What U.S. Cyber Command Must Do

By WESLEY R. ANDRUES

In June 2009, the Secretary of Defense announced the creation of U.S. Cyber Command (USCYBERCOM), a new subunified command to be led by the director of the National Security Agency (NSA). While the press colored the announcement with Big Brother undertones and hints of civil liberties surrendered, the real story lies in the intriguing legal landscape of USCYBERCOM and what it could mean for the security, efficiency, and economy of the military's networks. The Department of Defense (DOD), the largest single consumer of Federal information technology dollars, has struggled for decades to bring a singular voice and management process to its communications infrastructure. Although this is not the stated intent of the new command, USCYBERCOM must ultimately reconcile its role in information technology "ownership" and draw clear operational boundaries if it is to administer cyber security through unified standards and procedures.

As USCYBERCOM now has its first commander and begins shaping its core functions, fundamental changes in the legal landscape must occur in parallel with the new organizational structure if the command hopes to effect a "comprehensive approach to Cyberspace Operations."[1] In short, it must go beyond cosmetic organizational change and set to work on a campaign that genuinely reduces interdepartmental friction, repairs ailing processes, and truly empowers it to meet its mission, both specified and implied.

Step One: Establish Priorities

To compel its components to organize confidently and appropriately, USCYBERCOM must provide solid, intuitive operational imperatives and priorities. What tangible problem does the command seek to solve, and how does the formation of this single entity contribute to the integrity of DOD networks? One of the main impediments to answering this question is the lack of any meaningful cyberspace doctrine, or at least a serious consideration of how *cyberspace operations* differs from the closely related *computer network operations*, which is itself a key component of *information operations*. How does the emerging rubric of *cyber* now fit against the

Wesley R. Andrues is the Plans and Readiness Division Chief for the U.S. Army Global Network Operations Center.

broad operational backdrop of information operations as a whole? This is an elemental question that demands top-down clarification if USCYBERCOM expects to contain its mission space and lead decisively. The question must be answered: Is it about securing the *network* itself, or achieving military effects through the targeted application of *information in all its forms*? To call it both takes a middle road that complicates the identity of this new command and makes task organization exceedingly difficult.

It is not that DOD has failed to invest intellectual capital toward defining cyberspace. On the contrary, a good deal of self-examination is under way across all the Services, yet precious little substance has emerged signifying a strong, novel environmental foundation. To its credit, the Joint Staff devoted significant effort toward articulating broad cyberspace priorities in its *National Military Strategy for Cyberspace Operations* (2006). The basic premise echoed the notion that the United States must secure freedom of action in a "contested domain" and deny the same to its adversaries, yet its ambitious goal of achieving "military strategic superiority in cyberspace" glosses over the vast complexity of such an all-consuming endstate.

While the initial overtures at shaping USCYBERCOM have been well intentioned, it seems much of the doctrinal preamble has been disregarded in favor of organization for organization's sake. Although cyberspace proponents would argue that indeed there is enough basis to begin marshaling forces in earnest, the questions remain: what forces, where, and how? The standard litany of network threats and corresponding vulnerabilities sounds a familiar rally call, and while it is certainly true that bad people seek to do bad things to DOD networks, the best defense may lie in some decidedly familiar tactics. Information assurance, computer network defense, and computer network response actions have long been the weapons of choice in safeguarding DOD information, yet they have become upstaged by the new if not ill-defined focus on cyber. Cyberspace doctrine must demonstrate why those separate but complementary families of activities have failed DOD thus far and how a subunified command would distill them into a responsive and value-added operational art.

DOD (Cherie Cullen)

Gen Keith Alexander, commander, U.S. Cyber Command, speaks at activation ceremony

Perhaps real cyberspace doctrine should do little more than paint a gap analysis, demonstrating in meaningful terms how the existing ingredients of cyber security would be more effective under a central commander than distributed to those with a custodial responsibility for the network. Depicting the mission space with appreciable detail and articulating a handful of clear employment principles unique to USCYBERCOM may be the most important doctrinal first steps.

Step Two: Come to Consensus

While the cyberspace landscape is composed of innumerable stakeholders, there are at least two key positions to consider as USCYBERCOM begins to coalesce: the director of the NSA and the DOD Chief Information Officer (CIO). Both carry network security responsibilities born from law, and each controls a vast apparatus that validates the integrity of the military's networks; however, unless they can complement one another's mission areas, their overlapping responsibilities may hobble the effectiveness of a new command devoted exclusively to cyberspace operations and security.

