LEARNING TO OPERATE IN CYBERSPACE

By Rear Admiral William E. Leigher, U.S. Navy

With the establishment of U.S. Cyber Command and cyber security a national priority, operations in the 'fifth domain' are under way.

The term "cyberspace" to designate a somewhat mystical and ever-evolving network of computers, routers, switches, and people emerged in fiction in William Gibson's 1982 novel *Neuromancer*. The definition usually cited from that work is: "a consensual hallucination experienced daily by billions of legitimate operators . . . a graphic representation of data abstracted from banks of every computer in the human system . . . *unthinkable complexity* . . . lines of light ranged in the non-space of the mind, clusters and constellations of data" (emphasis added).[1] The Department of Defense defines it as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] Further, cyberspace operations are "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[3]

The DOD definition is meant to categorize doctrinally what is and what is not a cyber operation. But what does Gibson mean by operating in cyberspace's "unthinkable complexity"?

The Reality behind the Words

Definitions continue to evolve. But the real work ahead is describing the model for operating in cyberspace in a way that is analogous to a description of operating in the maritime or air domains. Cyberspace is a domain, and the Navy needs to approach it as such. The relationship of cyber activities to those in the domains of sea, land, air, and space also must be defined. No domain stands on its own.

About four years ago, the declaration of cyberspace as the fifth domain did not come without pushback. The argument generally goes that sea, land, air, and space emerge from nature, but cyberspace is completely manmade. While this is true, one logical model is analogous to the thinking about and using cyberspace as an operational domain.

Dan Keuhl from the National Defense University developed a model that suggests networks, and the attached devices and software that we use, make cyberspace relevant in a military sense.[4] Counterparts in the other domains would be vehicles, ships, airplanes, and satellites. Operating in and exploiting cyberspace can be seen as parallel to operating in the other domains, in the sense that each has unique physical characteristics. In this way, cyberspace is physically just as real as the other four domains.

U.S. AIR FORCE (JEREMY BURNS)

A workforce must be developed with the skills to "live" on the network. In September 2010 in Grafenwoehr, Germany, international military members participated in Cyber Endeavor as part of the world's largest communications interoperability exercise, Combined Endeavor.

How the Navy Operates

After we accept cyberspace as a domain, our thought process can shift to what it means to operate there. Specific warfighting principles must be developed—though what we understand about operations in the maritime and air domains has general analogies in cyberspace. The current methods of operating in cyberspace are not serving the Navy as well as they should be. In fact, principles currently in practice would not be tolerated in any other warfighting domain. Here are some examples:

• In the 1990s, the Navy created the Navy Computer Task Force–Computer Network Defense (NCTF-CND), in response to intrusions into our unclassified networks. This command evolved into the Naval Computer Incident Response Team, and eventually the Navy Cyber Defense Operations Command (NCDOC). Throughout this evolution, sensors were deployed to better detect intrusion—and, while the sensors themselves evolved, the operational mindset has remained on forensic study of malware and patching. We have not developed our way of thinking to grasp an active defense against external threats that will both prevent penetration and neutralize threats discovered inside our networks.

This has led to an ever-stronger fortification of our networks, but it has not resulted in better defenses. Unauthorized users continue to penetrate networks, and ways in which we can use networks to our benefit are increasingly restricted.

• Current CND practice is fundamentally reactive, not the predictive system used in the other operational domains. A reactive system is signature-based, meaning it only recognizes malware that has been detected previously, and does not provide warning for new software or exploits used to penetrate networks. This sort of operational methodology worked for antiship missile defense and electronic warfare, because the radars that missiles use to obtain a final targeting solution were not easily reprogrammable. The approach fails in an information-age environment where software can be altered in minutes to completely change the nature of a threat.

