Master Sergeant Charlie Sanders (left) and Captain Lashon Bush work on Mission Event Synchronization List in Joint Cyber Control Center during Operation *Deuce Lightning*, Grafenwoehr, Germany, February 2011 (U.S. Army/Lawrence Torres III)

# A Theater-Level Perspective on Cyber

By J. Marcus Hicks

*Gentlemen, the officer who doesn't know his communications and supply as well as his tactics is totally useless.*

—General George S. Patton

Most U.S. military cyber professionals will tell you that "defense is the main effort" and that providing secure and reliable communication is job one. In practice, however, most cyber discussions focus on sophisticated computer hackers conducting exploitation (espionage) or attack (sabotage) operations. The reasons for this seeming contradiction include cyber espionage intrusions, industrial-scale intellectual property theft, and denial-of-service attacks that cost millions of dollars and naturally capture headlines and the imagination. Likewise, the potential for cyber attacks to disrupt infrastructure with kinetic-like consequences provides fodder for books and articles that bridge reality

Major General J. Marcus Hicks, USAF, is Director of Operations, Headquarters Air Force Special Operations Command.

and science fiction, empowering armchair theorists to contemplate a new and different type of war and warrior.

Still, the military's main effort must be to provide, operate, and defend the ability to command and control (C2) forces. If we fail at this task, the commander's mission will likewise fail. Effective command, control, communications, and computer systems define the modern American way of war. This requires highly technical systems, consuming large amounts of bandwidth to support the intelligence, surveillance, and reconnaissance mission requirements that feed the C2 system. Our high-tech advantage enables and arguably defines much of the conventional overmatch currently enjoyed by the U.S. military and its allies. Our operational concepts assume levels of situational awareness and the ability to control forces with a level of precision unimagined a generation ago. To maintain that advantage, I too agree that defense is the main effort and that we must keep it the main effort.

In this article, I offer a theater-level perspective of cyber and hope to provide a view of what is in, what is out, how we are doing, where the thorny issues lie, and finally, some thoughts on a way ahead. This is not a new discussion, and I do not have all the answers, but I do have a unique perspective. From 2011 to 2013, I served as the U.S. Pacific Command (USPACOM) J6 as well as the director of the USPACOM Joint Cyber Center (JCC). My responsibilities included the cyber portfolio for over half the world, ranging from traditional J6 command, control, communications, and computer systems to the emergent mission of offensive cyber operations. As a career Air Force Special Operations pilot, I came to the cyber discussion with few preconceived notions or paradigms to shatter.

Managing the J6 portfolio, I was impressed with how strongly planning, architecture, and engineering efforts (provisioning) inform resilience and defensibility (operate and defend) and even offensive considerations (exploitation and attack). The reverse is also true. The more I learned about cyber, the better communicator I became. If we add to this portfolio the need to coordinate with allies, partners, and emerging partners, then cyber looks like an increasingly operational and inherently coalition activity. A few of my observations may be controversial, but most will be common knowledge to communicators and cyber professionals. My target audience is the operational community because I believe that command, control, communications, and cyber are a commander's business.

First, I have developed an expansive view of cyber, seeing no meaningful difference between information technology (IT) and cyber. Virtually everything is in—from the core of traditional communications and signals intelligence disciplines to command and control programs of record. Radio frequency (RF) spectrum management, telephony, crypto-management, security policy for information-sharing, and intelligence support to signals intelligence are all cyber or cyber-related activities. The current Department of Defense definition of *cyberspace* is "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1] Consistent with this definition, even administrative systems used to process sensitive information, support decisionmaking, or transmit decisions can be part of the C2 process even though they are not a recognized program of record. Cyber capabilities are essentially a high-tech, high-speed successor to written communications, maps, and calculations, providing intelligence and C2 capability. Like dispatches carried by riders on horseback a thousand years ago or conveyed by the telegraph a hundred years ago, cyber is subject to the vulnerabilities of intercept, exploitation, and disruption. The Great Game has entered the computer age.

Thus, I find it counterproductive to seek cuts in IT while investing in cyber capability. I do support seeking efficiencies in IT, cyber, or any other endeavor, but not at the expense of operational capability. Cutting manpower to operate military networks consistent with lean corporate models may work in peacetime, but it may not leave sufficient personnel expertise in the right places to operate and defend networks in a contested environment.

I generally agree with the conventional wisdom that separates traditional information operations and electronic warfare (EW) from the cyber enterprise. Cyber may enable information operations, but its discipline exists apart from the technology-centric cyber realm. Electronic warfare, however, is a more difficult question because it straddles the cyber fence. One could argue that anything involving RF spectrum management or controlled by computer processes with any external interface should be considered part of the cyber domain. Accordingly, EW could be part of the cyber enterprise, and I suspect it will migrate in that direction.

