CHAPTER 7

U.S. CYBER COMMAND'S ROAD TO FULL OPERATIONAL CAPABILITY

Michael Warner

INTRODUCTION

U.S. Cyber Command (CYBERCOM) achieved full operational capability in October 2010 as a sub-unified command under U.S. Strategic Command. Its course to this status took several turns due to a number of factors related mostly to the novelty of the cyber domain, which left considerable uncertainty in the minds of decisionmakers at several levels in the Department of Defense (DoD). What ultimately prevailed was the strong support of the Secretary and the conviction among senior defense leaders—even as they debated the particulars—that the nation needed something done swiftly to defend military networks. The main lesson of U.S. Cyber Command's accomplishment thus would seem to relate to the centrality of national-level policy concerns even in military matters. Secondary lessons include the importance of staff coordination and the staff's command of information vital to decisionmaking processes.

CYBERCOM's attainment of full operational capability (FOC) status took roughly 2 years from the time Secretary of Defense Robert M. Gates set the process in motion. In many ways, the process toward FOC typified the establishment of a major organization in the DoD, but in other respects, the novelty of the cyber domain—in which every Service, combatant command, and agency operates and even "fights"—added

unforeseen complexity to decisionmakers' roles. Indeed, nearly every senior leader in the Department had some equity that would be affected by the work of the new CYBERCOM, and many of those leaders had advice for the principals making the key decisions about it.

An examination of CYBERCOM's progress to FOC thus has to be more than a chronicle of the key events and relevant leadership actions. The formation of a major new defense organization in a new battlespace is automatically a primer in organizational change. This chapter surveys the events leading to FOC and reflects on their significance by drawing upon the documentation assembled by the CYBERCOM team that managed the process, supplemented not only by the memories of the team members but also by research in Command records. It is by no means definitive, but its accuracy and timeliness should complement the breadth and depth of research that will be possible in the future.

ANTECEDENTS

The Information Revolution has empowered people and institutions to work more efficiently and take advantage of unprecedented opportunities. At the same time, however, the networking of the world's information systems in "cyberspace" has opened new fields for criminality and coercion, and tied the security of private individuals to that of enterprises and nations in unforeseen ways. The importance of cyberspace to national security became a pressing concern after the end of the Cold War. Such concerns increased dramatically as exercises like "Eligible Receiver 97" demonstrated network vulnerabilities and, as Ameri-

can officials discovered with the Moonlight Maze incident in 1998, that foreign entities had been probing sensitive U.S. military networks.[1] The Joint Chiefs of Staff (JCS) in their 2004 *National Military Strategy* declared cyberspace a domain (like air, land, sea, and space) in which the United States must maintain its ability to operate.

The DoD and the Armed Services responded to these evolving challenges through a variety of organizational initiatives. The first of these was the Joint Task Force-Computer Network Defense (JTF-CND), a small organization chartered by the Secretary of Defense and reporting directly to him. JTF-CND operated in conjunction with the Department's de facto Internet service provider, the Defense Information Systems Agency (DISA), and attained initial operating capability on December 1, 1998.[2] President Bill Clinton under Unified Command Plan 1999 soon assigned JTF-CND to U.S. Space Command (SPACECOM). The offensive and defensive cyber missions came together under the same organization in 2000, when SPACECOM formally took over the DoD computer network attack planning. As a result, JTF-CND was re-designated the Joint Task Force-Computer Network Operations (JTF-CNO) in April 2001. When SPACECOM was dissolved and its functions merged into the reorganized U.S. Strategic Command (USSTRATCOM) on October 1, 2002, JTF-CNO had 122 positions and a $26 million budget. Its new mission, under Strategic Command and with the geographic combatant commands, was to:

> coordinate and direct the defense of DoD computer systems and networks; [and] coordinate and, when directed, conduct computer network attack in support of combatant commanders' and national objectives.[3]

JTF-CNO was headquartered in Arlington, VA, with DISA's Global Network Operations and Security Center (GNOSC), and had a 24-hour watch floor there.