At the heart of the overlap lies the working definition of DOD information systems. Are they no more than a collection of assets under a Federal manager, or do they assume the collective importance of a National Security System (NSS)? This blurred relationship has dogged the office of the CIO for some time. For example, in 2005 the DOD Inspector General declared that DOD "has not established a complete inventory of its information systems or consistently defined an information system."[2] This lack of a culminating definition stems more from the copious actors in the organizational soup than the inability to objectively define a box on a desk. For as elementary as it may seem to manage all military information technology (IT) as a commodity, the model is somewhat cleaved by the CIO's fiscal responsibility and NSA's de facto role as the guardian of the NSS. USCYBERCOM may well find itself working to suture this divide as it mandates security writ large and advocates for a homogenous set of protections. A case in point is the DOD planned IT capital investments for fiscal year 2010, which consist of nearly 6,000 line items, totaling over $33 billion.[3] With program titles running the gamut from Army Food Management Information System to DOD Pharmacy Data Transaction Service, there is a staggering amount of network and computing space to be considered as USCYBERCOM weighs its operational reach. If the network is viewed as a distributed series of Federal systems, then the central themes of the Federal Information Security Management Act arguably apply, and the

although cyberspace proponents would argue that there is enough basis to begin marshaling forces in earnest, the questions remain: what forces, where, and how?

DOD CIO (under the Office of Management and Budget) need only "provide information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access."[4] This formula seeks to reduce risk to an "acceptable level," applying fiscal tradeoffs based on the importance of the information system at hand.

Conversely, if the entire network is looked upon as an NSS (or perhaps even a "weapons system," as some have come to describe it), then a more exclusive set of protections is called for, meaning the network "shall be secured by such means as are necessary to prevent compromise, denial, or exploitation."[5] This nuance would favor a more pivotal role for NSA, whose influence on planning and programming information systems could feasibly eclipse that of the CIO. The Army Food Management Information System potentially becomes more than a mere line item among other disembodied enclaves; rather, it would be an integral part of a security system whose compromise is deemed unacceptable. Although accreditation processes exist today that establish nominal protections for all of these systems, they are little more than one-time approval events or periodic inspections with no long-term defense structures included. Under USCYBERCOM, each activity must ask itself the standing question, "Do I have the capability to validate the integrity of my network or application and increase the security of this system on demand?"

While certain checks and balances will, by legal necessity, continue to underlie the funding and administration of the military's networks, a new comprehensive charter must put to rest any confusion over how the overall network is defined and stratified by importance. Where CIO policies allow for a continuum of cost-appropriate security controls associated with the importance of the information, a new USCYBERCOM charter may, by necessity, impose more draconian protections and interoperability standards. By virtue of its advertised mission alone, USCYBERCOM must become the de facto network architect and chief advocate, for it cannot direct defensive action on a network incapable of executing its commands. One seemingly innocuous configuration change can introduce a bow wave of costly and lengthy implementation challenges among components. This is due largely to the fact that Service acquisition channels are diffuse and decentralized, and network enclaves can vary widely even within a single military branch.

In short, if USCYBERCOM is to engineer responsive processes and dictate universal protective measures on demand, there cannot be several versions of a network or multiple flavors of information security—one for the NSS and one for other "Federal" systems. Unless formally reconciled, this dichotomy potentially undermines USCYBERCOM unity of command, clouds resourcing decisions, and dilutes operational outcomes.

if USCYBERCOM is to engineer responsive processes and dictate universal protective measures, there cannot be several versions of a network or multiple flavors of information security

Naval officers conduct development test for Operational Adaptation Integrated Technology Demonstration to integrate information for warfighters

DOD (Cherie Cullen)

Step Three: Resolve Classic Tensions

The Goldwater-Nichols Department of Defense Reorganization Act of 1986 sought to meld the DOD tectonic divide between operational and administrative control of military forces. The same kind of studied treatment must be given to cyberspace and the way it is fielded, maintained, commanded, and controlled. The opinions and political implications are likely to be as contentious as those surrounding Goldwater-Nichols itself, but the Gordian knot of "who controls the network" must be put to high-level debate and codified in law, policy, or both. How USCYBERCOM organizes and executes its mission will be largely reliant on how DOD regards cyberspace—whether or not it is a single, ubiquitous, centrally managed entity, or a distributed network conjoined through diffuse pockets of geographic responsibility. While both are feasible, they must support the USCYBERCOM commander's most basic litmus test: Can I confidently, on demand, determine the identity and extent of the network, and can I make objective assessments on the state of its integrity? Can I then implement configuration changes to appreciably enhance security from end to end?

