CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Cyber Policy Task Force

Working Group Discussion Papers

Military Cyber Issues

Michael Sulmeyer

Introduction

The next President will be the first to inherit a military force structure for cyberspace operations charged with three missions: defend the military's networks and systems; provide offensive cyber support to regional military commands; and defend the nation from a cyberattack of significant consequences. The President will also inherit a military, an economy, and a society that are significantly and increasingly vulnerable to cyberattack, so establishing priorities and guidelines for cyber defense and offense must be a priority. This paper addresses key questions the next President will confront on military cyberspace operations.

Threats

Over the last eight years, the scale of the militarily-relevant cyber threats has grown but the threat to US interests has not radically changed. Foreign hackers continue to probe DoD's unclassified networks; phishing activities targeting members of the DoD community have grown. Several intrusions in national security systems include the 2014 intrusion into the Joint Staff's network and a 2015 intrusion into another unclassified DoD network. There is no public information available about the effects those and other intrusions may have caused. These compromises to the confidentiality of data and systems have become more frequent in their detection and occurrence, though it is unclear their sophistication represents a leap in adversary capability.

We are seeing a morphing of the threat towards holding data integrity and availability at risk (vice confidentiality and availability). Moreover, we are seeing growing use of cyber as an instrument of national power by both Russia (Ukraine electric grid) and China (theft of personnel and medical data) which portends a growing *potential* strategic threat to US interests should those capabilities be brought to bear on the US.

At the same time of increasing frequency of cyberattacks, the complexity and scope of capability possessed by competitor nation-states – Russia, China, DPRK, and Iran – continue to grow and mature. In the case of Russia, cyber is a mainstream instrument of national power, an instrument increasingly well integrated across multiple applications of cyber power (influence, disruption, and espionage key among them) and with other national instruments of state? power.

As the cyber threat landscape evolves, the most critical threats the next President will have to address will be the potential for a major power conflict and threats to critical infrastructure. Meeting these threats necessitates a policy that takes into account mission assurance and facilitates combined operations.

Potential Major Power Conflict

In the event of a conflict with another major power, each side will have strong incentives to employ offensive cyber capabilities early against the other side's military and supporting infrastructure to impede the deployment, employment, and command and control of the opposing forces. These cyberattacks, which would not kill anyone directly, are likely to appear low risk and offer a high payoff. This has important implications for crisis management - the next administration should prepare itself to make rapid decisions about the potential employment of offensive cyber capabilities, including to reduce the other side's ability to attack US military and civilian infrastructure. In this scenario, it is worth assuming that US military systems will have at

least *some* cyber vulnerabilities, though the extent and impact of an offensive cyberattack is unclear. Assuring the resilience of critical U.S. military systems, including nuclear forces and long-range strike systems, will be critical to sustaining deterrence vital to preventing great power conflict.

Threats to Critical Infrastructure

The next President will have to consider is how military cyberspace forces might be used to defend US critical infrastructure from a significant cyberattack. At present, the National Mission Force (NMF) constitutes a high-end component of the Cyber Mission Force (CMF) structure with the mission to defend the nation from a cyberattack of significant consequence. The Department of Defense has not been specific as to what exactly a defending against a "cyberattack of significant consequence" means in practice, but Admiral Michael Rogers, the commander of US Cyber Command, has indicated in recent speeches that defending critical infrastructure is at least one likely application.

The NMF is comprised of 13 National Mission Teams, as well as some number of support teams, which constitutes a rather lean component of the overall 133 team Cyber Mission Force. As such, any mission to defend critical infrastructure will have to be narrowly tailored not just in terms of the NMF's responsibilities but to focus on the most vulnerable components of critical infrastructure. Former Assistant Secretary of Defense Eric Rosenbach noted in April 2015 testimony that the NMF would likely only be called upon to defend against the top two percent of cyber threats to the nation. Prioritizing the most critical of critical infrastructure need not be public, but it should be a first step towards guiding the NMF in its possible responsibilities.

Mission Assurance

Adversary cyber activity can undermine US mission assurance of its weapons systems and their supporting platforms, and critical infrastructure maintained by and in the private sector. Protecting .mil and related networks has been the focus of the traditional defense mission for U.S. cyber forces. However, protecting off-network systems needs to be a priority. The key concern is that through a variety of mechanisms, malware can be introduced into weapons systems even without direct connectivity to an Internet-connected system. The presence of that malware may lead commanders to question the readiness of their systems and the ability of these systems to execute core functions. A threat introduced from cyberspace can have much larger consequences on the readiness of US forces to execute non-cyber related missions, such as combat air patrols or missile defense.