In 2002, the transfer of Defense-wide computer network operations responsibilities to USSTRATCOM occurred as discussions in the Department over these roles were increasing. USSTRATCOM soon approved the Joint Concept of Operations for Global Information Grid Network Operations. In June 2004, Secretary of Defense Donald Rumsfeld added the final step in this transformation by authorizing the creation of the Joint Task Force-Global Network Operations (JTF-GNO), with the three-star Director of DISA dual-hatted as its Commander (and as USSTRATCOM's Deputy Commander for Network Operations and Defense). The next year, Strategic Command's General James Cartwright (USMC) completed the task of rearranging USSTRATCOM by creating a series of joint functional component commands to perform the Command's various missions. The new Joint Functional Component Command for Network Warfare (JFCC-NW) would be commanded by the Director of the National Security Agency (NSA) and take on the offensive side of the now-defunct JTF-CNO's responsibilities.

When USSTRATCOM finished its reorganization, DoD had assembled a complicated arrangement of cyber capabilities and organizations. DoD also provided information technology services Department-wide via DISA; used NSA for cyber intelligence and information assurance; and administered some policy and oversight functions in the office of the Assistant Secretary of Defense of Networks and Information Integration (who was also DoD's Chief Information Officer). USSTRATCOM grouped its military cyber capabilities (both offensive and defensive) in two

organizations: JFCC-NW was paired with NSA, and JTF-GNO with DISA. Those two partnerships gave the offensive and defensive operators, respectively, access to subject matter expertise, but their bifurcation also meant that they talked less to one another than they had under the old JTF-CNO. Each Service had its own cyber component, moreover, to manage its own networks. This congeries of capabilities fully satisfied no one, and within 2 years a high-level effort to revise it was underway.

INITIAL DECISIONS IN 2008

In early-2008, Secretary of Defense Robert Gates wondered about better ways to organize the DoD's cyber functions, setting in motion studies of alternatives to the current arrangement. Indeed, the possibility of a "Cyber Command" had been discussed that February by General Kevin P. Chilton, the new Commander of USSTRATCOM, and senior officials from the Pentagon, Washington, DC, NSA, and the Office of the Director of National Intelligence. This preliminary work led to the Secretary's direction in May 2008 to task a Departmental-level review of cyber roles and missions, to be conducted by the Quadrennial Roles and Missions Review's Cyber Team. The team considered reorganization schemes that summer under the supervision of Principal Deputy Undersecretary of Defense (Policy) Christopher "Ryan" Henry and USSTRATCOM's Deputy Commander, Vice Admiral Carl V. Mauney (USN). This effort was among the earliest to contemplate the creation of a "Cyber Command," and it revived the notion that the new entity should oversee both the offensive and defensive facets of cyber operations. Another study group, led by

a former U.S. Air Force Chief of Staff, General Larry Welch, evaluated the issues for the Joint Chiefs under the auspices of the Institute for Defense Analyses (Welch was that organization's president). In sum, it appears that a consensus had emerged that the current division of labor between DoD cyber security and network attack organizations was sub-optimal and needed to be changed sooner rather than later. Secretary Gates heard the briefs, and on October 2, 2008, he "indicated that a four-star sub-unified Command under USSTRATCOM should be DoD's organizational endstate for cyber C2 [command and control]."[4]

At this point, Secretary Gates declined to decide the new entity's ultimate configuration and instead, on November 12, 2008 realigned the existing organizations. Citing "a pressing need to ensure a single command structure is empowered to plan, execute, and integrate the full range of military cyberspace missions," he directed USSTRATCOM, effective immediately, to "place [JTF-GNO] under operational control of Commander [JFCC-NW]."[5] This added a new job to the duties of Lieutenant General Keith B. Alexander (United States Army), who was already serving as both Director of NSA and Commander of JFCC-NW. More important, it meant that both the offensive and defensive components of DoD cyber capabilities would, for the first time, operate in close proximity to the nation's signals intelligence system.