Building an apparatus to answer these elemental questions would bring unprecedented organizational pressure onto DOD, as configuring for that capability would take the measured commitment and cooperation of everyone who touches a computer or radio set. If the commander of USCYBERCOM is ostensibly the sole recognized individual to make risk assessments for the network, a shared sense of urgency and a set of uniform response measures must exist for all components, regardless of the real estate they occupy or the organizational patch they display.

What cannot be ignored is that, once fully operationally capable, USCYBERCOM will be legitimized by a base execute order from the Secretary of Defense that will bestow it with the authorities needed to empower it on some global level. The question remains, however, of who will be required to abide by those authorities, and whether this party will recognize a command structure that straddles both Service and geographic concerns.

Other core professions beside cyberspace wrestle with this murky equation, namely the logistics community, which continues to proclaim that split authorities fundamentally impair mission effectiveness. Possible avenues of compromise for logistics, cyber, and any other global function include recharacterizing the Service Title 10 "sustain" contribution. Specifically, could computer security be considered a legitimate sustainment activity that is rightfully Service-owned to a predetermined point? Are there patently "operational" network activities that become the province of the theater commander when Service sustainment ends? Unless and until USCYBERCOM can draw these synthetic dividing lines and provide added value to the theater commander's mission, it is unlikely any significant progress will occur, and the tension between regional and global will remain for some time.

This may be yet another case where definitions of the network require a full makeover. Perhaps, like the NSS or an information system, a definition can be created that satisfies the theater commander and the assets within the geographic region while still supporting Service reach. The notion of a "global network" briefs well, but articulating the complex relationships within that network will be nothing short of mapping the human genome, an arduous but necessary step in managing expectations and empowering a single commander to operate on a nominal level.

Step Four: Define Cyber Forces

Despite the relative immaturity of the USCYBERCOM mission space, the term *cyber forces* is beginning to enjoy common use as though its meaning is intuitive. Yet because of the novelty of USCYBERCOM and its still evolving mission, cyber forces are far from readily understood or objectively applied. In fact, the term's use adds a dimension of complexity to an already years-old initiative to define an information operations career force. Sculpting an IO career force has been a department-wide mandate since DOD Instruction 3608.11 charged the military with creating a force to "plan and execute fully integrated IO."[6] Although USCYBERCOM—a new entity on the IO scene—cannot singlehandedly carry out the task of defining all IO forces, it is at least obligated to serve as the operational advocate for its cyberspace career force equities.

To date, no all-inclusive IO career structure has been codified, due largely to a lack of Service consensus on the extent and makeup of core IO skills and force composition. Thus, the key intent of the DOD instruction—to establish policy, definitions, and responsibilities for the force—has not yielded a decisive deliverable. Recent assessments from both the Under Secretary of Defense for Intelligence and U.S. Strategic Command (USSTRATCOM) have revealed numerous systemic problems in achieving, training, and sustaining a holistic IO force.[7] Although cyberspace forces represent a comparatively small slice of the greater IO talent pool, an objective and clearly understood cyber career force is likely to be just as elusive in its definition. It could be argued, after all, that everyone who touches a keyboard, from Servicemember to contractor, is a default member of the cyberspace rank and file. Even those who possess the rightful credentials to be part of a distinctive "cyber force"—for example, an Air Force communications officer or a civil servant who manages IT acquisition—may at times serve in fringe positions unhitched from any mainstream association with "cyberspace operations."

no all-inclusive IO career structure has been codified, due largely to a lack of Service consensus on the extent and makeup of core IO skills and force composition

The scope of cyberspace goes well beyond an isolated segment of DOD's vast Active, Reserve, civilian, and contracted population, and in order to develop a workable training and sustaining framework, USCYBERCOM must articulate who exactly makes up the fraternity of "cyberwarriors" operating and defending the network. Will an entirely new skill set inform the development of a new kind of work force, or will age-old specialties continue to exist, separate but equal, under the loose but unifying banner of cyber?