• Networks are not operated with the same rigor as systems critical to other warfare disciplines. In a manner consistent with our network-defense philosophy, the Navy has deployed sensors to better understand how our data flow and bandwidth are used. Software has been customized to allow the Navy's network operating centers to monitor in real time the performance of individual nodes for a strike group or theater. Yet we do not routinely operate this way in support of the numbered Fleet commands' communications and networking. This

is analogous to radiating radar while having the repeaters throughout the ship switched off.

Life on the Network

Successfully operating in cyberspace will involve adopting a model significantly different from current practices. The U.S. Tenth Fleet is rapidly developing and implementing a philosophy that supports real-time network operations and defense. It is based on three principles:

- Assure that command and control (C2) is in place so forces can be used.
- Maintain freedom of maneuver in cyberspace to allow the Navy to fight in the manner desired.
- Provide non-kinetic effects, or military fires that do not depend on explosives to achieve a desired outcome—offensive and defensive—in support of joint and Navy commanders.

These three lines of operation are both parallel and sequential. The continuum between operating and defending networks begins with the requirement to provide assured, continuous C2 and extends to ensuring that the Navy can use cyberspace to its advantage. The adjacent range of operations involving exploitation and attacks in cyberspace makes use of the same freedom of navigation to move freely between protected operating areas and foreign cyberspace.

A key to operational success will be developing a workforce with the skills to "live" on the network. Our cyberspace operators must continually train and execute in the operating environment. In the same way, a submarine gains tactical advantage from operating in the subsurface environment while concurrently countering adversaries.

In cyberspace, this means developing defensive and offensive cyber-warfighting skills through "on-net" operator proficiency. The network has a character and flow that can be compared to the effects of weather or terrain in maritime and land domains. This sense of the domain has a direct relationship with tactics and the delivery of material in support of a campaign. Navy tactics, techniques, and procedures will evolve rapidly as Sailors gain operational-domain experience.

Defensive Actions

During peacetime and in phases 0, 1, and 2 of conflict, we are very comfortable thinking through the defensive aspects of warfare. Most of anti-air warfare is defensive in nature in that it protects high-value units, and much of the contemporary discussion about maritime and air domain is dominated by ballistic-missile *defense*. The same is generally true of antisubmarine warfare and a discussion of barriers and choke points. Thus, it is natural that defensive measures figure prominently in the cyberspace warfighting discussion.

The first step is to develop a strategy and set of operational practices to defend cyberspace as an operational domain. As for most such procedures, rules of thumb guide network defense. Number one is the 85 percent rule, referring to the percentage of problems normally confronting the Navy that basic network security can handle. This includes a modern operating system that is regularly patched, strong passwords, and sound training. Programmatic solutions primarily satisfy these responsibilities through servicing, manning, training, and equiping.

