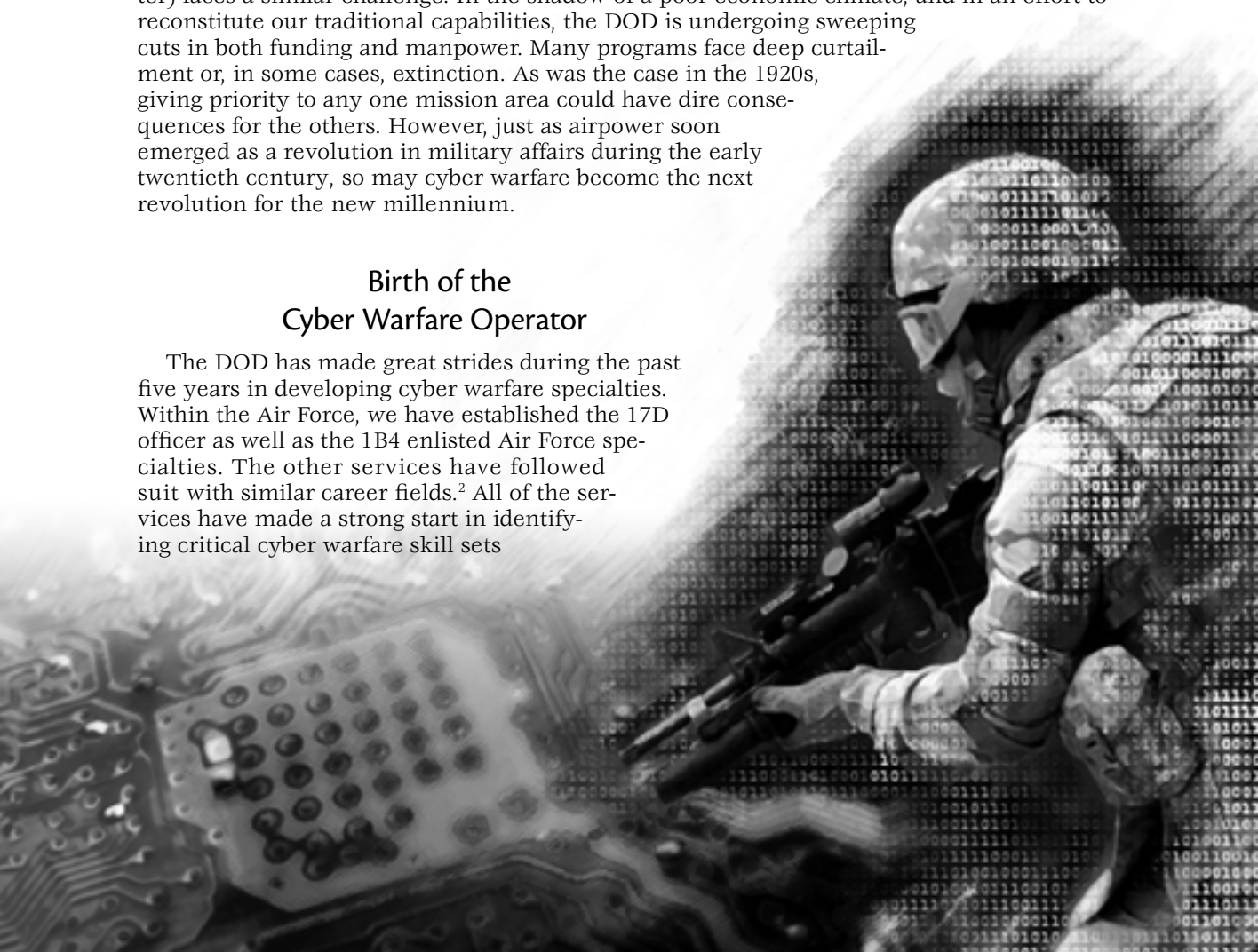
Disclaimer
The conclusions and opinions expressed in this document are those of the author cultivated in the freedom of expression, academic environment of Air University. They do not reflect the official position of the U.S. Government, Department of Defense, the United States Air Force or the Air University.

The Cyber Warfare Professional

Realizations for Developing the Next Generation

Lt Col Timothy Franz, USAF

In 1924 US Army leaders faced the difficult decision of determining how they should distribute their budget within an increasingly fiscally constrained environment. Giving priority to any single mission area could mean disaster for the others. One particular program that attracted much interest—the Lassiter Plan, designed to expand the Air Service at an estimated cost of $90 million per year—would consume more than one-third of the Army's budget.[1] Today the US Air Force (as well as the Department of Defense [DOD], for that matter) faces a similar challenge. In the shadow of a poor economic climate, and in an effort to reconstitute our traditional capabilities, the DOD is undergoing sweeping cuts in both funding and manpower. Many programs face deep curtailment or, in some cases, extinction. As was the case in the 1920s, giving priority to any one mission area could have dire consequences for the others. However, just as airpower soon emerged as a revolution in military affairs during the early twentieth century, so may cyber warfare become the next revolution for the new millennium.