Several events factored in the Secretary's thinking and the timing of his order. In particular, NSA had played a key role in detecting the presence of foreign intelligence malware in DoD classified networks in October 2008, and was helping DoD organizations neutralize the infection in an operation named BUCKSHOT YANKEE.[6] Additionally, Secretary Gates was,

at this point, reasonably certain he would be asked to stay on under the incoming administration of President-elect Barack Obama, which would allow him to implement broader changes he was directing in DoD cyberspace organizations.

FORMING A COMMAND, JANUARY 2009-MAY 2010

President Obama took office on January 20, 2009, and, by coincidence or not, discussions over implementing the Secretary of Defense's order around that time took a decisive turn. The previous month, a blue-ribbon panel convened to advise Secretary Gates on managing the nuclear weapons stockpile had concluded that USSTRATCOM had too many missions, and publicly recommended that the Command's responsibilities be narrowed to nuclear matters only (leaving cyberspace and other missions to other DoD organizations).[7] In March, USSTRATCOM assembled a team of planners to work with NSA and JFCC-NW experts at Fort Meade, MD, to develop a commanders' estimate, which Alexander could use to explain to Chilton how he planned to exercise the operational control of JTF-GNO, granted him the previous November. The estimate's scope was expanded in April, however, to encompass options for a new Cyber Command, shortly before rumors of a new military command hit the news media.[8] Alexander briefed Chilton on May 1 on the progress toward the commander's estimate.

A few days later, Alexander explained to the House Armed Services Committee in a public session that the replacement of analog technologies by digital networks meant the world was now linked in

"the same network." The U.S. military had seized opportunities resulting from this development but was not yet addressing the accompanying risks; indeed, in Alexander's view, the current approach to cyber security "does not work." Hinting at the DoD impending decision, he added:

> we're looking at the steps of what we have to put together in the sub-unified command as an option, or in a Joint Functional Component Command—how will we put these capabilities together to ensure our networks are secure and provide us freedom of maneuver in cyberspace.[9]

Secretary Gates gave his answer on June 23, 2009. "Effective immediately," he directed USSTRATCOM "to establish a subordinate unified command designated as U.S. Cyber Command (USCYBERCOM)." JFCC-NW and JTF-GNO would be dismantled and their personnel reassigned to USCYBERCOM, which the Secretary "preferred" to see based at Fort Meade with NSA. The Joint Chiefs of Staff were to issue a planning order to USSTRATCOM to develop an implementation plan, and initial operating capability was to be reached by October 2009, with full operating capability following in October 2010. USCYBERCOM was also authorized direct liaison privileges with the geographic combatant commands.[10]

USSTRATCOM responded smartly to the Secretary's direction. The commander's estimate team had already been re-chartered as the "Implementation Planning Team" 2 weeks earlier. Talks between senior officers from USSTRATCOM, NSA, JFCC-NW, JTF-GNO, and DISA set the stage for the Implementation Planning Team's work. Meeting at NSA, the team started drafting an Implementation Plan and

created a "cyber story board" to explain the emerging concepts. That brief served as the basis for briefings delivered across Washington and the military in ensuing months. Meanwhile, Chilton sent the finished Plan to the Chairman on September 1; it listed 13 required tasks for reaching initial operational capacity (IOC) but did not set hard criteria for determining FOC. Instead, the Plan included several dozen tasks of varying importance and specificity to complete by October 1, 2010, in its larger matrix of actions for attention between 2009 and 2011.[11] At FOC, the Plan's "Commander's Intent" was that:

> USSTRATCOM [Unified Command Plan] authorities and planning responsibilities related to cyberspace will have been transferred to CDRUSCYBERCOM [Commander, USCYBERCOM], and USCYBERCOM's capacity and capabilities for cyberspace operations will have matured to a point where it can plan, synchronize, and execute cyberspace operations as a supported or supporting command.[12]

The new organization soon began to grow, building on existing JTF-GNO and JFCC-NW manpower. On October 16, 2009, President Obama nominated Alexander to be the first Commander of USCYBERCOM. A couple weeks earlier (on October 5), JFCC-NW and JTF-GNO had begun to merge their staffs and operational centers into a consolidated staff. It in turn began hiring senior officials to head its "J-Code" directorates.[13] Many of the functions of the JFCC-NW Deputy Commander now went to the new chief of staff, Major General David N. Senty (United States Air Force Reserve), to manage for the consolidated staff.