U.S. Air Force (Jerry Morrison)

Deputy Secretary of Defense makes presentation at cyberspace symposium

Step Five: New Rules of Engagement

Closely related to the underlying Service/combatant command schism, DOD standing rules of engagement (SROE) present a host of procedural and organizational challenges for USCYBERCOM. At its heart, the SROE advocate for the inherent right of self-defense for all geographic combatant commanders, thus giving them the autonomy to plan and conduct cyber operations as conditions dictate, theoretically free from USCYBERCOM control. While the creation of USCYBERCOM alone will not compel a rewrite of the SROE, this new command is nonetheless an element to be considered in the next iteration of the Chairman's instruction, and emerging relationships must carefully consider the command's span of control, especially in terms of operational preparation of the environment (OPE).

This notion of OPE is a nontrivial element in determining how USCYBERCOM will integrate with other combatant commands, particularly for intelligence-gathering. Where geographic combatant commands enjoy legitimate latitude under OPE to assess regional adversaries, the same may not legally hold true for USCYBERCOM, even though its commander must, at any given moment, possess a cohesive and decisive state of the battlespace. Any claim by the commander of USCYBERCOM to this OPE privilege, however, begins to suffer when one considers that he also wears the hat of the NSA director. Prevailing thought, however, wants to ascribe classic command authorities to USCYBERCOM regardless. The commander of USSTRATCOM, General Kevin Chilton, USAF, explains on the subject of computer attack: "Most of the work that needs to be done before the [cyber] attack is [intelligence-centric], and it's very critical to it. But in my view, this is not an [intelligence] mission. This is a combat operation that requires exquisite [intelligence] support, just like every other combat operation."[8] Several questions then follow: Which combatant commander would take on this "combat operation," and how would it be synchronized globally? And what of U.S. Northern Command? Would it fit that traditional combatant command model within the continental United States, or be trumped by the laws governing the military and domestic intelligence?

Despite the creation of USCYBERCOM as a command entity, joint rules of engagement may remain one of its most vexing operational challenges. Nothing should be imposed that dilutes the authority of the geographic combatant commands, yet at the same time, something must be promulgated to account for and to instantiate USCYBERCOM's global role, especially as it relates to intelligence.

Step Six: Avoid Escalation of Hostilities

More than the nefarious appearance of the government's impact on civil liberties, the real concern with USCYBERCOM should be in the way that it is perceived by world partners at large. This public and deliberate creation of a new command presents the outward face of a military arm with a predilection for "preemptive" actions in cyberspace. Because the so-called adversary is all but invisible, however, and hostilities can be obscured in a global miasma of virtual identities, USCYBERCOM will bear the perennial responsibility of "connecting the dots" to form an unassailable case for action, either defensive or offensive. The command must demonstrate tactical prudence, restraint, and transparency lest it become the target of blame for every inexplicable and potentially tragic cyber incident around the world.

To even presume that cyberspace is now a legitimate military attack vector or to issue a declaratory policy to that effect not only provokes America's adversaries (and domestic criminals alike), but also potentially upsets many long-held precepts of the Geneva Conventions, such as the protection of civilians. For example, if the United States were to one day retaliate in kind to a cyber attack against its infrastructure, it would be manifestly difficult to safeguard noncombatants against the resulting collateral damage. Yet long before this prickly scenario could even be played out, a number of critical determinations would have to be reconciled, such as what constitutes cyber hostilities. From whom did the attack emanate, and was the act sanctioned by the home country or cause? What is a proportional use of force in cyberspace? Will U.S. retaliation invite further attacks beyond what its defenses are capable of handing?

While USCYBERCOM planners will no doubt wrestle with these application-of-force issues for some time, their efforts should be guided by a sound body of rules and a deterrence policy rooted in an international construct. Some of the hallmarks of Cold War deterrence hold up to the medium of cyberspace deterrence, particularly in terms of the "general" and "immediate" approach. For instance, a general deterrence posture seeks to dissuade anyone with the fundamental capability to attack, while immediate deterrence singles out those with the presumed intent to carry out the attack. Of course, this blunt

LTG Carroll Pollett, director, Defense Information Systems Agency, addresses audience

U.S. Army (Eric G. Steen)

USCYBERCOM efforts should be guided by a sound body of rules and a deterrence policy rooted in an international construct

policy construct is only a starting point for deeper discussion and may not withstand the innumerable caveats that will permeate the debate as it relates specifically to cyber.