Birth of the Cyber Warfare Operator

The DOD has made great strides during the past five years in developing cyber warfare specialties. Within the Air Force, we have established the 17D officer as well as the 1B4 enlisted Air Force specialties. The other services have followed suit with similar career fields.[2] All of the services have made a strong start in identifying critical cyber warfare skill sets

and mature, formal, professional career paths. However, these specialties serve only as the first generation of what must inevitably become a much more diverse field of professionals.

This article explores four key realizations that we must consider as the DOD develops its next generation of cyber warfare professionals. First, since cyber war fighting is a team event, it requires constructive efforts from a broad range of professionals. Second, the diversity of cyberspace drives the need for a system that more effectively identifies and categorizes the technologies and functions within cyberspace. Third, we must expand the culture of today's cyber warfare professionals to one that encompasses war fighting. Finally, because cyber warfare capabilities can vary in sophistication, we require an effective means of illustrating those levels of sophistication. Although the content of this article and some of its examples draw on the Air Force experience, the concepts remain service-agnostic and appropriate to any organization developing cyber warfare capabilities.

Realization One: Cyber War Fighting Is a Team Event

We frequently hear people unfamiliar with the Air Force ask Airmen, "What do you fly?" However, just as successful air operations involve much more than skilled pilots, so do successful cyber warfare operations encompass more than just cyber warfare "operators." Rather, it takes a team of cyber war-fighting professionals, each with his or her own responsibilities and skill sets, to establish, control, and project combat power in and through cyberspace. Accordingly, we can group these professionals within four distinct roles. Cyber warfare operators plan, direct, and execute offensive and defensive activities in and through cyberspace. Cyberspace technicians provide and sustain assigned portions of cyberspace.[3] Cyber warfare analysts and targeteers offer intelligence support to cyber warfare operations. Finally, cyber warfare developers design and build cyber warfare tools and weapons.

Responsibilities and skill sets for each role differ, depending upon whether the position supports offensive or defensive operations. Offensively, cyber warfare operators employ cyber warfare weapon systems and tools from ground, air, or space platforms. To remain effective, they must maintain combat-mission-ready status qualifications in these weapon systems and tools as well as expertise in the technologies and functions of adversary networks and systems. Cyberspace technicians who support offensive operations maintain the cyber warfare weapon system and supporting infrastructure. Duties range from installation and configuration to troubleshooting and repairing the hardware and software components of their assigned platform. Analysts and targeteers fuse all-source intelligence to analyze adversary networks and prepare offensive targeting solutions for cyber warfare weapons and tools. Like cyber warfare operators, they must also be experts in the functional application of assigned network and system target sets. Finally, cyber warfare developers maintain engineering and software-development skills in order to ably construct new (or modify existing) weapon systems, weapons, and tools. Accordingly, the nature of developers' work requires maintaining expertise in the technologies of potential targets that their weapons and tools are designed to affect.

For defensive operations, responsibilities and skill sets of cyber warfare professionals differ somewhat. Cyber warfare operators assigned to these missions defend and control specified portions of cyberspace, which can range from a simple local area network (LAN) within a single facility or airborne platform to an entire global network. Regardless of the scope of responsibility, operators must be experts in the function of that protectorate and, to some extent, the technologies that comprise it. They employ defensive weapon systems and tools, and individual responsibilities vary, depending

on the position assigned. Operators at the tactical level may control perimeter network sensors to defend against unauthorized attempts to access a network, while those at the operational level may direct large-scale, dynamic configuration changes in response to adversary attacks. Working hand in hand with cyber warfare operators in network defense, cyberspace technicians provide and sustain assigned portions of cyberspace. Like their operator brethren, their roles and responsibilities vary. Some technicians may be desktop computer experts, while others may have responsibility for infrastructure components such as routers and switches. Regardless, each technician must be skilled in the technologies and functions of his or her area of expertise and operate in accordance with mission priorities and defensive strategies established for the defended network. Intelligence analysts offer predictive threat analysis in support of defensive network operations. They fuse all-source analysis of technical, social, economic, and even political triggers in order to recommend proactive and, when necessary, reactive defensive measures to the cyber warfare operator. Such analysts must demonstrate expertise in adversary capabilities and tactics as well as maintain knowledge of the function and technologies of the networks they are charged to protect. Finally, developers for defensive operations have core skills similar to those of their offensive counterparts; however, they focus on developing cyber warfare weapon systems and tools that protect and defend networks.

Although every US military service has taken certain steps toward creating cyber warfare operators, they have made uneven efforts to professionalize the technician, analyst, and developer roles. Much as our predecessors deliberately sought to transform truck mechanics into aircraft maintainers and ground intelligence personnel into aerial targeteers, we must take further action to develop all cyber warfare professionals if we wish to produce a superior cyber warfare force.

Realization Two: The Diversity of Cyberspace

Cyberspace encompasses many technologies configured within networks that perform a broad array of functions. Although no universally accepted definition of cyberspace exists, most experts would agree that it is far reaching and includes a multitude of networked systems, ranging from the most common administrative networks (e.g., a home or office LAN), to space-based long-haul communications, to complex control systems for critical infrastructure assets. A closer look within any of these "functional" networks reveals different technologies (e.g., operating systems, communication protocols, software applications, etc.). Further, we find that technologies are not always exclusive to any one type of functional network. Rather, the same technologies may pervade different functional networks but with distinct applications for each. For example, the same network based on Microsoft Windows and Internet Protocol (IP) might be constructed in one manner to function as a banking service and in another to function as a manufacturing control system. In other words, the same technologies could have multiple functional applications.