LOW-HANGING FRUIT, MARCH TO AUGUST 2010

The Pentagon had expected confirmation hearings for Alexander before the end of the year. For a number of reasons, however, the confirmation was delayed.[14] Alexander testified before the Senate Armed Services Committee on April 15, 2010, and 3 weeks later, the Senate approved both his nomination to head the new USCYBERCOM and his promotion to general.[15] With this step taken, on May 21, the Secretary of Defense presided at a promotion ceremony in NSA headquarters, deactivating JFCC-NW, and declaring that USCYBERCOM had achieved IOC.

The new Command had to have a way of measuring progress toward FOC. In April, Senty began tracking a series of metrics based on the Implementation Plan (I-Plan) and a dozen commander's priorities that his staff had recently crafted for then-Lieutenant General Alexander.[16] On July 27, Senty's staff, which had helped draft the I-Plan, requested Command staffs to provide weekly details of progress toward FOC and a re-validated list of milestones.[17] The resulting "Strategy to Tasks Status Update" brief sorted dozens of I-Plan actions according to the commander's priorities into 23 tasks and placed them in a matrix that would be the main device for tracking progress. The work paid off that summer and fall, when the staff's matrix repeatedly won praise for the situational awareness it provided to senior leaders.

Creating situational awareness in cyberspace was also vital for the new Command. On March 5, 2010, the consolidated staff merged watch personnel and expertise (mostly from JTF-GNO and JFCC-NW) in

a combined Joint Operations Center (JOC) at Fort Meade. Control of USCYBERCOM operations from the combined JOC began on May 17, along with new procedures designed to "operationalize" DoD information networks. By August, the JOC was functioning well enough to continue JTF-GNO's watch function.

Another hurdle was the move and assimilation of JTF-GNO, the planning for which had begun by August 2009. In Fiscal Year 2010, JTF-GNO was authorized 66 military and 138 civilian personnel, some of whom would return to DISA, their parent organization. Many of those who chose to go with USCYBERCOM needed upgraded security clearances before they could effectively support the Command's mission at Fort Meade. The upgraded clearances all sat with the DISA in Arlington, VA (DISA's Director, Lieutenant General Carroll Pollett, also served as JTF-GNO's Commander). That in itself added another complicating factor, as DISA had been slated by the Base Realignment and Closing (BRAC) process in 2005 to move to a new headquarters building at Fort Meade in 2011. Thus, DISA was in the midst of planning its own move north. All these factors came together to delay JTF-GNO's transition. USCYBERCOM had assumed JTF-GNO's command and control functions by early-June, but the full transition of personnel and databases that had been slated to occur on June 30 had to be pushed back 2 months. JTF-GNO was formally disestablished at a ceremony at DISA on September 7.

Finally, on August 5, the Senate confirmed the nomination of Major General Robert E. Schmidle (USMC) to be the first Deputy Commander, USCYBERCOM; he was promoted to lieutenant general 4 days later and reported for duty on August 10. These moves set in place many of the personnel and structural

issues that came with setting up a new command, and the new command had effectively accomplished several organizational tasks that demonstrated progress toward FOC, but challenges still remained.

TOUGH ISSUES, JUNE TO OCTOBER 2010

Several issues seemed likely to persist even after the declaration of FOC. As Senty's aide explained, these issues amounted to "building capability and capacity in Service cyber forces, and gaining the requisite authorities and fully resourcing the Command."[18] Each presented an interlocking series of complications for every decisionmaker who approached it. Gates himself introduced another problem set in August. The issues collectively prompted high-level debates over the wisdom of declaring the Command to be in FOC status later rather than sooner.

