The US should establish a public national policy regarding

cyber attack for all sectors of government···; the US government should conduct a broad, unclassified national debate and discussion about cyber attack policy···; and the US government should work to find common ground with other nations regarding cyber attack."

Subsequently, in the section entitled "Supporting Cyber attack Capabilities and Policy", the NRC report formulated the following recommendation: "The US government should ensure that there are sufficient levels of personnel trained in all dimensions of cyber attack and the senior leaders of government have more than a nodding acquaintance with such issues."

One of the major issues associated with the cyber force need is the number of professionals that are required by it. Recently, the Department of Homeland Security (DHS) cited that it was attempting to recruit 1000 cyber specialists over the next 3 years (Nakashima&Krebs 2009)]. However, a respected subject expert on the subject, Jim Gosler, Sandia National Laboratory, postulated that nearly 20,000 to 30,000 cyber specialists would be needed to protect military, government, and private sector networks (Gosler 2010). This suggests that an enormous amount of intellectual capital will be needed to respond to the US's needs.

3. CURRENT CAPABILITIES

The Services – Army, Navy, Air Force and Marine Corps – are all taking unique and Service-specific organizational and doctrinal approaches to cyberspace. This is understandable and not necessarily bad, in that it will create more opportunities and diverse concepts for the development and even employment of cyber capabilities. This mirrors the situation in the other domains and functional environments and in that sense provides a greater menu of choices for the joint force commander to use. The drawbacks center on three potential developments. First is the possibility that there will be wasteful and unnecessary duplication of effort, which becomes even more likely with highly classified and special access programs. Second is the distinct possibility that some Service-specific capabilities will not mesh or be interoperable with other Services' programs and systems. Third, if everyone is defining cyber through the lenses of existing domains—air, land, sea, and outer space—it begs the question whether anyone is looking at cyber through a primarily cyber lens. This was the argument behind the creation of "air forces" during the period of World Wars I and II, but it also raises the question of whether military cyberspace needs its own "Billy Mitchell".

3.1 UNITED STATES AIR FORCE (USAF)

The Air Force may have been the most "visionary" Service, and its publication in 1995 of "Cornerstones of Information Warfare" signed by the then-Chief of Staff General Ron Fogelman and Secretary of the Air Force Sheila Widnall marked a key point in the Air Force's conceptual development of cyber capability (Fobelman&Widnall 1995). In 2007 the Air Force publicized its planned establishment of an Air Force Cyber Command, to stand alongside its Commands for Air Combat and Space operations. But this was widely and loudly assailed by the other Services, which saw this as a grab for "cyber turf", and as a result the Air Force modified its plan. The Air Force's organizational approach now centers on its recent creation of a numbered air force – the 24th Air Force, headquartered in San Antonio – as a component element under the Air Force Space Command (Axe 2009). There is a technical logic to this, as a tremendous amount of the Air Force's and the entire DOD's cyber connectivity resides on space-based platforms. The 24th AF's mission is to provide cyber support to the warfighter. This includes cyber situational awareness; freedom of action for friendly forces in the cyber domain; synchronization of network operations; and enabling effects in/through/from cyberspace. (Webber 2009) Functionally, these include information operations, combat communications, and network warfare. In 2007 the USAF's Scientific Advisory Board published a report on operations in a "cyber-contested" environment, which included a definition of cyberspace that included the entire electromagnetic spectrum (EMS) as the cyber domain. While this approach agrees with that used in the recent "Cyberpower and National Security" book written at the National Defense University (Franklin, et. al., 2009), the inclusion of the EMS makes it different from and more inclusive than the official DOD definition. The Air Force has a doctrine for cyberspace operations in draft, Air Force Doctrine Document 2-11, but it has remained in draft for more than two years, and prospects for a rapid issuance seem slim (Air Force Doctrine Center 2008).