To defend a network effectively, a cyber warfare team must understand both the technologies that comprise the network and the function it performs (i.e., the mission it supports). Although the makeup of an industrial control system versus an air and space operations center (AOC) network might demand similar technology expertise, the former has a completely different architecture, mission, and prioritization scheme than the latter (i.e., its function). In an offensive role, a cyber warfare team must understand the technologies of the target system as well as its function. On the one hand, comprehending the technologies allows one to select the correct weapon or tactic to gain access, escalate privileges, exfiltrate data, degrade enemy systems, and

so forth.[4] On the other hand, understanding the function permits one to know how, when, and where to put "effects on target."

Today's cyber warfare professionals (both offensive and defensive) maintain expertise in only a very limited number of functional networks and technologies. Unfortunately, the threat is ubiquitous, requiring us to expand beyond our current scope of capabilities. Concerning our defensive capabilities, threats have graduated beyond attacks against common administrative networks and websites to demonstrate effects against critical infrastructure resources such as air traffic control and utility-managing supervisory control and data acquisition (SCADA) systems.[5] Offensively, key centers of gravity against which we would conduct operations include similarly diverse types of networks and technologies. Common military targets represent an assortment of functions constructed with a mix of commercially available and proprietary technologies that lie beyond our current offensive expertise. For both, we can reasonably assume that the sophistication level of the threat will only develop further with time. As the world slowly comes to the realization that cyberspace is the soft underbelly of many a nation (including our own), the United States will need to extend its war-fighting know-how beyond our present potential.

As the DOD expands its cyber warfare capabilities, we cannot simply say generically that we need more cyber warfare operators, technicians, or analysts, just as we cannot say generically that we need more pilots, weapon system officers, or aircraft maintainers. The Army Air Corps (and, later, the Air Force) found that no single pilot could expertly fly every airframe.[6] Similarly, no single cyber warfare professional can operate equally well across all of cyberspace. Every military pilot grasps the fundamentals of operating in the air, but each one specializes in specific weapon systems and missions. We will demand similarly discrete proficiencies of our cyber warfare professionals. Although all of them need grounding in the fundamentals of their domain, each must specialize in specific platforms, missions, and areas of cyberspace. Otherwise, the breadth of knowledge required for any individual to understand how to offensively affect or defensively protect all functions and technologies within cyberspace would take more than a lifetime of training.

Better management of cyber warfare capabilities in the future calls for a logical system that identifies and categorizes functions and technologies within cyberspace. One approach involves grouping technologies and functional networks by common characteristics or utility. For technology "classes," an easy-to-understand example would entail combining all UNIX variants into one class and all Windows-based operating systems into another. Some or all tactical digital information link protocols might form one class (e.g., Link 16, Link 22), while a collection of control system protocols (e.g., MODBUS, RP-570, or Conitel) might determine another.[7] Turning to the grouping of functional networks, we see that two functional "classes" might include banking networks and AOC networks. It may also make sense to organize some classes by geographic similarities or by the standards of a prevalent company. For instance, perhaps all water-utility control systems in the southeastern United States are similar enough to place them in the same class, or perhaps all chemical production facilities built by a specific company might share enough network similarities to fit logically into a single class. The preceding examples are not intended to resolve the divisions but only to illustrate the concept; actual classes could very well differ in size and composition. In any event, the formal establishment of logical classes of technologies and functional networks would assist in clearly identifying specialties and skill sets. Further, the modular nature of such a framework would offer many advantages in organizing, training, and resourcing cyber warfare capabilities.[8] The following points continue the illustration.

Applying Concepts: Offensive Example

Functional and technology "classes," if intelligently organized, would translate into skill sets that personnel could learn in a reasonable amount of time and that could be maintained within a structured continuous-training program.[9] Having individuals remain current in a certain number of functional and technology classes would allow easy assembly of the right team for specific missions. In the notional example that follows, an offensive cyber warfare mission calls for operational preparation of the battlespace against country Green's banking system. The known technologies for this system include IP-based and Windows 2000 technologies. Given this information, commanders select the following crew for the mission:

- Captain America (operator): An expert qualified in Technology Class B (IP-based, Windows-/UNIX-based technologies), he has a basic qualification in Functional Class R (banking systems) and is weapon-qualified in the "Babbage" weapon suite [fictional], which includes capabilities specifically designed to affect IP-based, Windows-/UNIX-based technologies.
- Senior Airman Good and Airman First Class Wrench (technicians): These personnel maintain the weapon system platform that Captain America operates and assist in the setup, loading, and configuration of the Babbage weapon suite.
- Lieutenant Wonder (cyber warfare analyst/targeteer): An expert qualified in Functional Class R (banking systems), she has a specialized focus on banks in Green's theater region and a basic qualification in Technology Class B (IP-based, Windows-/UNIX-based technologies).
- Mr. Hornet (weapon developer): A member of the team that designed the Babbage weapon suite, he is an expert in Technology Class B (IP-based, Windows-/UNIX-based technologies).