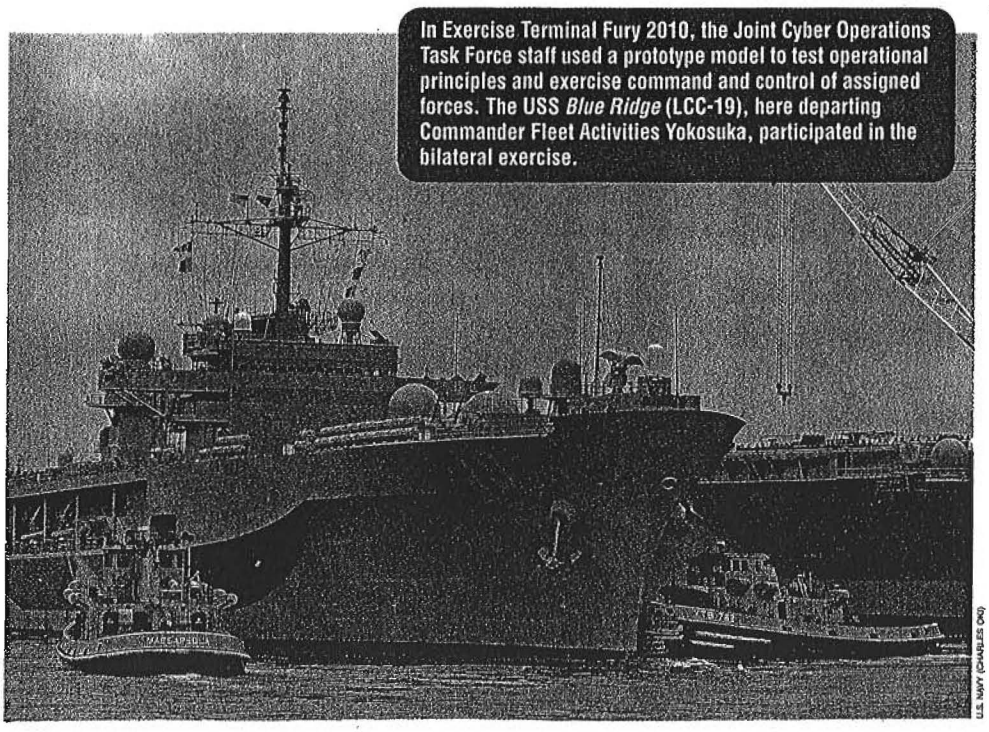
It is not unlike preparing for damage control. The remaining 15 percent of the problem is the dynamic part of network defense, where we confront adversaries and actors who, for varying reasons, attempt to penetrate Navy networks.

Aggressive Tactics

The tactics applied to the 15 percent solution include service and national sensors that are used to knock down known threats. This is the operational role of the network-defense service providers such as NCDOC. But there are shortfalls to a sensor- and/or signature-based system. As noted earlier, these capabilities have been deployed reactively instead of in a predictive way.

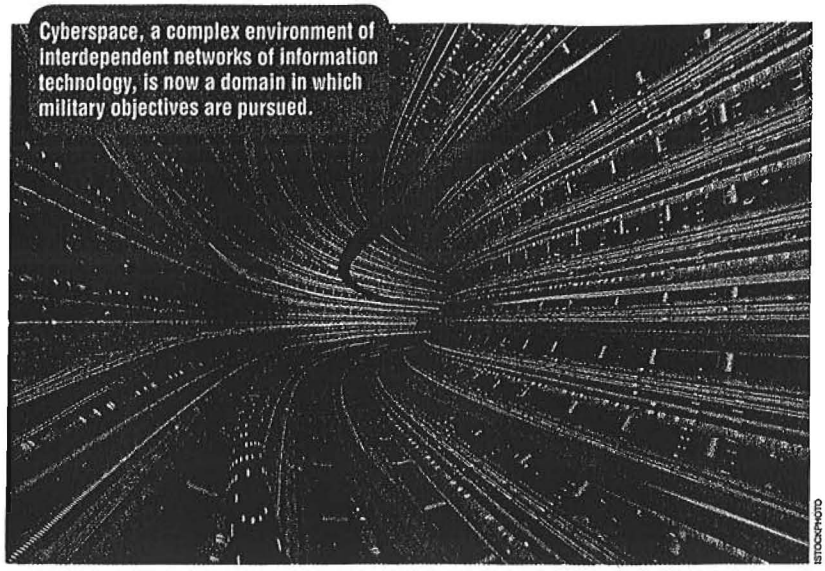
Even as we learn to use sensors in a real-time manner, operationally these systems have a significant shortcoming. Like the SLQ-32 Electronic Warfare system, they hit only on known radar signatures. This means that a network exploit not yet discovered is unlikely to be detected.

Changes to the cyber environment may happen instantaneously, so the sensor-based systems must



In Exercise Terminal Fury 2010, the Joint Cyber Operations Task Force staff used a prototype model to test operational principles and exercise command and control of assigned forces. The USS *Blue Ridge* (LCC-19), here departing Commander Fleet Activities Yokosuka, participated in the bilateral exercise.