Combined Operations

While US allies and partners continue to expand their capabilities to engage in cyber operations, those efforts remain largely focused on increasing resilience and defensive operations with combined offensive cyber operations remaining a distant second priority. Even then, individual nations are likely to retain tight control over their cyber capabilities and the means through which those capabilities are launched. Partnership opportunities, however, may arise from the need to help allies and partners protect their networks and possibly certain high-value pieces of critical infrastructure.

Key Military Cyberspace Issues

Given the nature of cybersecurity threats to US interests, the key military cyberspace questions the next President will confront include the cyber mission force structure, the potential elevation of US Cyber Command to a unified command, the dual-hat role of the Commander of US Cyber Command, the role of the military services, civilian oversight of military cyberspace activities, and partnerships across the US government and with the private sector.

Force Structure

The Obama Administration invested heavily in the creation of a Cyber Mission Force compromised of 133 teams of three types:

- 13 National Mission Teams to defend the nation from a cyber attack of significant consequence;
- 27 Combat Mission Teams to support regional Combatant Commanders with offensive cyber operations;
- 68 Cyber Protection Teams to defend DoD networks and assets;
- 25 Support Teams to provide additional analytic and planning resources to the National Mission Teams and Combat Mission Teams.

US Cyber Command's primary focus over the last several years has been to bring these 133 teams to a level of readiness to execute their missions. Training this force is time-intensive, but Admiral Rogers recently testified that over 90 percent of units should reach initial operating capacity by the target date of FY2018. Even then, however, these units will continue to need additional time gathering operational experience and to manage the inevitable turnover in personnel until the pipeline for new, full-trained, and experienced personnel is stabilized and properly supported by a career management mechanism that captures and sustains cyber talent over succeeding careers.

The next President should assess how these forces are assigned and consider alternate constructs that may reflect the experience of four years of building the cyber mission force. Among others, one consideration may involve how best to balance between preparing to counter geographical vs. technical threats.

National Guard and Reserves

Although the 133 teams of the Cyber Mission Force are essentially an active-duty force, the National Guard and the Reserves can be powerful supplements to the CMF. Indeed, Congress mandated that the Department of Defense examine how the Guard and Reserves could contribute to the national cyber force posture in Section 933 of the 2014 National Defense Authorization Act. The traditional inclination is to consider employing these forces in the aftermath of a cyber intrusion or serious operation. However, the next administration should consider how the Guard and Reserves can be used ahead of an incoming cyberattack to better protect critical assets before an incident. The capability of National Guard units to operate across the range of State (Title 32) and federal (Title 10 and 50) authorities, combined with the ability of the private sector to generate and sustain deep talent in citizen-soldiers/airmen/sailors makes the use of the National Guard and Reserves a cost-effective, high leverage, force for integration and augmentation.

Sub-Unified or Unified Command

As of May 2016, US Cyber Command remains a sub-unified command subordinate to US Strategic Command. Recently, there has been a debate about whether to elevate U.S. Cyber Command to the status of a functional unified command. Proponents of elevation stress that such an arrangement would streamline operational authority between the National Command Authority and the Commander of US Cyber Command, cutting out the middle man (the commander of US Strategic Command). Others express caution that the increase of bureaucracy to operate a unified headquarters staff outweighs the negligible operational impact of elevation.

The original logic of placing Cyber Command under Strategic Command reflected the historical origins of cyber operations and the inherent advantage of leveraging existing capabilities. The National Security Agency has the mission for computer network exploitation and the collection and analysis of foreign signals intelligence under Title 50, but was not authorized to conduct Title 10 offensive or attack missions. Instead, prior to the standup of US Cyber Command, US Strategic Command employed a stand-alone Joint Functional Component Command for Network Warfare (JFCC-NW) for Title 10 offense and a Joint Task Force for Global Network Operations (JTF-GNO) for Title 10 defense. Under this pre-US Cyber Command construct, the Director of NSA was dual hatted as the commander of JFCC-NW and the Director of the Defense Information Systems Agency (DISA) was dual hatted as the commander of JTF-GNO. Both of these Title 10 constructs were rolled into US Cyber Command, preserving subordination of each of these functions to U.S. Strategic Command and the firewalling of Title 10 military operations from the intelligence support provided by NSA.

One reason to elevate Cyber Command is to allow Strategic Command to focus on its core competencies of nuclear deterrence, space operations and global strike. While analysis behind that element of this change is beyond the scope of this paper, the impact that elevating Cyber Command would have on Strategic Command is an important aspect of the decision.

Elevating Cyber Command should also be seen as an opportunity to empower the command with non-traditional authorities it may need to better execute its missions. For example, last year's National Defense Authorization Act included a small test program that authorized Cyber Command (albeit on a limited basis) to bypass the military services and directly acquire capabilities. The inspiration for this authorization was likely the perceived need for agility in capability development and deployment in the dynamic domain of cyberspace. The model tracks the experience of US Special Operations Command, to which Congress granted several unique authorities when it mandated the command's creation in the mid-1980s.