Extending our example, one can see how a modular class structure would have the added advantage of flexible crew pairings. Suppose a subsequent mission calls for disruption of country Orange's chemical production plant. Intelligence indicates that this system uses technologies similar to those of the banking system in country Green. In this case, the chemical production plant includes UNIX-based servers using IP-based protocols. The similarities in target technologies to those seen in the earlier mission allow the operator, technicians, and weapon developer to remain the same, while swapping out the cyber warfare analyst/targeteer in favor of more relevant functional network expertise:

- Captain America (operator): An expert qualified in Technology Class B (IP-based, Windows-/UNIX-based technologies), he has a basic qualification in Functional Class S (chemical production plants) and is weapon-qualified in the Babbage weapon suite.
- Senior Airman Good and Airman First Class Wrench (technicians): These personnel maintain the weapon system platform that Captain America operates and assist in the setup, loading, and configuration of the Babbage weapon suite.
- Staff Sergeant Braveheart (cyber warfare analyst/targeteer): An expert qualified in Functional Class S-4 (chemical production facilities built by Sunnybell Inc.), he has basic qualifications in Technology Class B (IP-based, Windows-/UNIX-based technologies).[10]
- Mr. Hornet (weapon developer): A member of the team that designed the Babbage weapon suite, he is an expert in Technology Class B (IP-based, Windows-/UNIX-based technologies).

As illustrated, the class concept allows us to more easily identify and select an appropriate crew complement to go against a specific target network. However, as cyber warfare matures, we can expect missions to target not only a single functional network but a combination of different interconnected functional networks. A broader example exposes how separate crews, identified by different functional classes, can integrate to produce more robust effects across a multifunctional network. For example, suppose a mission calls for disrupting power to one of country Orange's electrical power grids. Intelligence has shown that a certain SCADA system connected to a business LAN front end manages the target grid. Further, intelligence indicates that somewhere in country Orange a radio frequency link may serve as an access point into that business LAN.

The expertise required to exploit and gain access to the link, navigate around the defenses of the business LAN, and finally produce effects within the control system would be too much to expect of a single operator or crew. However, our class concept helps organize crews appropriately in order to complete the assigned mission. First, a crew qualified to exploit radio frequency communications (perhaps from a manned or remotely piloted aircraft) flies within range of country Orange to gain initial access. Second, another crew (qualified in the technologies and functions of the front-end business LAN) leverages the radio frequency access to enter the business LAN, overcome its defenses, and tunnel into the control system. This allows a third crew to remotely access the control system and disrupt power. Completing the operational picture, one can envision overhead assets (e.g., remotely piloted vehicle or satellite imagery) providing battle damage assessment in support of the ingress and egress of an air strike package or a special operations ground team. Although this example may seem too complicated to work, consider the complexity that goes into a single airborne strike mission. Similar to composite air operations, cyber warfare missions of this magnitude must eventually become commonplace.[11]

Applying Concepts: Defensive Example

When we discuss network defense in today's Air Force, we really mean only capabilities and forces that defend the Nonsecure and Secret Internet Protocol Router Networks (NIPRNET and SIPRNET, respectively).[12] However, if we peer within the fence line of most bases, we find many other networks critical to the successful execution of the Air Force mission. Examples include those that manage an installation's supporting infrastructure, such as utility control systems (e.g., water, electric power, and gas) as well as heating, ventilation, and air conditioning systems. Organizations such as security forces and the fire department rely upon networks that manage physical security sensors; fire alarm/fire suppression; and chemical, biological, radiological, nuclear, and explosive monitoring devices. Additional networks support airfield operations, radar systems, and airborne command and control (C2) links.[13] As we expand network defenses beyond the NIPRNET and SIPRNET, our concept of functional and technology classes proves useful by more easily identifying the systems we are charged to defend, as well as arranging the skill sets in which we must organize and train our cyber warfare professionals.

Like their offensive brethren, units assigned to the operation and defense of a network must maintain expertise in certain technology and functional classes. However, instead of focusing on the technologies and functions of target networks, these units must understand the functions and technologies of the networks they are responsible for defending. Applying our class concept to an example, we see that one unit may be designated to operate and defend Functional Class G networks (Patriot Battery Systems), and another designated to do the same for Functional Class J networks

(electrical power SCADA systems). Accordingly, these units would include personnel who maintain qualifications in the designated functional class as well as in the relevant technology classes.[14]

Further Advantages to Categorizing Cyberspace

Beyond the benefits to the training and organization of cyber warfare forces, categorizing cyberspace within functional and technology classes offers other advantages through easier identification of war-fighting requirements. That is, suppose a combatant commander (CCDR) needs to degrade country Orange's integrated air defense system (IADS) X or defend US air control system Z. Requirements such as "degrade country Orange IADS X" or "defend US air control system Z" may be clear enough to determine needed conventional forces; however, such verbiage is difficult to translate into language useful for obtaining and apportioning cyber warfare capabilities. Breaking down requirements into functional and technology classes helps to more clearly articulate cyber warfare disconnects within the program objective memorandum (POM) process. In addition, it can assist the CCDR's planners in requesting appropriate cyber warfare forces from the services.