U.S. NAVY (CHARLES DIX)


Cyberspace, a complex environment of interdependent networks of information technology, is now a domain in which military objectives are pursued.

ISTOCKPHOTO

operate at network speed, with operators monitoring but not executing individual actions. Though the stealth-like features and speed of the engagement in cyberspace are operationally challenging, the difficulty in attributing an attack to a specific entity may be a show-stopper with rules of engagement. Actions taken by a nation-state versus patriotic hackers acting on behalf of a nation are easily blurred. This was the likely scenario in the brief 2008 conflict between Russia and Georgia. It is not always evident against whom network defenders are protecting. The right of self-defense in cyberspace has not been thoroughly established. Most discussion of defensive cyberspace actions focuses on CND-response actions (CND-RA) and not denying operating space to an adversary.

Doctrinally, CND-RA is the ability to remotely "hack back" to an attacker or intruder who has penetrated a network or computer system. The reasonable analogy in the other domains is a counter-fire strike, which is an offensive tactic to deny an adversary further action. Developing the capability to conduct CND-RA is important, but it is secondary to protecting the network as an operational environment and denying that space to an adversary.

To actively defend, network operators must be able to see and understand how our own systems work and how information flows through them, as well as visualizing the impact of external forces attempting to penetrate friendly cyber environments. The real-time awareness of cyberspace and experienced operators with on-net skills will become the basis for dynamic network-defense operations and the principal element in protecting cyberspace as an operational environment.

Going on Offense

We must learn how to select targets in cyberspace. As in the other warfighting domains, the choice and tactical employment of weapons makes a difference. With physical targets, the range of the delivery platform or a weapon system is a limiting factor in the ability to strike. The factors considered by a cyber-attack planner are different from those faced by a kinetic weaponeer.

In cyberspace, access to a specific target at a particular time may depend on the on-net operator's ability to understand and react to changes to networks or operating systems in an environment that contains both hardware and software components. Early attempts to select cyber targets have concentrated on developing methods to use network attack as a way to neutralize targets that defy a kinetic solution.

While cyber-attack planners certainly must work to develop capabilities against hard targets, the offensive use of cyberspace will probably evolve in a much more measured way. Options to use denial-of-service weapons or controlling botnets (robot networks that operate autonomously) to limit an adversary's ability to use cyberspace are the likely first offensive tactics. In terms of effect on the campaign, these can be considered "level of effort" targets to degrade an adversary's C2 or disrupt the left side of the kill chain, or those intelligence and targeting activities that provide the firing solution.