Second, cyber is an increasingly operational activity. The American way of war heavily relies on cyber capability. Furthermore, given the increasingly contested cyberspace domain, it follows that cyber capability must represent a substantial focus for the military. The military recognized this initially in standing up the Joint Task Force Global Network Operations and, more recently, U.S. Cyber Command (USCYBERCOM). Still, much of the cyber overmatch we currently enjoy developed from long periods of operations in Iraq and Afghanistan, against technologically unsophisticated adversaries, which provided a virtual sanctuary for our own capabilities. As we withdraw from Afghanistan, worry about Iran, and rebalance toward the Pacific, we have a renewed and increased emphasis on developing and maintaining our ability to operate in contested and denied environments against technologically sophisticated adversaries. Recognizing that potential adversaries pose threats to our intelligence, logistics, and C2 functions, commanders and the operational community are realizing that we must treat cyber more like an operational activity and less like an administrative support function. This makes sense since the C2 system is effectively the commander's primary weapons system. Thus, the capabilities provided by cyber are operational imperatives and truly a commander's business.

Third, cyber is inherently a coalition activity. Whether the mission is humanitarian assistance and disaster relief or combat operations, the United States rarely goes it alone. We maintain treaty alliances across the globe, continually seek to improve relations with existing partner nations, and expand partnerships with others. We aim to improve collective security and reduce the possibility of miscalculation where tensions exist by leveraging coalitions and their capabilities. These activities require varying degrees of information-sharing with substantial policy and technical implications.

Like other geographic combatant commands, USPACOM engages with more than 20 allied, partner, and emerging partner states across the Pacific to evolve and improve communications interoperability through activities such as RF spectrum management, security policy agreements, tactical data-link coordination, and crypto-management. These activities are as far from hacking as possible, but they provide the foundational elements of cyber and are critical to the main effort.

Foundational cyber activities directly address the combatant commander's priorities of strengthening relationships with allies and partners and building partnership capacity. The cyber security instruction we offer during bilateral and multilateral engagements consists primarily of best practices from the disciplines of information assurance and computer network defense. These offerings are increasingly popular and have served not only as catalysts for relationship-building but also as necessary preconditions for the development of secure, trusted, and reliable information-sharing capabilities. If we hope to operate successfully with allies and coalition partners, we must invest in relationships and cyber capabilities with integral mission partner capability.

Fourth, cyberspace has a global and regional component. Like other traditional military activities, cyber has a global and regional element. We recognize that the domain is too large and activities too complex to be centrally managed by a single operations center. At the same time, however, the physical characteristics of the global information grid (GIG) do not lend themselves to purely regional control. Thus, we need to strike the right balance between global and regional equities. From my perspective, we should err on the side of giving geographic combatant commanders more capability and authority to plan to create cyber effects as well as command and control their command and control, or as Admiral Robert F. Willard often stated, their C2 of C2.

Fifth, because cyber has become so critical to the American way of war, I see real value in having a single organization within a combatant command manage the entire cyber portfolio. In particular, I value the current Joint Cyber Center (JCC) construct that combines all cyber activities from across the command staff. In the legacy construct, the J6 manages the "provide, operate, and defend" portfolio; the J2 works exploitation through intelligence channels; and the J39 supervises the cyber attack mission under the information operations rubric. Some other variant could work, but my experience suggests that operationally minded individuals viewing challenges through a cyber lens would develop more holistic and innovative solutions than could be achieved by individuals from organizations that support cyber as a collateral duty. Simply put, because cyber is its primary focus and singular mission, the JCC can focus more energy into this critical and dynamic domain. In other constructs, cyber could be rendered a secondary focus in organizations with competing domain demands, such as the J2 or J3.

The objective of a JCC, with the entire cyber portfolio, is to develop an operationally focused tool for the commander in partnership with the rest of the J-staff. Advantages include inherent efficiencies of remaining within an existing staff organization for administrative overhead, which also allows for dual-hatting of certain low-density JCC and J6 personnel. More importantly, the JCC integrates directly into the theater commander's decision cycle through battle rhythm events, thus retaining cyber decisions at the theater commander level and avoiding bifurcating C2 by outsourcing critical C2 functions to a separate component. Thus, the USPACOM Joint Cyber Center operates with some characteristics of a separate component, but one more efficient and closer to the theater commander. Many constructs could work, and I do not favor a one-size-fits-all approach or a centrally directed solution. We will need to experiment and evolve as conditions dictate. Availability of resources, more than any other condition, will suggest the best organizational construct. Combatant commands with fewer cyber resources will organize differently than those with more assigned cyber forces. Similarly, subunified commands and component commands may organize differently from their combatant command as circumstances dictate.