To illustrate the concept within the POM process, we could imagine translating the technologies comprising country Orange's "IADS X" into certain technology and functional classes. Inputs into the process would now effectively say, "We're requesting new (or more) manpower, weapon systems, training and education courses, as well as test and training ranges to affect these specific technologies and functional networks that comprise country Orange's IADS X." These disconnects, if fulfilled, will support the CCDR's requirement to affect IADS X. By articulating "POMable" cyber warfare requirements, we improve their chances of withstanding the scrutiny of funding panels. Furthermore, by tying them back to the needs of the CCDR, we also identify areas of risk if certain programs are not funded (e.g., if we do not fund the development of cyber warfare capabilities to affect IADS X, CCDRs must either assume risk in that area or fulfill the requirement through other capabilities). Obviously, this is a very simplistic example. Real-world instances would likely prove more complex since any single technology class might pervade many functional classes and, in turn, feed a multitude of the CCDR's requirements.

Having the ability to identify cyber warfare requirements more easily will also prove useful to the CCDR's planners when they assign capabilities within a "forces for" document, when they request service capabilities for contingency operations within an evaluation request message, or when they develop time-phased force and deployment data.[15] Today, such documents generically identify cyber warfare professionals. However, at some point, tasking a "cyber operator" will not be enough. For example, pulling someone knowledgeable about telephone systems will not help a CCDR who is looking for an expert in SCADA.

A logical system for categorizing groups of technologies and functions within cyberspace does not formally exist today.[16] However, we will need one if we wish to organize, train, and resource cyber warfare capabilities effectively in the future.

Realization Three: The Need for a War-Fighting Culture

The Air Force may have anointed our cyber warfare professionals with a new title and badge, but their culture must change if we are to morph them into the war fighters we envision for the future. Unfortunately, several obstacles slow our ability to establish a true war-fighting culture within this community. First, most of today's cyber warfare professionals come from the communications and information career fields. As such, they have historically focused on

keeping communications up and running—not on completely understanding the missions supported by each communications link or node. Consequently, true understanding of mission impact caused by losing a link or node commonly occurs only after that loss takes place and customers begin to complain. A second cultural challenge comes in the way we currently define cyber war fighting. For example, at present we limit cyber "defense" primarily to detecting intrusions at the boundaries, discovering malware internally, and "blocking" what we find at the gateways, service delivery points, or firewalls.[17] Our cyber defenders need more familiarity with the full range of hostile threats to our information systems and more skill in fighting through attacks from such threats. The culture of today's cyber warfare professionals must evolve from one that provides service to one that offers a balance of service, security, and knowledge of threats, all in the name of mission assurance.

Developing a "war-fighting culture" for cyber warfare professionals means creating a different mind-set. On the offensive side, that mind-set comes more naturally because of the nature of the mission. However, on the defensive side, such a perspective takes extra effort. Networks support specific missions. One cannot adequately defend a network without knowing the mission that network supports as well as the threat that holds it at risk. Unfortunately, the "comm" culture historically has placed more emphasis on the health and availability of the network than on the mission for which it exists. We do need our cyber defenders to have expertise in the technologies of their networks; we also need them to have expertise in the supported missions, in ways of prioritizing those missions, and in knowing how degradation or loss of certain portions of the network affects those missions (before it happens). Further, our cyber defenders must know their enemy. Understanding the scope of the threat as well as its capabilities and limitations; common tactics, techniques, and procedures (TTP); historic and current trends; and primary motivations is critical to preparing for, prioritizing against, and maneuvering in response to that threat. Only by comprehensively understanding both the mission and the adversary can we even begin to effectively defend—and, ultimately, assure—missions in and through cyberspace.

Defensive cyber war-fighting actions consist of preparing for an attack, responding to it, and then recovering from it. Preparation entails establishing and securing the network. Fundamentals such as a defense-in-depth architecture, information assurance mechanisms, and strong C2 provide the foundation. Distributed sensors, both external and internal to the network, that detect, eradicate, and block threats round out the preparation. Responding to an attack translates to fighting through it. This means implementing such concepts as dynamic configuration controls (e.g., wartime IP addresses, frequency hopping, physically/virtually hot-swapping equipment), active deception techniques (e.g., honeynets), and the use of deliberately misleading server names.[18] In addition, our cyber warfare professionals must be able to quickly reroute blue (friendly) communications to secondary and tertiary paths when certain links and nodes are lost, as well as reroute red (enemy) attacks down innocuous paths. By understanding how the network supports the operational mission, defenders would know when and where we can afford to endure network disruption. At times, suffering a loss or degradation somewhere on the network would be acceptable if it doesn't affect a critical mission. If an adversary believes that his network attack is succeeding, he may continue to spend resources and time on an expendable target, permitting us to address other priorities. An effective defensive response also entails knowing how to fight integrally within the entire network C2 enterprise as well how to fight in isolation. It's one thing to defend a network with fully operational capabilities and C2 intact. It is quite another to do so after losing connectivity with

the Integrated Network Operations Security Center, 624th Operations Center, or AOC. Can we still assure the mission? Response also includes striking back at the threat. Our defenders do not necessarily execute such actions directly (since offensive capabilities involve a completely different skill set); rather, those actions require coordinating through a C2 chain to allow an operations center or AOC to direct appropriate kinetic or nonkinetic responses. Finally, war fighting includes recovery activities such as reconstituting rapidly and in a prioritized fashion. Adequately trained cyber warfare specialists can do this effectively because they understand the mission, network, and priorities.