Although there are some noteworthy first steps toward establishing an international set of cyber norms—evident in bodies such as the Convention on Cybercrime—any global framework governing military response actions in cyberspace will surely materialize at an onerous pace. After all, how can the rules of war, built upon the tactile presence of combatants and weapons and sovereign territory, be retooled for a world where "troops" can be dispatched in milliseconds from a multitude of nation-states?

U.S. Air Force (Scott T. Sturkol)

Airman operates computer network to sustain, troubleshoot, and repair standard voice, data, video network, and cryptographic client devices

But Can It?

Although USCYBERCOM is emerging as a unique DOD entity—an entirely new departmental approach to network security and operations—its ability to influence cyberspace's underlying organizational impediments is potentially limited. Objectively speaking, there is only so much a subunified command can do to generate the kind of widespread change needed to set environmental conditions. Although the commander now exercises "authoritative direction over all aspects of military operations, joint training, and logistics," this authority by itself may not go far in creating the sea change needed for this new mission area.[9]

That said, there are undeniable handholds within current doctrine that may allow USCYBERCOM to exercise something more than just a titular presence in cyberspace. For example, the inherent Directive Authority for Logistics power that the commander wields legitimately presents him with a possible means for optimizing resources and prevents duplication of effort among Service components. In the context of cyberspace, this may mean the commander carries a significant influence over resourcing activities that occur well upstream of new technologies and acquisitions. Though he is perhaps not the sole recognized chief architect, the commander of USCYBERCOM may at least evolve into the "chief aggregation officer" for DOD networks.

To that end, the commander will enjoy sizable influence in network configuration and the interoperability of network components, especially as USCYBERCOM's mandate to gain situational awareness into the networks looms large. An interesting analogue to this scenario can be seen, again, with the logistics community. Although U.S. Transportation Command (USTRANSCOM) bears the overall responsibility for in-transit visibility of logistics, it has not yet delivered on this critical task. A recent Government Accountability Office report states, "Because DOD has lacked a coordinated and comprehensive approach to managing joint theater logistics, efforts to advance joint theater logistics across the department have been fragmented."[10]

the commander will enjoy sizable influence in network configuration and the interoperability of network components

Much like USCYBERCOM, this fragmentation in materiel delivery has caused many to advocate for a U.S. Joint Logistics Command that would consume the gamut of logistics missions that currently straddle USTRANSCOM, the Defense Logistics Agency, and the Service logistics entities. Ultimately, this command would assume responsibility for the global end-to-end supply chain.[11] Thus, it is not without precedent that USCYBERCOM should be heralded as an emerging solution for the military's continuing shortfalls in operating and securing its information systems. And as USTRANSCOM controls the crosscutting $10 billion Transportation Working Capital Fund, so too should USCYBERCOM control a segment of funds devoted exclusively to cyberspace operations. Although this premise is tenuous at best—especially as it applies to the ethereal world of cyberspace—it offers an area of further study that may well pay literal dividends for the USCYBERCOM commander.

In the end, there is potential for a subunified command to make a tangible impact on a functional area such as cyberspace, but until there is constituent change in the fabric of cyberspace doctrine, policy, and resource control, USCYBERCOM may emerge as a well-intended office whose real authorities prove negligible in the long run. **JFQ**

NOTES

[1] Secretary of Defense Memorandum, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," June 23, 2009.

[2] DOD Inspector General Report D–2005–029, "Quality Integrity Accountability Management of Information Technology Resources Within DoD," January 27, 2005.

[3] DOD Information Technology Budget Exhibit, Fiscal Year 2010, President's Budget Request, May 2009.

[4] Office of Management and Budget Circular No. A–130, "Management of Federal Information Resources," appendix III, "Security of Federal Automated Information Resources."

[5] Committee on National Security Systems Directive 502, "National Directive on Security of National Security Systems," December 16, 2004.

[6] DOD Instruction 3608.11, "Information Operations Career Force," November 4, 2005.

[7] DOD Inspector General Report D–2009–090, "Information Operations Career Force Management," July 2, 2009.

[8] General Kevin P. Chilton, USAF, remarks delivered to the LandWarNet Conference, Fort Lauderdale, FL, August 21, 2008.

[9] Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, May 14, 2007).

[10] Government Accountability Office Report, "Efforts to Improve Distribution and Supply Support for Joint Military Operations Could Benefit from a Coordinated Management Approach," June 2007.

[11] Defense Science Board Summer Study on Transformation, "A Progress Assessment, Volume I," February 2006.