## How Are We Doing?

From the "provide, operate, and defend" side, cyber has rapidly evolved from Service-provided administrative IT systems with some connection to dedicated C2 systems to become critical warfighting systems for the joint force. Unsurprisingly, the pace of change has left suboptimal legacy infrastructure in place that renders it more difficult to operate and defend. Concurrently, cost savings measures have centralized operations and stripped system administrators—read "cyber operators"—to levels more in line with corporate IT structures than operational C2 systems. Similarly, outsourced contracts maintain Service-level agreements that are optimized more for routine, peacetime operations than for exercises or contingencies. Taken together, it is easy to see how over-centralization of operations centers and minimal manning could lead to capacity overload with anything other than a routine disruption, which might be an acceptable level of risk if the networks were purely administrative. Since, however, we have built a concept of operations that relies heavily

Secretary Hagel tells troops cyber may be biggest threat to U.S. security (DOD/Erin A. Kirk-Cuomo)

on our overmatch in C2 capabilities, those capabilities must be operated and defended as a weapons system.

Operationally responsive networks do not rely heavily on compliance-based security measures. Centrally mandated security policies enforced across the enterprise through a rigorous inspection regime are necessary and show progress toward treating cyber as an operational domain. However, the ability to dynamically adjust security policies, to sense—rather than inspect for—compliance, and to isolate compromised portions of the GIG before a risk to one becomes a risk to all is critical to ensuring secure and resilient operational capability. My experience through exercises and contingencies unambiguously suggests that we must develop a concept of operations, capability, and capacity to defend, recover, and reconstitute our cyber capability in the face of a contested environment.

By way of analogy, every Air Force aircraft I have flown comes with technical orders (TOs) on maintaining and operating them. For example, the TO AC-130U-1, known as the "dash one," is a massive volume of procedures for operating the AC-130 gunship. Like in all dash ones, chapter three is dedicated to abnormal and emergency procedures and includes certain emergency procedures (EPs) deemed sufficiently critical to commit to memory, verbatim. These "boldface EPs" cover time-sensitive, life-threatening eventualities, such as engine fires and loss of cabin pressure. Before flying an aircraft, fully qualified pilots must first study normal and emergency procedures, demonstrate unerring understanding and recall of boldface procedures, and train for their practical implementation in high-fidelity simulators. Much routine training is dedicated to operating with degraded systems and addressing emergencies. This is pretty standard for operational weapons systems. Similar analogs exist on ships, in missile silos, and more.

Unfortunately, this analog breaks down for network operations. Technical specifications normally exist and system administrators are often highly skilled, but networks are not treated as weapons systems. The vendor providing a network does not provide a dash one or even anticipated failure modes that would normally constitute "chapter three." Thus, networks that are not treated as weapons systems lack boldface EPs and deliberate processes for training to operate when under attack or degraded due to a natural disaster. Those networks are not easily severable to isolate damage or infected enclaves. Nor are they capable of providing enhanced security for the most critical systems or information. At USPACOM, we have demonstrated time and again

Admiral Michael Rogers addresses audience and workforces of U.S. Cyber Command, National Security Agency, and Central Security Service at his assumption of command ceremony, April 2014 (National Security Agency)

that the implementation of responsive network security measures is ponderous and inexact due to complex C2 arrangements, insufficient manning at major operations centers, a dearth of network instrumentation, or an inability to take action at a regional location due to excessive centralization.

We have built in these foundational problems by making our C2 system reliant on economically efficient networks originally deployed by the Services as administrative tools. Additionally, we have centralized network operations and reduced manning to such an extent that only routine technical problems are easily manageable. Service-level agreements with contractors are not responsive to operational requirements in exercises and contingencies. Centralization by definition reduces regional capability. Excessive centralization leaves combatant commanders little or no capability to manage risk across the areas and operations for which they are responsible.

## A Way Ahead

Although the current state of cyber may seem less than ideal, there is reason for optimism. Much has been done already to set conditions for success in the cyber domain. Additional resourcing and the standup of USCYBERCOM and combatant command JCCs are the most obvious examples. Ongoing discussions about workforce development and the Joint Information Environment (JIE) give further reason for hope. Still, as we set the framework for future cyber capabilities, getting it right is critical, and the time to act is now.