Realization Four: Not All Cyber Warfare Capabilities Are Equal

No cyber defense will repel every attack, and no cyber offensive capability will succeed against every adversary. A mechanism to identify the sophistication level of our cyber warfare capabilities is important if we wish to set clear standards for training and manage expectations of leadership. During events such as Red Flags or Air Force Weapon School exercises, air aggressors employ such a mechanism in the form of a "threat replication" matrix to identify the level of sophistication to which they will train blue forces in any particular engagement. For example, will they operate at a level-one threat intensity, representative of older enemy aircraft models and more basic TTPs, or will they fly at a level-four intensity, representative of the most advanced capabilities and TTPs employed by more sophisticated adversaries? Information aggressors are in the process of implementing a similar threat matrix to replicate an adversary's cyber warfare capabilities during training exercises. We will leverage this example to offer a concept for identifying the level of sophistication at which any cyber warfare capability is operating.

Table 1 represents a conceptual matrix for identifying the sophistication level of a defended friendly network. The first dimension of the level, labeled "technology," reflects the sophistication of the technologies used to operate and defend the network (for simplicity, the example matrix depicts only operating system technologies). A network operating at technology-level one might employ early operating systems such as an older Windows variant or a Sun system. At level two, it may use something more current or cutting edge such as Windows 7 or Snow Leopard. Level three represents an organically developed operating system or a trusted computing environment that may not be available commercially to the public (e.g., Next-Generation Secure Computing Base or Kylin).[19]

The second dimension of the example, labeled "TTP," represents the sophistication of the defensive TTPs employed. For example, level one might identify a network employing the most basic defensive configuration

Table 1. Sophistication levels for a defended network

Defended Network		LEVEL OF SOPHISTICATION		
		One	Two	Three
Administrative Networks	Technology	- Sun Operating System / Windows XP / Vista	- Windows 7 / Snow Leopard	- Next-Generation Secure Computing Base / Kylin
	TTP	- Simple LAN / Unpatched	- Defense in Depth / External/Internal Sensors	- Honeynets / Denial and Deception

typical of a simply configured, unpatched LAN. Level two might be organized with a more defense-in-depth approach along with external or internal monitoring mechanisms. Level three could reflect the most sophisticated network defenses we've seen, employing advanced techniques such as honeynets and deliberate denial-and-deception tactics. Bringing the two dimensions together, a network may operate with lower-end equipment (level-one technology) but have experienced operators who employ level-two TTPs. Or a network may have leading-edge equipment (level-three technology) but employ forces with relatively weak defensive training (level-one or -two TTPs).

Similarly, sophistication levels for offensive capabilities (table 2) identify technology levels by the complexity of the weapon system or tool employed. For example, level-one technology might consist of tools or weapons openly available on the Internet (e.g., "script-kiddy" tools), whereas level two could represent something more sophisticated, such as commercially available tools or weapons. Level three would reflect proprietary, organically developed offensive capabilities. TTP levels for offensive cyber warfare capabilities range from the least sophisticated, noisy, attributable ones (level one) to TTPs that employ advanced techniques (e.g., active deception, highly cloaked anonymous operations, etc.) capable of producing second- and third-order effects (level three).[20]

Identifying the sophistication levels of our cyber warfare forces has twofold importance. First, such levels translate to a better understanding of training standards. In other words, knowing these levels assists our cyber warfare professionals in identifying the level of sophistication at which they currently operate. Similarly, it helps them determine the level they need to attain in order to meet standards or to match or defeat known adversaries. Articulating standards not only defines training requirements but also builds operational rigor into war-fighting forces. Second, defining sophistication levels manages expectations of leadership. Manning, funding, and time are three investment variables which drive the sophistication level of any technology and TTP that we acquire or develop. Tools, like the matrix displayed, that illustrate the sophistication level of cyber warfare capabilities will help leaders more clearly understand what an investment will buy. Unless they maximize the investments, the resulting technologies and TTPs may be less than world class (i.e., level three) and therefore less capable than those of our adversaries. Understanding this point permits leaders to better understand and accept the risk, or reprioritize resources to attain the sophistication level desired.

Conclusion

In the last 100 years, airpower revolutionized military operations so completely

Table 2. Sophistication levels for an offensive cyber warfare capability

Adversary Target		LEVEL OF SOPHISTICATION		
		One	Two	Three
Administrative Networks	Technology	- In Wild Scripts / Tools	- More Complex / Commercial Off the Shelf	- Organic / Government Off the Shelf
	TTP	- Lone Points of Presence / Noisy / Attributable	- Multiple Points of Presence / Nonattributable	- N-Order Effects / Deception

that leaders around the world recognized air supremacy as essential to victory in war. In the next 100 years, the same may be said about cyber superiority. As the DOD further develops our cyber warfare capabilities, we need to address several realizations in order to bring us closer to success. These include establishing a strategy to cultivate all cyber warfare professionals (versus just the operator); creating a system that identifies and categorizes functions and technologies within cyberspace; developing a warfighting culture among our cyber warfare professionals; and utilizing an instrument that illustrates the sophistication level of cyber warfare capabilities. To address some of these realizations adequately, we will inevitably need to make significant investments. In today's climate of dwindling resources, how much will the DOD put into the future of cyber warfare? Our leaders face challenges analogous to those that confronted their predecessors in 1924. They made the correct choice. Will we? ✪

Notes

1. James P. Tate, *The Army and Its Air Corps: Army Policy toward Aviation, 1919–1941* (Maxwell AFB, AL: Air University Press, 1998), 28–34.