The first set of challenges revolved around questions of authority. What authorities would USCYBERCOM possess? As a sub-unified command, it operated under the authorities delegated to it by its institutional parent, USSTRATCOM, which in turn were derived from the Unified Command Plan approved by the outgoing President George W. Bush in December 2008. That same month, Gates had directed USSTRATCOM to draft a global campaign plan to secure, defend, and operate DoD information systems. USSTRATCOM had responded with Operation GLADIATOR PHOENIX, delivering a draft of its execute order to the Joint Staff in May 2009. Staffing and coordinating the order in the Department began promptly, but with the change in direction dictated by Gates' announcement of his intent to create a cyber command that June and the delay in the Commander's confirmation, it was not completed until after the Command reached IOC

a year later. Chilton briefed Gates on GLADIATOR PHOENIX in June 2010, and Gates approved it on February 11, 2011.

USCYBERCOM also had to determine how it would exercise command and control over the Service cyber components that were to be assigned to it. USCYBERCOM also had to plan how it would integrate its operations with those of the geographic combatant commands. The Joint Chiefs discussed these challenges in August 2010, directing the Command to run a series of tabletop exercises to identify the relevant issues. Schmidle ran the first of these at Fort Meade in October. The event helped to demonstrate that the Command was assuming its responsibility to advance the debates over lines-of-authority in the new cyber domain.

As questions about USCYBERCOM's authority were ironed out, questions about resourcing emerged. The new Command's leaders waited months to learn which Service units the Pentagon would assign to USCYBERCOM. The Services had begun reorganizing their cyber capabilities in late-2009, with the idea of creating headquarters units (in addition to those already assigned to USSTRATCOM) that would function with the proposed USCYBERCOM. Over the next few months, the Services created the Army Cyber Command; Marine Forces Cyber Command; Fleet Cyber Command/U.S. Tenth Fleet; and Air Force Cyber Command/24th Air Force. As USCYBERCOM neared its FOC date, however, these forces remained in an institutional limbo, not yet assigned to any command. Gates approved the new Assignment Tables for all the unified commands only in December 2010—after FOC—and USSTRATCOM delegated operational control of various Service cyber units and their headquarters to USCYBERCOM a few days later.

A third set of questions about efficiencies also emerged close to the FOC target date. On August 9, 2010, Gates added another consideration for decision-makers at USSTRATCOM and USCYBERCOM. Speaking at a Pentagon press conference, he announced broad budget cuts across the DoD; defense agencies and unified commands in particular were to hold their future personnel totals to Fiscal Year (FY) 2010 levels. USCYBERCOM had not been scheduled to receive real increases in manning until FY11. Its combined JFCC-NW and JTF-GNO numbers totaled just over 500 FY10 billets, vice the 900-plus it had been projected to have in FY11 to perform its significantly expanded mission. The Command formally appealed for an exception in September, and several weeks later Deputy Secretary of Defense William Lynn granted the request.

At the same press conference on August 9, Secretary Gates also announced his intention to change the way the Department organized itself to administer its information networks. The Secretary stated a desire to shed the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) position and to divide its functions (along with some of those of the Joint Staff's J6) between DISA, the DoD Chief Information Officer, and possibly USCYBERCOM as well. Behind the scenes, moreover, another move was afoot. Gates quietly asked for options for increasing DoD reliance on a network architecture derived from a "cloud computing" proposal. The possibility of expanding USCYBERCOM size and mission was very much on the minds of senior defense officials as the date set for FOC drew near.

With Gates' October deadline for FOC approaching, Alexander noted USCYBERCOM accomplishments on the road-to-FOC tasks listed by the Secre-

tary, noting the remaining challenges (IT efficiencies, manpower, and personnel), and recommended the Secretary approve the declaration of FOC. Although concerns persisted over the risks created by those gaps, Chairman of the Joint Chiefs of Staff Admiral Michael Mullen (USN) and Vice Chairman General James Cartwright (USMC) urged the Secretary to declare USCYBERCOM to be in FOC status. On Sunday, October 31, 2010, Lynn approved FOC for USCYBERCOM. His statement noted that the Command had accomplished Gates' five critical tasks from the previous May, and ordered USSTRATCOM to articulate requirements for personnel, authorities, and information technologies efficiencies.[19] Thus, in a sense, USCYBERCOM's real work was just beginning.