3.2 UNITED STATES NAVY (USN)

The USN has also taken organizational steps to create its needed cyber capabilities. In 2006 the Chief of Naval Operations tasked his Strategic Studies Group at the Naval War College to study the implications cyberspace posed for the Navy, and they issued their report in 2007. The SSG saw cyberspace as a primary warfare area for the Navy, which would impact virtually everything the Navy does. As did the Air Force, cyberspace is driving an increasing integration of intelligence and communications, organizationally as well as operationally. In 2009 the Secretary of the Navy issued instructions designed to establish Navy-wide policy for the creation of cyber capabilities and organizations. Its intent was to insure the security and functionality of Navy supply and logistics chains, command and control systems, and

assure freedom of action in cyberspace. (Department of the Navy 2009) The Navy's most recent and important action was its recent activation of Fleet Cyber Command, with its operational element provided by the new 10th Fleet at Fort Meade, MD. The establishment in early 2010 of 10th Fleet headquarters at Fort Meade is an indication that this fleet's seas will not be liquid but rather cyber. While the Navy is still developing doctrine and concepts for the operational employment of cyberspace, this is not standing in the way of its use right now, and some have suggested that the Navy has the most effective approach. Fleet Cyber Command's most pressing needs include inspection, testing, situational awareness, operationally focused testing, use of talented people, and continuous monitoring of its networks, according to the 10th Fleet Commander, Vice-Admiral Bernard McCullough III (Montalbano 2010).

3.3 UNITED STATES ARMY (USA)

While the Army has not yet created an Army entity dedicated specifically to cyber—unlike the Navy or Air Force—the Army's concept does envision the creation of an Army Cyber Forces Command that would have the Army's Intelligence and Security Command (INSCOM) and its Network Enterprise Technology Command (NETCOM) as its two key subordinate components. Within INSCOM is the Army 1st Information Operations Command, which draws heavily on the Army's signals and intelligence communities. The Army's Combined Arms Center (CAC) at Ft Leavenworth recently released its draft Cyber-Electronics Concept of Operations (CONOPS), which is taking a very broad look at what constitutes the cyber domain, what it means to warfighting and Army operations, and what we mean by the term "cyberwarfare". The U.S. Army Training and Doctrine Command (TRADOC) approved the Army's first official cyberspace operations concept on February 5, 2010. TRADOC Pamphlet (Pam) 525-7-8, The U.S. Army Concept Capability Plan (CCP) for Cyberspace Operations (CyberOps) 2016-2028 outlines the Army's vision for integrating cyberspace operations and the use of cyberspace into the commander's overall operations. This CCP forms the baseline for the on-going Cyber/Electromagnetic Contest Capabilities-Based Assessment (CBA) that will validate required capabilities and develop solutions to get the right capabilities to commanders and soldiers. TRADOC Pam 525-7-8 takes a comprehensive look at how the Army's future force in 2016-2028 will leverage cyberspace and CyberOps. This pamphlet includes a conceptual framework for integrating CyberOps into full-spectrum operations, thereby providing the basis for follow-on doctrine development efforts. This pamphlet also establishes a common lexicon for Army CyberOps, and describes the relationship between cyberspace, the other four domains (air, land, maritime, and space), and the EMS. Lastly, it explains how converging technologies will increasingly affect Foreign Service Officer and influence capability development, thereby enabling the Army to influence the design, development, acquisition, and employment of fully integrated cyber

capabilities[2]. The CAC is exploring the implications of this new domain and how it will shape the Army's future plans, organizations, and operations (Training and Doctrine Command 2010).

3.4 UNITED STATES MARINE CORPS (USMC)

The Marines are certainly not unaware of or indifferent to the criticality of cyberspace to USMC operations. The Marine Corps focus remains support to the Marine Air-Ground Task Force (MAGTF), which is accomplished through Marine Corps Network Operations Support Center (MCNOSC). The Marines established their Marine Corps Information Operations Center in July 2009. While the Marines have had an Information Operations doctrine for several years, they do not as yet have one for cyber. The Marines are the third Service to create a major organization focused specifically on cyber, with the creation in early 2010 of Marine Forces Cyber (MARFORCYBER), with a presence at Fort Meade. MARFORCYBER will be the Marine Corps' element of the as-yet-unestablished USCYBERCOMMAND and will be the USMC's spear point for operations in cyberspace. While the MCNOSC and MCIOC are separate organizations, they will be the two key components of MARFORCYBER. Some of MARFORCYBER's key activities and responsibilities are already well established, such as network operations and SIGINT, but the real challenge will be to develop the coordination between the "2" and "6" communities: communications and intelligence. It seems apparent that most USMC activities in cyberspace will concentrate on network operations and information assurance (Marine Corps 2003, Craft 2009, Marine Corps Headquarter 2010).