2. Henry S. Kenyon, "U.S. Army Ponders Cyber Operations," *Signal Online*, 15 October 2009, accessed 6 December 2010, http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=2082&zoneid; and "General Officer Programs," Navy Recruiting Command, accessed 6 December 2010, http://www.cnrc.navy.mil/noru/orojt3/generalofficer.htm.

3. Other terms are commonly used today to represent this role (e.g., "technician," "maintainer," "specialist," "communicator," etc.). The author chose the term "technician" because it appeared both adequate and less controversial than some of the others.

4. "Escalate privileges" is common cyber warfare vernacular for an attacker's efforts to upgrade his or her privileges within a network from normal user rights to those of an administrator in order to move freely within that network.

5. See Rose Tsang, *Cyberthreats, Vulnerabilities and Attacks on SCADA Networks*, working paper (Berkeley, CA: University of California, Goldman School of Public Policy, 2009), 5–6, accessed 20 December 2010, http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf; *Global Energy Cyberattacks: "Night Dragon,"* McAfee White Paper (Santa Clara, CA: McAfee, 10 February 2011), 3, http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf; and *Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems*, Federal Aviation Administration, report no. FI-2009-049 (Washington, DC: US Department of Transportation, 4 May 2009), 4–5, http://www.oig.dot.gov/sites/dot/files/pdfdocs/ATC_Web_Report.pdf. SCADA systems are "used extensively by power, water, gas, and other utility companies to monitor and manage distribution facilities." See Harry Newton, *Newton's Telecom Dictionary*, 20th ed. (San Francisco: CMP Books, 2004), 725.

6. In 1925 Gen William "Billy" Mitchell identified three primary missions for an air force (pursuit, bombardment, and attack). See William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Miliary* (New York: G.P. Putnam's Sons, 1925), 164–71. Today there are over a dozen missions, including counterair; strategic attack; airlift; air refueling; and intelligence, surveillance, and reconnaissance, just to name a few. See Air Force Doctrine Document (AFDD) 3-1, *Air Warfare*, 22 January 2000, 8–24, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-1.pdf. In 1921 fewer than 900 pilots were on active duty, with about two dozen different aircraft types in service. See Tate, *Army and Its Air Corps*, 19; and "Air Corps Development, 1919–1935," National Museum of the US Air Force, accessed 13 February 2011, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=724. The US Air force now flies over 50 distinct aircraft types with more than 13,000 pilots, and each aircraft type has its own specialty code. See *Air Force Officer Classification Directory* (Randolph AFB, TX: Air Force Personnel Center, April 2010).

7. Protocols define the rules by which devices talk with each other; they comprise procedures or conventions relating to format and timing of data transmission between two devices and cover such

matters as framing, error handling, transparency, and line control. See Newton, *Newton's Telecom Dictionary*, 664.

8. Although this article addresses how the concept of functional and technological classes applies to military forces, it has application across the civilian and commercial sectors as well. A logical partitioning of cyberspace across functional and technological lines could help nonmilitary organizations organize their own networks more effectively.

9. There are more training variables to address with this statement, including how many functional and technological classes is reasonable for any individual to maintain, but the basic concept remains the important point.

10. For the purposes of this example, the hypothetical Sunnybell Corporation constructs chemical production facilities across the world. Its widespread presence makes it a good candidate for its own functional class.

11. The concept presented in this paragraph leads to the idea of identifying offensive cyber warfare units based on their ability to affect specific technology and/or functional classes. However, when one considers the multitude of differing technologies and functional networks in cyberspace, one realizes that it may not be practical to physically locate all expertise at one location (e.g., we'll likely never have enough personnel to give each offensive unit its own set of analytical expertise in railroads, electrical power, etc.). We must give additional thought to using a virtual network of functional expertise if we wish to implement these concepts successfully. For example, perhaps a pool of chemical production facility experts is physically distributed across the country, and these individuals can be linked together virtually. This would facilitate assignment of this expertise to different units at different times, depending upon the present mission. That is, Unit X is assigned to affect a chemical production facility on one day while Unit Y is assigned to affect a chemical production facility (perhaps the same one, perhaps a different one) on another day. However, perhaps both units share the same team of targeteers qualified in Functional Class S (chemical production facilities).

12. Network defense is the employment of network-based capabilities to defend friendly information resident in or transiting through networks against an adversary's efforts to destroy, disrupt, corrupt, or usurp it. See AFDD 3-13, *Information Operations*, 11 January 2005, 20, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-13.pdf.

13. Although some of these systems may occasionally ride the backbone of a NIPRNET or SIPRNET connection, network defenders are often unaware of their presence. In reality many of these systems are operated as independent networks and thus fall outside the operational area of today's network defenders.