CONCLUSION

The creation of USCYBERCOM marked the culmination of more than a decade's worth of institutional change. DoD defensive and offensive capabilities were now firmly linked, and, moreover, tied closely, with the nation's cryptologic system and premier information assurance entity, the NSA. That interlocking set of authorities, personnel, and organizations would also be better able to partner with both the geographic combatant commands and other U.S. Government agencies to defend the nation in cyberspace and ensure its freedom to maneuver in this new and challenging domain.

In organizational terms, USCYBERCOM's stand up represented an enormous amount of work performed at a fast pace. Despite a compressed schedule, the consolidated staff at USCYBERCOM and the legacy organizations it subsumed were able to accom-

plish a great deal by October 2010. They established a Joint Operations Center at Fort Meade, and disestablished USSTRATCOM's Joint Functional Component Command for Network Warfare as well as its Joint Task Force for Global Network Operations. The latter task took considerable planning and effort because JTF-GNO's activities and workforce had to be moved from Northern Virginia to Fort Meade while leaving the daily functioning of DoD information networks unimpaired. The consolidated staff fashioned effective command and control of cyber forces in the Services and reinforced a good working relationship with the DISA. It installed liaison officers at the combatant commands and cyber support elements as well, and deployed expeditionary teams to support operations in Iraq and Afghanistan. It also made progress in support of operational planning by the combatant commanders and in building processes for them to issue requirements for cyber support. In addition, the Consolidated Staff completed actions or made progress on a number of other matters, and accomplished all of this relatively seamlessly, keeping DoD operations secure while making the transition transparent to users of its information systems.[20]

Three important issues remained unresolved at USCYBERCOM's attainment of FOC. First, DoD had a shortfall of assigned cyber force capacity to plan, operate, and defend its networks and ensure freedom to access and maneuver in cyberspace. Second, the Command inherited authorities from predecessor organizations that seemed sufficient to defend DoD networks, but insufficient to protect the U.S. Government's networks or those associated with critical infrastructure in ways that the evolving cyber threat seemed to require. Thus, there was a respectful airing

of views in 2010 over the levels of risk associated with various options for pushing forward with a declaration of FOC for a new organization in a new domain. What drove the decision in the end was the leadership and support of the Secretary, as well as the conviction among senior leaders. Even as they debated the particulars, they agreed with one another that, because the nation needed something done swiftly to defend its military networks, it was riskier to hold USCYBERCOM in an indeterminate status than to advance its formation despite the lack of final resolution for these tough issues.

The process by which USCYBERCOM reached FOC was unique because cyberspace is a unique domain. Nonetheless, the events are worth recounting and patterns noticed because they have relevance for organizational change in DoD and for other sorts of organizations adapting to work in cyberspace. In this vein, there are several observations that might have more broadly applicable significance across DoD, particularly in regard to the attainment and declaration of FOC for a new command.

First and foremost, an FOC declaration for a major command entity is inherently a policy (and perhaps political) judgment. It broadcasts as U.S. policy the DoD belief that it could one day have to fight in a certain place or in a certain manner. Therefore, no determination of FOC can ever be entirely military in nature—and thus it will be driven by considerations partly outside of "objective" criteria and metrics. Similarly, IOC and FOC are the Secretary's to set and determine and declare. It is difficult to know in advance just how the world, the threat, and DoD will look as FOC nears. His vote on whether an entity is "ready" is the only one that counts. All other DoD actors in the process serve in an advisory capacity.

The policy implications notwithstanding, setting criteria for an FOC determination is important, as everyone concerned has to live with the results of a declaration when it comes. Criteria should be set early and well—and not chosen in any sort of ad hoc manner. Their meaning and relative centrality for FOC need to be understood, and they should not be changed as the process unfolds (they are either met, or unmet). When new items or tasks are added or obsolete ones removed from a list of FOC criteria, such an amendment needs to be executed with copious documentation and justification—in short, transparency. The initial standards for FOC should also designate the entity authorized to make such amendments and explain the process for doing so.