3.5 OTHER ACTIVITIES

There are two major cyber changes that are likely to affect the future of the cyber force structure: the creation of the US Cyber Command and the recent issuance of the Quadrennial Defense Report (QDR).

3.5.1 US Cyber Command

In June 2009 the Secretary of Defense issued instructions for the establishment of a joint command subordinate to US Strategic Command and devoted to the cyber mission (Gates 2009). US Cyber Command is to be headed by the Director of the National Security Agency and promoted to the rank of "General". He would thus be

2 A portion of this section has been published in the *Thoughts of a Technocrat* Blog on March 12, 2010 (http://djtechnocrat.blogspot.com/2010/03/us-army-cyberspace-operations-concept.html).

"dual hated", serving simultaneously as the Director, NSA (DIRNSA) and subordinate to the Secretary of Defense, and Commander US Cyber Command and subordinate to the Commander US Strategic Command. In the new organization, both the offensive (Joint Functional Component Command for Network Warfare (JFCC-NW)) and defensive (Joint Task Force – Global Network Operations (JTF-GNO)) organizations would be folded into it. The DOD has repeatedly stressed that its role would be to protect military, not civilian, networks. This proposal has raised significant issues in the US Congress (e.g. harmonizing civil liberties and national security) and as of this writing remains under discussion and not yet confirmed by the Congress.

3.5.2 Quadrennial Defense Review (QDR)

The 2010 version of the Quadrennial Defense Review (QDR) contained a substantial discussion of the criticality of cyberspace to U.S. military plans and operations, emphasizing the need to better secure the networks and systems that make up the Global Information Grid (GIG). The 2010 QDR identified three broad goals: freedom of action in cyberspace; prevention and deterrence of conflict; and cyber support to homeland defense. The QDR poses key questions with respect to the challenge of obtaining cyber deterrence and the relationship of cyber activities to the information environment. The QDR development effort had a sub-panel devoted specifically to the cyber issue, and it drafted a "cyber strategy" that focused on the goals cited here. Since one of the key impact areas of the QDR is on resources, the DOD and Services will inevitably be affected by the QDR in the dedication of scarce resources to create capabilities in the cyber domain. The QDR outlined four steps being taken to further develop DOD's cyber capabilities. First is the need to develop a comprehensive approach to the DOD's operations in cyberspace. The next is to develop further human expertise and broaden awareness of how much the U.S. military depends on cyberspace for real military capability. Third is the need to centralize command of cyber operations, which is the driving need behind the proposed establishment of USCYBERCOMMAND. Last is the need to further develop partnerships across the interagency and into the broader society and commercial sector (Departmemt of Defense 2010).

4. SELECTED ACTIONS TO MITIGATE SHORTFALLS

The authors of this paper believe that at least five recommendations should be implemented to mitigate existing shortfalls in the cyber force structure: education; higher education and recruitment; certification, retention, professional development and workforce management; exercises; and security clearance requirements. For

each of these recommendations, the following discussion characterizes the existing status and proposes recommendations to mitigate shortfalls.

4.1 EDUCATION

Currently, few public schools offer computer science courses due to lack of funding, qualified teachers, standards, and curriculum. Consequently, limited numbers of students study computer science at the high school or college level, and extremely few students enter the cyber workforce.

To mitigate this issue, it was recommended that we improve K-12 education. To implement this concept, we recommend that we provide formal training and set aside grants for K-12 instructors in computer science. In addition, it is important to institute standards for computer science in science, technology, engineering, and mathematics education and to make computer science courses available to middle and high school students. Although this recommendation does not directly affect the cyber pyramid, it provides the foundation for long-term cyber security.

4.2 HIGHER EDUCATION AND RECRUITMENT

Currently, Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) are dissatisfied with quality and quantity of computer security specialists.

With respect to *quality* they have observed that computer science programs are insufficiently staffed with qualified, experienced faculty. In addition, there is a significant disconnect between what universities are teaching and what the US government and private sector need.