Developing an operationally minded cyber workforce is a critical requirement. Born of the communications and intelligence disciplines, the cyber community has leveraged career operators to provide an operational focus for traditional supporting functions. Reminiscent of the early days of carrier aviation, cross-decking traditional operators to provide a cadre of senior officers to advance a new concept is a sound and proven technique. Creating operationally minded cyber operators from the beginning of their careers will be necessary for the long term and constitutes the real test.

As the Services struggle with this effort, aviation provides another useful analog. Like aviation, cyber requires many disciplines and training standards across a multitude of mission areas to function properly. Therefore, just as the aviation community is made up of pilots, maintainers, air traffic controllers, weather specialists, airfield managers, engineers, and more, we should embrace the notion that many different career fields will make up the cyber enterprise. Network operations personnel should have different training and follow a different path than those trained in exploitation or attack missions. Like pilots of different aircraft performing different missions, cyber operators will have different specialties at the tactical level. Most officers, however, should broaden across other specialties as they progress through their careers in preparation for leadership of larger, more diverse organizations.

Said differently, we do not have to recruit and train every cyber professional to the same standard. We can recruit a variety of talents and use them appropriately without trying to train everyone as a hacker. The challenge lies in ensuring that all career paths remain competitive for leadership opportunities at all levels, lest we create a class system with all its negative connotations.

Like pilots, all cyber operators will need a basic knowledge and skill set. Also, they will need advanced knowledge and skill in their particular tracks. Here, the track seems to split between defense and offense, between those with the "provide, operate, and defend" mission and those on-net operators with the "exploit and attack" mission. I recommend that we send quality individuals to both tracks because I am not convinced one is inherently more difficult than the other. This is particularly true if we operate and defend the networks as a weapons system, especially in a contested environment. Additionally, since defense must remain the main effort, we cannot let it become viewed as a second-class activity.

Along with personnel, we need to field the best equipment we can afford to avoid taking a proverbial cyber knife to a cyber gunfight. Fortunately, a solution is in our grasp as long as we focus on operational capability and not IT efficiencies.

Developing an operationally responsive infrastructure is a critical requirement. Deployment of the JIE can solve most of our cyber material shortfalls so long as the focus remains on ensuring that the next generation of military networks provides defensible warfighting capability to commanders. The effort originated as "IT Efficiencies" and morphed into "IT Effectiveness" before becoming the JIE, so there will always be a healthy emphasis on cost savings. The JIE aim, however, is to improve information capability and network defensibility through network normalization, a single security architecture, and reduced infrastructure where consolidation and other best practices make sense.

Given the criticality of cyber to coalition effectiveness and interoperability, we require the inclusion of coalition capability into the next JIE stage. Leveraging commercial solutions for classified networks, we envision rapidly establishing a specific network enclave for a particular exercise or event that coalition partners can join and use to share classified information releasable to the coalition members. When no longer required, the network enclave could be easily disestablished. This kind of flexibility could prove valuable across the operational spectrum from small-scale missions to large coalition operations.

The same technology, currently undergoing advanced testing, would also provide increased cyber situational awareness and defensibility. The design specifically allows for protection of certain enclaves or communities of interest. Thus, critical data will be more resilient and secure than the overall network, further improving cyber security through a defense-in-depth approach.

Vast distances and the maritime nature of the Pacific theater dictate a data center consolidation plan consistent with a potentially disconnected, intermittently connected, low-bandwidth environment. In anticipation of natural disasters or contingencies, redundant and dispersed data centers across the area of responsibility are crucial.

Finally, the operating concept for the JIE must provide geographic combatant commanders sufficient capability and authority to manage risk to their command and control while a global enterprise operations center manages risk to the global information grid. Consistent with other traditional military activities, disputes between geographic and global priorities would be arbitrated by the Secretary of Defense as the first common boss in the chain of command.

The exquisite command and control capability cyber provides represents a foundational aspect of current U.S. military capability. Since cyber and IT are indivisible, we must take a holistic approach to cyber. As the domain becomes increasingly contested, we need to operationalize cyber, and we fail to do so at our own peril. To do so, traditional operators should become more aware of and well versed in cyber, and cyber operators must become more operationally minded. We have an opportunity to develop the next generation of operationally minded cyber warriors who will underwrite the American way of war and create effects currently unobtainable. Necessarily, our next-generation warfighting network must be a weapons system for the next-generation war, not an administrative network for the interwar peace. Ultimately, cyber should be to the 21st-century military professional what logistics was to their 19th- and 20th-century counterparts: the discourse of professionals and the business of commanders. JFQ

## Note

[1] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, July 16, 2013).