Organizationally, "Stoplight charts" or other metrics for criteria impose salutary discipline on the analysis of progress toward FOC. They also help seniors and staff to coordinate their perceptions and their actions. Obviously they are only a tool, however, and should not come to represent an end in themselves. Finally, staffs need to use those tools to coordinate with one another. IOC and FOC by definition involve a new staff emerging from an existing one. Both staffs must be synchronized. This is doubly tough to accomplish when the staffs are geographically separate—which only increases its importance.

ENDNOTES - CHAPTER 7

1. James Adams, "Virtual Defense," *Foreign Affairs,* May/June 2001.

2. Timothy Madden, *A Legacy of Excellence,* Arlington, VA: Joint Task Force-Global Network Operations, 2010, p. 6.

3. U.S. Strategic Command Public Affairs press release, February 2003, available from *www.iwar.org.uk/iwar/resources/JIOC/computer-network-operations.htm*. See also Ellen Nakashima, "Warriors in the Battle for Cyberspace," *The Washington Post*, September 25, 2010.

4. Joint Staff, J-5 Cyber Division, "Proposed SecDef Memorandum to Establish a Subordinated Unified Command for Cyber under USSTRATCOM," Joint Staff Action Processing form for J-5A 30217-09, April 20, 2009.

5. Secretary of Defense to Service, Command, and agency heads, "Command and Control for Military Cyberspace Missions," Washington, DC: DoD, November 12, 2008. The Secretary also stipulated that DISA's Director "will continue to serve as Commander of JTF-GNO and will remain responsible providing the JTF-GNO network and information assurance technical assistance as required."

6. Ellen Nakashima, "Cyber Intruder Sparks Response, Debate," *The Washington Post*, December 8, 2011.

7. James Schlesinger *et al.*, "Report to the Secretary of Defense on DoD Nuclear Weapons Management," December 2008, p. 54.

8. Staff e-mail to planning team invitees, "Cyber Mission Planning Team Off-Site," April 9, 2009; Siobhan Gorman and Yochi J. Dreazen, "New Military Command to Focus on Cybersecurity," *Wall Street Journal* online, April 21, 2009.

9. Testimony before the House Committee on Armed Services, Subcommittee on Terrorism, Unconventional Threats and Capabilities, May 5, 2009, pp. 7-8.

10. Robert M. Gates, Secretary of Defense, "Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Command for Military Cyberspace Operations," June 23, 2009.

11. "Initial operational capability" (IOC) is a term borrowed from the defense acquisition world to denote attainment of a significant ability to wield a new weapon or system as deployed in field conditions. There is no consensus on how long IOC should

take for a large DoD organization. The closest historical parallel to the establishment of USCYBERCOM, both institutionally and chronologically, was the establishment of U.S. Africa Command, which was announced in February 2007, reached IOC on October 1, 2007, and attained FOC on October 1, 2008.

12. USSTRATCOM, "United States Cyber Command Implementation Plan," September 1, 2009, p. 43.

13. For example, Major General David Lacquement (United States Army) came aboard in September as J3, and Major General Suzanne M. Vautrinot (United States Air Force), JFCC-NW's Deputy Commander, wore two hats as the Staff's J5.

14. The Senate Armed Services Committee scheduled the hearing after its staffers were briefed on plans for USCYBERCOM. Briefings of key members and staffers began in November 2009.

15. The Senate approved the nomination by unanimous consent on May 7, 2010.

16. This was the result of a series of meetings of the Consolidated Staff from December 2009 to February 2010, culminated by a Staff brief of Vice Admiral Mauney at Fort Meade in March 2010.

17. USCYBERCOM Chief of Staff's office, e-mail to multiple recipients, "Report Card on CDR's [commander's] Priorities—New Weekly Reporting—Due 4 Aug," July 27, 2010.

18. USCYBERCOM J0, "USCYBERCOM's Road to Full Operational Capability [FOC])," Information Paper, August 11, 2010 (U/FOUO).

19. Deputy Secretary of Defense to Commander, USSTRATCOM, "Full Operational Capability (FOC) of US Cyber Command (USCYBERCOM)," October 31, 2010,

20. Keith B. Alexander, "Building a New Command in Cyberspace," *Strategic Studies Quarterly*, Vol. 5, No. 2, Summer 2011, pp. 3-4.