With respect to *quantity* they have stated that educational institutions and the US government are not effectively recruiting talented youth for the cyber professions. Consequently, there is large base of potential talent that is not being tapped.

To deal with these issues, the authors propose the following recommendations. First, there is widespread support for the US Cyber Challenge and similar initiatives. The US Cyber Challenge is a national competition and talent search to find and develop 10,000 cyber security specialists (United States Cyber Challenge 2009). Three large-scale competitions are envisioned: CyberPatriot, for high school students, conducted by the Air Force Association; the Digital Forensics Challenge conducted by the DoD Cyber Crime Center (DC3); and the Network Attack Competition conducted by the SANS Institute. Second, there is interest in channeling interest through a variety of techniques including support through national competitions, internships,

scholarships and specialized training programs. As an example, House Resolution 4061 would create a cyber security scholarship program (Koss 2010). Third, there is interest in developing standards for teaching cyber security. Finally, we need to recruit top rate faculty and offer incentives to encourage them (e.g. fellowships).

Although the CNCI has stressed the importance of expanded cyber education, there are concerns that it has not been explicit in this initiative. The Government Accountability Office (GAO) recently issued a report on Cyber security that assesses the status of the CNCI (Government Accountability Office 2010). In that report they observe that "Stakeholders have not yet reached agreement on the scope of cyber security efforts". Consequently, they recommend that the Director of the Office of Management and Budgeting (OMB) "reach agreement on the scope of CNCI's education projects to ensure that an adequate cadre of skilled personnel is developed to protect federal information systems."

Furthermore, as noted in (Associated Press 2010), the US military academies have increased their emphasis on cyberwarfare. At the US Military Academy at West Point, cyber security has been part of the curriculum taken by all students for years. Currently, information technology has been required for approximately ten years for all cadets who don't test out of the class. At the Air Force Academy, they have created an emphasis on the subject in 2004 by adding classes in cryptology, computer science, information warfare, and network security. Currently, every freshman at the Air Force Academy takes a class that includes some aspects of cyberwarfare. Since then, the school has graduated more than eighty students with an emphasis on cyberwarfare. Finally, the US Naval Academy Computer Science Department is running its first-ever cyber security course for students who are not computer science majors. Since December 2009, the Naval Academy created the Center for Cyber Security Studies. This activity is coordinated with the NSA and establishes a six-week internship program. In addition, they have created two new elective courses in computer science: Cryptography and Network Security and Computer Forensics.

4.3 CERTIFICATION, RETENTION, PROFESSIONAL DEVELOPMENT, AND WORKFORCE MANAGEMENT

The US government is not the most attractive employer (e.g. with respect to salary limitations). In addition, dynamic computer professionals often feel stifled and powerless in a large bureaucracy.

To address this issue, the authors believe that the following recommendations should be implemented. First, it is important to develop a cyber security talent management

plan that would serve to coordinate professional training and staffing needs. Second, there is interest in establishing exchange programs between the US government and the private sector. This would serve to educate members of the private sector so that they would understand the magnitude of the cyber security problem. Third, since the cyber security problem is continuing to evolve, it is important to have the US government support continuing education, certification, and development. Fourth, given the need to attract talented cyber security professionals, it is important to offer special hiring and pay authority. Finally, steps should be taken to employ the certification process so that it has a strongly rooted business case (Tipton 2009).

In the area of certification, the DoD has recently mandated that US Government cyber defenders must be able to perform "ethical hacking" (Montalbano 2010). The term "ethical hacking" was coined by IBM in the 1960s to define a way for IT security researchers to emulate the work of hackers so they can better defend networks. In a February 25, 2010 update to a directive on information security, DoD now requires its computer network defenders to pass Certified Ethical Hacker certification from the International Council of E-Commerce Consultants. This test is designed to explore the defender's ability to understand the mindset, tools and techniques of a hacker.