There is no prohibition on granting special authorities to a sub-unified command as Cyber Command as currently structured, so special authorities need not be a function of elevation. However, elevation would reflect the senior leadership's affirmation that cyber operations have become just as crucial to the national defense as the other functional commands and sustain the current permission-to-operate-without-exacting-coordination delegated by U.S. Strategic Command to US Cyber beyond the current personality-dependent situation.

Regardless of whether President Obama elevates Cyber Command before the end of his term, the next administration should evaluate Cyber Command's authorities and ensure it can set its own requirements for acquisition. It should also be authorized and resourced to acquire needed

capabilities as rapidly as possible. In addition to these capability-development authorities, the readiness of the 133 teams of the Cyber Mission Force should drive whether additional recruitment and retention authorities are needed so Cyber Command can attract, develop, retain, and career-track top military and civilian talent.

The Status of the Dual-Hat Commander

At present, the Commander of US Cyber Command is dual-hatted as the Director of the National Security Agency. This arrangement reflects the origins of US Cyber Command from when the commander of one of its predecessor organizations, JFCC-NW, was dual-hatted with the NSA Director. The logic of this arrangement was to empower one individual with the ability to leverage the combined resources of NSA and the uniformed services and pivot quickly between defense, exploitation and attack as needed. Given that the underlying mechanics of these operations were often similar, anointing one individual to conduct full-spectrum computer network operations was compelling.

One area of tension the dual-hat arrangement creates, is that one person – the dual-hatted commander and director – is required to represent two opposing interests in considering an offensive cyber operation: the operational gain and the potential intelligence loss. The responsibility of balancing these equities will only become more challenging as Cyber Command achieves greater readiness and independent capabilities. A system in which operational gain and potential intelligence loss have senior advocates could have advantages. This issue will become more acute as US Cyber Command and the role of cyber operations within the Department continue to grow.

The next President will have the opportunity to review this dual-hat arrangement and determine if the NSA and Cyber Command should be led by different individuals. More than most issues discussed in this paper, this decision has deep, technical issues at stake and should be made based on an analysis of capabilities development and readiness at each institution There is no immediate reason to act, the current arrangement under Admiral Michael Rogers appears to be working well. At the time when Admiral Rogers's appointment expires, it would be worth exploring whether breaking the dual-hat would help these institutions accomplish their missions more effectively.

Beyond the questions of whether and how to convey authorities for acquisition and intelligence collection to a stand-alone U.S. Cyber Command, the issue of the specific relationship between NSA and U.S. Cyber Command will demand significant attention. The Director of National Intelligence and NSA's non-DoD customers will argue strongly for a relationship that does not subordinate NSA to US Cyber Command. The Department will nonetheless still want the relationship to retain the intimacy and collaboration enjoyed under the present scheme.

The Role of the Military Services

While US Cyber Command has the lead for US military operations in cyberspace, the four military services play a crucial role as force providers to the cyber mission force. This is similar to the role they play for conventional forces. The services train national mission teams, combat mission teams, and cyber protection teams, each using its own procedures to organize and train these units. While there are joint training standards, each service is responsible for assigning

individuals to units and getting them into training pipelines to support their eventual Cyber Command missions.

Unless a broader Goldwater-Nichols-like reform movement changes the relationship between the services and the combatant commands, there is no reason to make such a change only for cyberspace. As the services continue to train forces for the CMF, however, it may be worth re-examining how each service recruits and retains top military and civilian performers to exchange best practices. Again, the experience of Special Operations Command in supporting career-long professional development tracks will be a useful model for US Cyber Command. Finally, because each service draws from different communities (from signals intelligence to communications) to create cyber mission teams, the services need to have sufficient resources to ensure these other disciplines do not atrophy at the hands of the cyber mission force.

Civilian Oversight of Military Cyberspace Activities

The Office of the Secretary of Defense (OSD) is the traditional instrument for civilian oversight of the military. For activities in cyberspace, OSD's Chief Information Officer is a civilian partner to Cyber Command's (and the Defense Information Systems Agency's) design of network standards and policies. For acquisition issues, the Under Secretary for Acquisition, Technology, and Logistics is the Department's top decision authority for major system procurement. For operational questions, the Under Secretary for Policy (specifically the Deputy Assistant Secretary of Defense for Cyber Policy) and the Under Secretary for Intelligence provide civilian oversight.