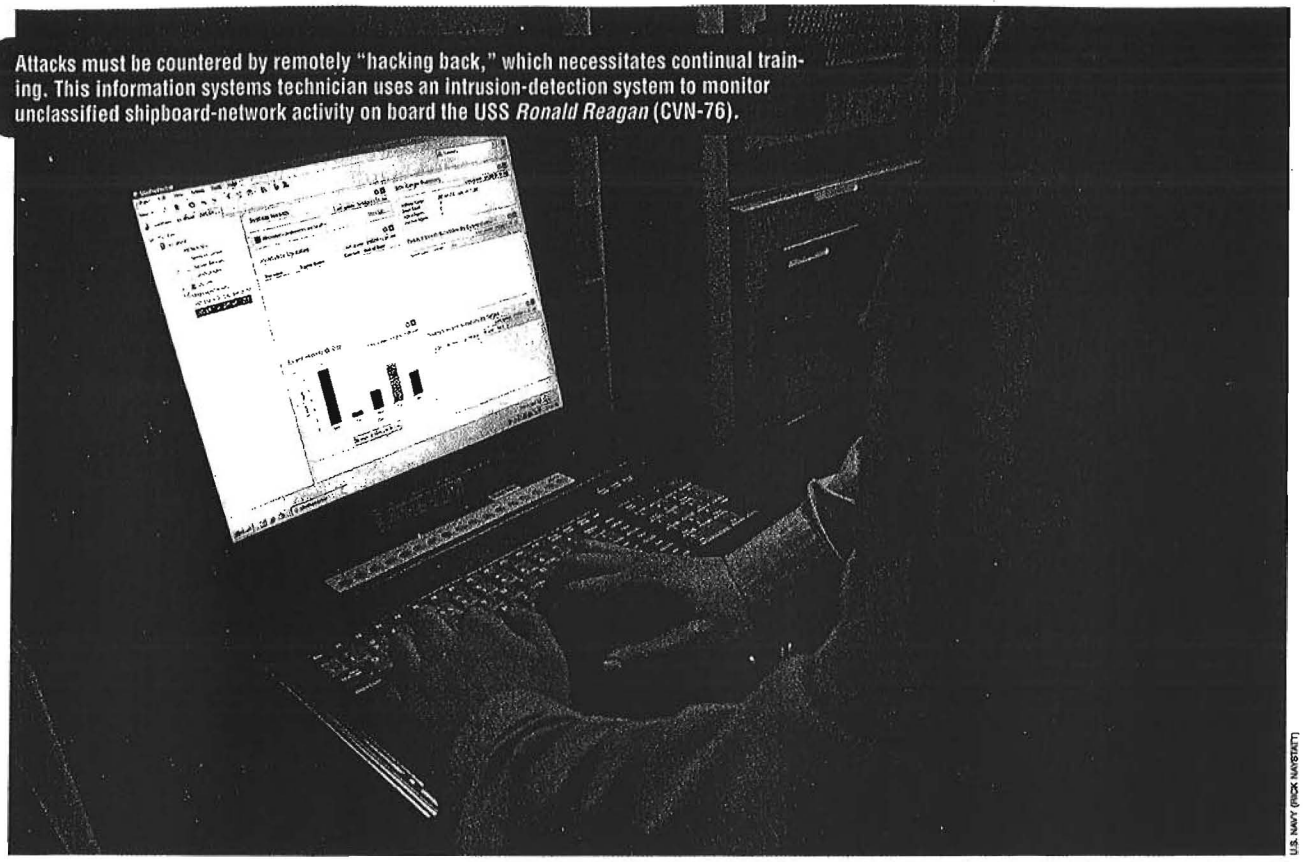
In the near future, efforts may be focused on integrating a campaign that supports actions in phase 2 of the conflict. However, because cyber weapons are nondestructive and may be unattributable, consideration must be given to their use during phases 0 and 1 of conflict to shape impending hostilities and provide alternatives to destructive weapons at later stages in the confrontation. Cyber-attack planners will also consider delivering "effects," or various types of malware, to opponents as a de-escalatory measure.

Both the longevity of the effect delivered and second- and third-order effects are also offensive cyberspace considerations. In the near term, sequencing of an attack in conjunction with kinetic strikes and the persistency of effects will be the focus of cyber planning.

A next step in the evolution of offensive cyberspace may be the delivery of effects to shape a campaign or to seize the initiative in attacking a specific target. This may degrade a specific capability that is key to the center of gravity, such as logistics. It may also focus on targets outside the geographic area of operations to either distract a defender from the main efforts or target a national-level capability such as public utilities or financial systems.

As cyber targeteering matures, additional factors such as the integration of cyber effects throughout a campaign, added emphasis on precision attacks on military targets, and controlling unintended consequences like damage to innocent cyberspace "bystanders" will be added to a planner's considerations.

Experience with kinetic strikes has led to "no-strike" lists or other sets of rules that help control engagements. Because of the interdependencies of networks and systems, cyberspace presents its own challenges. Attacking a control system for a power grid may provide the commander options to disable defensive systems, but



Attacks must be countered by remotely "hacking back," which necessitates continual training. This information systems technician uses an intrusion-detection system to monitor unclassified shipboard-network activity on board the USS *Ronald Reagan* (CVN-76).