14. This example uses a singular unit to illustrate the concept of applying functional and technological designations to cyber warfare units in an effort to spur further discussion. Actually the span and complexity of many networks may (and do) require the use of multiple units to cover all aspects of operation and defense. The topic of organizational structure for a complex network enterprise is hotly debated today within the cyberspace community and would require discussion outside the scope of this article. However, the general concept of applying functional and technological class designations to units and personnel charged with the operation and defense of networks is the salient point.

15. The secretary of defense's "Forces for Unified Command Memorandum" assigns forces and resources to combatant commands. See Joint Publication (JP) 5-0, *Joint Operation Planning*, 26 December 2006, I-26, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf. CCDR planners use evaluation request messages to solicit course-of-action inputs from subordinate units. See ibid., I-15.

16. Although not formalized, a foundation does exist on which to build a logical categorization. The concept was first introduced in Maj Timothy P. Franz, "IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way-Ahead for Network Warfare Forces" (master's thesis, Air Force Institute of Technology, March 2007) as "network classes." It matured into a concept of "functional classes" and "technology classes" during the early stages of 17D/1B4 development by the Professional Cyberspace Education Working Group led by Headquarters US Air Force and then later within the Air Force's Cyberspace Technical Center of Excellence at the Air Force Institute of Technology. The effort has since ended due to manpower constraints, but the groundwork still exists.

17. The author acknowledges that more is involved than these actions, but they provide a good synopsis.

18. Physical hot-swapping is the process of replacing a failed component while the rest of the system continues to function normally. See Newton, *Newton's Telecom Dictionary*, 400. Whereas hot-swapping refers to swapping out a physical component, *virtually hot-swapping* refers here to the concept of swapping out a virtual machine or dynamically changing logical addressing in response to or in preparation for an attack. The au-

thor acknowledges that current technological advances do not fully support the concept of virtual hot-swapping today.

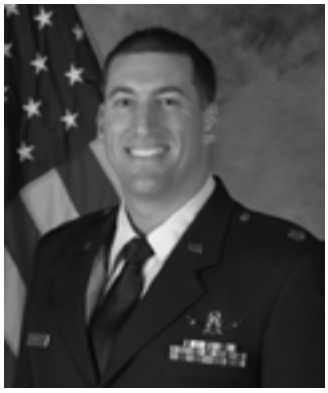
A honeynet is a network set up with intentional vulnerabilities to invite attack so that defenders can study an attacker's activities and methods and use that information to increase network security. See "Honeynet," *NetworkDictionary*, accessed 20 December 2010, http://www.networkdictionary.com/security/h.php. In the context of this paragraph, the term also indicates the use of honeynets to delay or deceive a potential attacker.

19. "Trusted computing" is defined as a locked-down computer architecture that can give guarantees about the application software it is running and that allows applications to communicate securely with other applications and with servers. See Mark Dermot Ryan, "Trusted Computing and NGSCB," University of Birmingham School of Computer Science, 2004, accessed 30 December 2010, http://www.cs.bham.ac.uk/~mdr/teaching/TrustedComputing.html.

The Next-Generation Secure Computing Base (NGSCB) is new security technology for the Microsoft Windows platform that employs a unique hardware and software design to enable new kinds of secure computing capabilities to provide enhanced data protection, privacy, and system integrity. See "Microsoft Next-Generation Secure Computing Base—Technical FAQ," Microsoft TechNet, accessed 30 December 2010, http://technet.microsoft.com/en-us/library/cc723472.aspx#EEAA.

Kylin is an operating system developed by academics at the National University of Defense Technology in the People's Republic of China and approved for use by the People's Liberation Army. Although the underlying infrastructure of this system is actually a UNIX variant of FreeBSD, for the purposes of this article, it offers an example of a close-to-proprietary operating system. See Rohit, "What Is Kylin Operating System?," *Spectrum*, accessed 13 February 2011, http://krititech.in/wordpress/?p=138; and Gerard, "Kylin, a Chinese FreeBSD Based, Secure O/S," *FreeBSD News*, 4 January 2011, accessed 13 February 2011, http://www.freebsdnews.net/2011/01/04/kylin-chinese-freebsd-based-secure-os/.

20. "Noisy" refers to a network attack vector that is highly detectable due to the unsophisticated tools and tactics employed by the attacker.



Lt Col Timothy Franz, USAF

Lieutenant Colonel Franz (BS, University of Central Florida; MS, Air Force Institute of Technology) is the former commander of the 57th Information Aggressor Squadron, responsible for training Air Force, joint, and allied personnel by replicating current and emerging information operations threats. Prior to that assignment, he served as chief of force development at Air Force Cyber Command (Provisional), where he developed strategies for and led the development of cyber warfare Air Force specialties, including related recruiting and accession, training and education, and professional development programs. During his career, he has served as a missile combat crew commander, evaluator, instructor, and flight commander, as well as an information operations space analyst, tactician, planner, and special technical operations chief. Lieutenant Colonel Franz is a distinguished graduate of Squadron Officer School and of the Air Force Institute of Technology, where he completed his intermediate developmental education in residence.