4.4 EXERCISES

The authors of this paper believe strongly that the US government must test how cyber security functions in a crisis. To that end, it is vital that all aspects of doctrine, organization, training, matériel, leadership and education, personnel and facilities (DOTMLPF) are assessed, holistically. In particular, realistic exercises must include the active participation of the private sector. We observe that typically, there is an overabundance of rules of engagement for conducting exercises that should be relaxed. In addition, it has been observed by the GAO that there has been a failure to incorporate lessons learned from exercises into the evolving DOTMLPF process (Government Accountability Office 2008).

To deal with those concerns, there is broad agreement that the US government must conduct "whole-of-government" exercises, including participation by the private sector at all stages of the exercise. It is vital that these exercises be realistic and that lessons learned are implemented across the interagency and the private sector. As an initial step, Lockheed Martin Corp and Johns Hopkins University's Applied Physics Laboratory have been awarded contracts by DARPA "to develop next-generation computer security testing systems against enemy cyber attacks" (Burnett 2010).

4.5 SECURITY CLEARANCE REQUIREMENTS

Currently, only a subset of graduating qualified computer professionals are clearable US citizens. Furthermore, the security process is long and expensive. Consequently, slots go unfilled or are filled by a person with lesser professional credentials but the right clearance level.

To deal with this issue, efforts should be made to hire more US citizens in the cyber workforce. Alternatively, efforts should be made to improve the clearance process (e.g. make it more efficient, more affordable, faster) or to institute more effective compartmentalization.

5. IMPLICATIONS FOR NATO

This paper has addressed the problems that the US faces in building a cyber force structure. The challenge of building a cyber force structure for NATO is beyond the scope of this paper and should be the subject of future research activities. However, many of the recommendations cited in this paper should be considered for application in the NATO context. These include: enhancements in lower and higher education; actions to improve the intellectual capacity of the cyber workforce (see Figure 2); steps to improve the planning, execution, and implementation of lessons learned for effective exercises; and the satisfaction of security clearance requirements. In addition, we believe that several of the initiatives in the CNCI should be broadened to address NATO cyber security issues (e.g. redirect Research and Development; develop leap-ahead technologies; develop cyber deterrence strategies).

6. SUMMARY AND RESIDUAL ISSUES

It is broadly acknowledged that current capabilities do not begin to satisfy cyber force needs. To mitigate these shortfalls, it is recommended that a *set* of actions should be taken. These include starting education early; improving higher education and recruitment; enhancing certification, retention, professional development, and workforce management; conducting and learning from more credible exercises; and paying additional attention to clearance requirements.

Overall, a coherent, consistent set of actions must be taken. This paper has also served to identify a set of issues that need to be addressed by senior decision-makers. In particular, senior decision-makers need to consider the following issues:

- Have the US Services adequately addressed career progression (note: many individuals in uniform are retiring and supporting cyber security as contrac-

tors)?

- Does NATO conduct realistic exercises and implement changes reflecting "lessons learned"?
- Should nations employ "patriotic hackers" (mirroring the perceived actions by the Russian government in their attacks against Estonia and Georgia (Bumgarner&Borg 2009))?
- What should be the role of the private sector and government organizations (e.g. the recent discussions between Google and the National Security Agency (NSA)) (Nakashima 2010b)?
- What steps can be taken to expedite the attribution problem?
- How should we refocus the Alliance's cyber deterrence posture?