U.S. NAVY (RICK NAVSTATT)

cascading effects from the loss of electrical power to a region must also be considered. This is not a unique problem, but it is one with which cyber planners have little practical experience.

Command and Control *and* Cyberspace

Philosophically, challenges include making the distinction between cyberspace as an operational domain and the systems that constitute the capabilities of cyberspace. Early doctrinal discussion led to coining the term C5I, which includes command, control, communications, computers, combat systems, and intelligence.

It was seen as a set of operational and tactical-level processes, decision aids, and awareness or visualization tools. But the C5I discussion falls far short of helping guide our way through cyberspace operations, particularly because C2 is a command function that draws from each warfighting domain. Cyberspace has its own operational characteristics and tactics, techniques, and procedures, as well as a specific relationship with the principles of C2 and the 17 elements of operational art.

Command being the inherent responsibility for the commander, the question becomes controlling cyberspace operations. In this regard, it is instructive to review Admiral Robert Willard's seminal article "Rediscover the Art of Command and Control" (U.S. Naval Institute *Proceedings*, October 2002). Admiral Willard's basic rule of effective C2 requires that the commander exercising control should have "better insight into what is required to win the day than is evidenced by the subordinate commander's actions."[5] Thus, the question of the commander's ability to "control" in cyberspace guides not only what happens in cyberspace, but also the actions that must be synchronized with operations in the other domains.

Following are the commander's objectives for exerting control, implying the task of synchronization between various warfare areas and operational functions.

- *Maintain alignment* with the operational mission.
- *Provide situational awareness* in the framework of the agreed-upon common operational picture.
- *Advance the plan* on the timeline and adjust to deviations accordingly.
- *Comply with procedure* to achieve standardization and effectiveness.
- *Counter the enemy* and be responsive to emerging intelligence, surveillance and reconnaissance.
- *Adjust apportionment* of assets and resources, including time.[6]

Each of these six objectives applies to cyberspace operations. Although the latter share some characterizations with other domains, their most common feature is time—specifically, speed of execution. This becomes clear through a comparison with antisubmarine warfare. As in cyberspace, submariners are challenged to operate in the same environment as does an adversary submarine. However, whereas antisubmarine warfare develops relatively slowly, cyber operations can change significantly in milli-

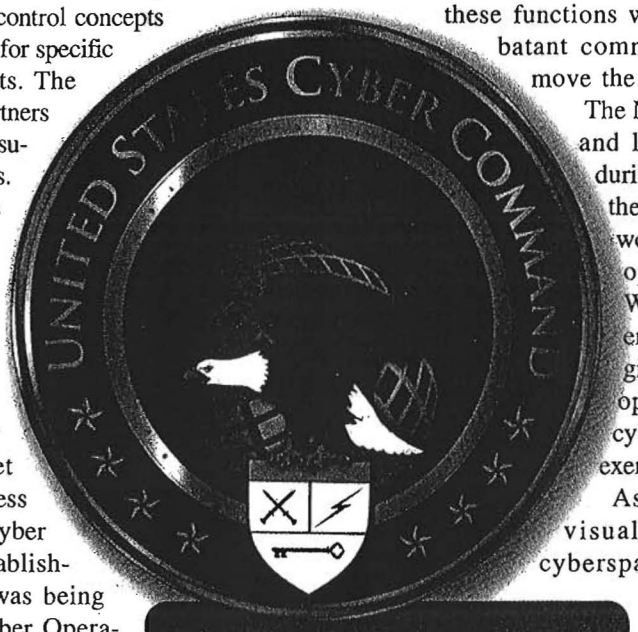
seconds. As cyberspace tactics, techniques, and procedures evolve, it will be critical to understand both the unique and the similar aspects of control functions.

A Model for Cyber C2

In May 2010, the Tenth Fleet staff, along with several partner commands and corporations, deployed in support of U.S. Pacific Command and Commander, Joint Task Force 519, to participate in Exercise Terminal Fury 2010 (TF10). Operating as the Joint Cyber Operations Task Force, the staff used a prototype organizational model to test cyberspace operational principles and exercise command and control of assigned forces.