Three years ago, Congress mandated the creation of a Principal Cyber Advisor (PCA) to the Secretary of Defense to serve, among other things, as the focal point for coordination within the Department and to be a single point of contact for Congressional interaction with the Department on cyberspace issues. The details of how the PCA has functioned are mostly not publically available, including what its specific responsibilities have become and how successful it has been at coordinating across the Department's many offices. According to statute, the PCA must be confirmed by the Senate (so an Assistant Secretary or higher in rank) within the Office of the Under Secretary for Policy.

The next President will have the opportunity to review this arrangement to see if it adequately provides the degree of civilian oversight that the Defense Department requires. One consideration may be to propose to Congress that it elevate the PCA to a full Assistant Secretary position to perform the intended coordination and oversight functions. In that sense, this new Assistant Secretary would be similar to the Assistant Secretary for Special Operations and Low Intensity Conflict, which Congress called for as it created U.S. Special Operations Command in the 1980s. Thus, part of the decision about how to best structure civilian oversight needs to reflect US. Cyber Command's continued evolution.

Another balancing act within OSD will be the role of the Department's Chief Information Officer relative to any new Assistant Secretary. The CIO should be organized within the emerging office of the Under Secretary for Business Management and Information, responsible for overseeing the operation and protection of the Department's enterprise systems. A separate, likely Senate-confirmed individual within the office of the Under Secretary for Policy should be responsible for the oversight of military planning in cyberspace and offensive cyber operations.

Despite the common refrain that offense and defense are merely two sides of the same coin in cyberspace, the civilian oversight and coordination functions in OSD are sufficiently distinct to warrant this division of labor.

Partnerships across the U.S. Government

Law enforcement

Despite its growing size and stature within the US defense establishment, US Cyber Command and its components can only accomplish so much on a national level. During the Obama administration, the responsibilities for the Department of Homeland Security expanded to enable better coordination with owners and operators of critical infrastructure. The FBI also emerged as a powerful, operational entity within the U.S. government whose domestic law enforcement authorities and growing technical experience offered a strong complement to externally-focused military operations.

Greater cooperation between the military and law enforcement is not just prudent – it is required due to how the domestic and international jurisdictions dividing the military and law enforcement communities break down in cyberspace. Indeed, cyber operations against the United States using international and domestic infrastructure represent a new form of "lawfare," a term coined over a decade ago to describe how terrorists exploited gaps in U.S. law. As a result, the U.S. military *must* work with counterparts in law enforcement to combat threats that reject the current division of domestic and international labor within the U.S. national security establishment.

One opportunity the next administration may wish to explore is how to use the military services' investigatory offices to bridge the military-law enforcement gap. For example, the Air Force's Office of Special Investigations (AFOSI) has unique authorities through its counter-intelligence mission to undertake domestic forensics investigations, even if the chain of evidence leads them outside of Air Force networks. At present, the limited number of AFOSI agents in the field undertaking cyber-related work limits the extent of cooperation. However, if AFOSI and its Navy and Army counterparts were given increased resources for cyber-related investigations and activities, they could grow into a natural bridge between US Cyber Command and the domestic U.S. law enforcement community.

Intelligence

The need for close partnerships between US military cyber forces and the intelligence community cannot be overstated. For US military forces to be able to prevent or preempt an adversary's offensive cyber operations against the United States, intelligence – no matter the type or source – is critical. Without it, military cyber forces will be confined to a reactive posture.

Previous administrations have provided the resources and organizational flexibility to foster close collaboration between the intelligence and military cyber communities. For the next administration, the opportunity will be to streamline the speed at which information can be shared between intelligence and military communities, as well as from those communities to law enforcement and other institutions that may benefit from specific, threat-based information. Calls for sharing at real-time or near real-time speeds are laudable, and there are undoubtedly obstacles

that can be removed to increase the speed at which some information can be shared between some entities. However, system-wide real-time sharing is probably still a distant possibility.

Partnership across Private and Public Sectors

Finally, the protocols and thresholds governing DoD defense of civilian infrastructure must be further defined and exercised to ensure efficient and effective transitions between the various roles assigned to private sector and government organizations. The ends of the spectrum (peace and tranquility on the one end and state-to-state conflict on the other) are well understood and similarly well-practiced. Experience navigating the transition between the two is virtually non-existent. Given that sharp transitions favor the aggressor who chooses the time, place, and pace of action, an integrated and coherent defensive scheme is the best mitigation, complemented by an overlay of collaboration amongst the parties owning, operating and defending cyber infrastructure. This reality calls out for a collaboration between the private and public sectors. A simple division of effort, however attractive, will not suffice. Information sharing that enables shared situational awareness and rapid, fluid shifts of defensive efforts will be a key enabler. Privacy and security will be difficult to align but must be the goal to ensure an enduring solution that works across sectors and national boundaries.