REFERENCES

- Air Force Doctrine Center, 2008. Cyberspace Operations. Draft Air Force Doctrine Document 2-11, Maxwell AFB, AL, 2008.
- Associated Press, 2010. Cyberwarfare Gains Interest At Military Academies. Available at: http://wiz.com/local/Cyberwarfare.Military.2.1545372.html [Accessed March 8, 2010]
- Axe, D. Air Force Establishes 'Reduced' Cyber-war Command. *Danger Room* (August 18, 2009).
- Blair, D.C., 2010. Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, February 2.
- Bumgarner, J., Borg, S., 2009. *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008.* A US-CCU Special Report, August 2009.
- Burnett, R., 2010. Lockheed Training Unit Lands Deal to Make 'Cyber Range' for Next-Gen Security Software. *Orlando Sentinel,* February 3.
- Craft, J., 2009. Presentation to NDU Cyber Force Structure Conference, 29 October 2009.
- Department of Defense, 2010. Quadrennial Defense Review Report, February.
- Department of the Navy, 2009. *Cyberspace Policy and Administration Within the Department of the Navy,* SECNAV Instruction 3052.2, 6 March 2009.
- Deputy Secretary of Defense Memorandum, 2008. The Definition of Cyberspace. May 12.
- Fogelman, R., Widnall, S., 1995. *Cornerstones of Information Warfare.*
- Gates, R., 2009. *Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations.* Memo, 23 June 2009.
- Gonzales, D., et al, 2005. *Network-centric Operations Case Study: Air-to-Air Combat with and without Link 16.* , RAND, Santa Monica, CA.
- Gosler, J., 2010. *Personnel communications,* January 2010.
- Government Accountability Office, 2008. *DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise.* GAO-08-825.
- Government Accountability Office, 2010. *Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative.* GAO-10-338.
- Koss, G., 2010. House Cyber security Bill Eases Toward Passage. CQ February 4.
- Kramer, F.D., Starr, S.H., Wentz, L.K., 2009. *Cyberpower and National Security.* Potomac Press, 2009.
- Marine Corps, 2003. *Air-Ground Task Force Information Operations.* Marine Corps Warfighting Publication 3-40.4, 9 July 2003.
- Marine Corps, 2010. *HQ MARFORCYBER Information Brief.* 25 January 2010.
- Montalbano, E, 2010. The Navy Becomes the Third Branch of the U. S. Military Military to Establish an Organization to Oversee Its Cyber security Activities and Protect Against Attack. *Information Week,* February 1, 2010.
- Montalbano, E., 2010. The Department of Defense mandate solidifies the practice of ethical hacking within its ranks of security pros. *Information Week*, March 2.
- Nakashima, E., Krebs, B., 2009. As Attacks Increase, U.S. struggles to Recruit Computer Security Experts. *Washington Post,* December 23.
- Nakashima, E., 2010a. FBI director warns of 'rapidly expanding' cyberterrorism threat. *Washington Post* March 4.
- Nakashima, E., 2010b. Google to Enlist NSA to Help It to Ward off Cyber attacks. *Washington Post,* February 4.
- NRC, 2010. *NRC Prize for Cyberdeterrence Research & Scholarship.* [Accessed March 11, 2010] Available at: http://sites.nationalacademies.org/CSTB/CSTB_056215

- Owens, W.A., Dam, K.W., Lin, H., 2009. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities.* National Research Council.
- The United States Cyber Challenge, US Cyber Challenge Version 1.1, May 8, 2009.
- Tipton, W.H., 2009. DoD Certifies the Power of Partnership. *IAnewsletter*, Volume 12, November 4.
- Training and Doctrine Command, 2010. *TRADOC Pamphlet 525-7-8: The US Army's Cyberspace Operations Concept Capability Plan, 2016-2028.* Fort Leavenworth, KS: 22 February 2010.
- Webber, R., 2009. *NDU Cyber Force Structure Conference.* 29 October 2009.

GLOSSARY

Abbreviation	Meaning
ADM	Admiral
CAC	Combined Arms Center
CBA	Capabilities-Based Assessment
CCP	Concept Capability Plan
CWID	Coalition Warrior Interoperability Demonstration
CONOPs	Concept of Operations
DARPA	Defense Advanced Research Project Agency
DHS	Department of Homeland Security
DIRNSA	Director, NSA
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
EMS	Electro Magnetic Spectrum
ICANN	Internet Corporation for Assigned Names and Numbers
INSCOM	Intelligence and Security Command
JFCC-NW	Joint Functional Component Command for Network Warfare
JTF-GNO	Joint Task Force – Global Network Operations
K	Kindergarten
MacForCyber	Marine Forces Cyber
MAGTF	Marine Air Ground Task Force
MCNOSC	Marine Corps Operations Support Center
NATO	North Atlantic Treaty Organization
NDU	National Defense University
NETCOM	Network Enterprise Technology Command
NRC	National Research Council
NSA	National Security Agency
QDR	Quadrennial Defense Review
SACEUR	Supreme Allied Commander Europe
US	United States
USA	United States Army
USAF	United States Air Force
USMC	United States Marine Corps
USN	United States Navy