Approximately 150 personnel supported the task force at various locations in Pacific Command. A facility was created to assess emerging cyberspace control concepts and provide a planning location for specific defensive and offensive effects. The main cell included industry partners who used specific cyberspace visualization and analysis techniques.

The Joint Cyber Operations Task Force is an emerging concept that will continue to develop. In the context of Navy and DOD organization, the exercise was conducted during a period of significant organizational change for cyber forces. U.S. Tenth Fleet had been in commission for less than five months, and U.S. Cyber Command had its formal establishment ceremony while TF10 was being conducted. Also, the Joint Cyber Operations Task Force was a late addition to TF10, and cyberspace exercises had not been extensively planned. The operational design allowed the task force commander to exercise authorities held by U.S. Cyber Command, as well as being operationally responsive to both the Pacific Command and CJTF-519 commanders.



The new U.S. Cyber Command logo was displayed during the command's activation ceremony at Fort Meade, Maryland, in May 2010.

The Pacific-based commanders used the model effectively, and it received positive feedback as an organizational structure for cyber C2. Additional exercises must be conducted to more thoroughly integrate the Joint Cyber Operations Task Force structure with established Intelligence (J2), Operations (J3), and Command, Control, Communications, and Computer Systems (J6) organizations of the combatant commands. Sound doctrine to support the operational level of war for cyberspace operations is needed, similar to the principles of maneuver. From the doctrine and tactics, commanders will better understand cyber operations, especially as they relate to those in the other domains.

As Admiral Willard stated, the "tenets of C2 are timeless, but with cyber operations warfare is faster and more complex, thus commanders must assimilate the six areas of control at high speed and in conjunction with other warfare area plans."[7] Although the speed of cyberspace activity is a distinctive feature of the domain, TF10 put it in the context of a major theater operation and demonstrated that adapting operational principles from other warfare areas can work in cyberspace.

The experience also showed the need to align cyber operations with service components and combatant commanders. Although the latter have the requirement to completely understand all aspects of an operation, execution is the responsibility of the service components. Because joint-force maritime and air-component commanders' execution depends on sound network operations and defense, the services must retain C2 of these functions without impeding the combatant commander's responsibility to move the plan forward.

The Navy's network, intelligence, and leadership were organized during the past year to maintain the service as the finest in the world. Just as air power developed rapidly at the onset of World War II, cyberspace operations will proceed apace, given the existing threats and opportunities. The seams in cyber C2 will be closed with exercises and experience.

As our understanding and visualization of it improves, cyberspace's relationship to and synchronization with the other domains will guide the way to new defensive and offensive capabilities, increasing the combat effect for both cyber and kinetic weapons. Time is of the essence. U.S. Tenth Fleet and its partners will rapidly engineer and field new operational capabilities to take full advantage of cyberspace.

1. William Gibson, *Neurmancer* (New York: Ace, 1984), p. 268.
2. *Joint Pub 1 Doctrine for the Armed Forces of the United States* (Washington, DC: Joint Staff), dated 2 May 2007 and incorporating change 1, 20 March 2009) GL-8.
3. *Joint Pub 1-02, DOD dictionary of Military and Related Terms* (Washington, DC: Joint Staff), dated 12 April 2001 and amended through 30 September 2010, p. 118.
4. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," *Cyberpower and National Security*, ed. Franklin D. Kramer, et al. (Dulles, VA: National Defense University Press and Potomac Books 2009), p. 29.
5. Robert F. Willard, "Rediscover the Art of Command and Control," U.S. Naval Institute *Proceedings*, October 2002, p. 53.
6. Ibid., 53–54.
7. Ibid., 54.

Rear Admiral Leigher is the deputy commander of U.S. Fleet Cyber Command, U.S. Tenth Fleet.