Refocusing Cyber Warfare Thought

Maj Sean C. Butler, USAF

In September 2007, more than 65 subject matter experts from around the Air Force gathered at the US Air Force Academy to discuss the way ahead for institutionalizing cyber training and force development.[1] This occasion followed the establishment of a provisional Air Force Cyber Command (AFCYBER) (a major command) in November 2006, which itself followed the Air Force's incorporation of cyberspace into its mission statement less than a year prior. Cyber power advocates of the decade leading up to this point were finally building momentum for establishing cyberspace as a fully recognized war-fighting domain. Unfortunately, these victories came at a cost—a fact that started to become evident at the 2007 conference.[2]

Conference organizers showed participants the definition of cyberspace adopted by the Department of Defense (DOD) in its *National Military Strategy for Cyberspace Operations*, published in 2006: "A domain

characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[3] They also described the outline of the Air Force's plan for structuring the cyber career field, with two primary cyber "shredouts" for computer network operators and combat systems (electronic warfare [EW]) officers.[4] Almost immediately, this revelation led to some uncomfortable questions and awkward implications. Why had the service placed two vastly different career fields into a single training pipeline? Does radar jamming belong to the same class of warfare as computer network "hacking"? Does this mean we should consider the airborne laser part of cyber warfare since it utilizes the electromagnetic spectrum (EMS)? The participants, experienced Airmen who hailed from both sides of the divide, asked these and other questions, leaving them largely unanswered.

Fortunately, both the DOD and Air Force have since corrected or deemphasized most of the aforementioned problems underlying this framework, albeit not without substantial upheaval. Less than two years after publication of the definition of cyberspace in the *National Military Strategy for Cyberspace Operations*, the DOD updated it to a more focused and practical foundation for doctrine: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[5] Shortly thereafter, the Air Force downgraded the provisional AFCYBER major command to a numbered air force subordinated to the new US Cyber Command subunified command, and never fully incorporated combat systems officers into its cyber career field.[6] For the most part, the service dropped the explicit focus on the EMS and physical characteristics.

The efforts of early cyber power advocates to draw attention and resources to cyberspace as a military operational domain have borne fruit in recent years.[7] However, the body of theory and doctrine that developed was arguably influenced (possibly unconsciously) by the

very process of struggling to overcome conservative resistance. Recurrent themes attempt to portray cyberspace as more comfortably analogous to the traditional domains of land, sea, air, and space. In addition to highlighting its physical characteristics, current doctrine transfers basic principles and tenets from other operational domains to cyberspace, apparently assuming, without careful consideration, their applicability to the new context. (The article examines some examples of this practice later on.)

Cyberspace unquestionably has a physical element that carries with it certain war-fighting implications, and many fundamental principles of war will undoubtedly apply to cyber war. However, the approach is flawed, in that the doctrine appears to look for ways to prove that "cyberspace is like other domains" instead of fully accounting for its unique properties. Rather than continually focus on the relatively mundane physical elements of cyberspace, military thinkers should embrace its unique logical or virtual nature and consider its implications. Understanding the uniqueness of cyberspace provides foundational clarity of thought towards extending domain-specific theory and formulating doctrine.

Cyberspace as a Physical Domain

Early attempts to describe cyberspace as an operational domain tended to emphasize its grounding in the physical world as a defining characteristic. Again, this is understandable since theorists were attempting to establish cyberspace as a domain on par with land, sea, air, and space—all domains within the physical world. Proponents sought to carve out their own slice of the same physical universe in order to place cyberspace fully alongside the other traditional domains.

In his seminal work *Strategic Warfare in Cyberspace,* one of the most influential early studies of cyber warfare, Col Gregory Rattray, USAF, retired, cautioned against treating cyberspace as a purely virtual environment: "Cyberspace . . . is actually a *physical domain* resulting from

the creation of information systems and networks" (emphasis in original).[8] Clearly, cyberspace has a physical manifestation in the form of the electronic devices used to communicate, and Colonel Rattray was not misguided in reminding information warriors not to discount physical interactions with cyberspace. However, this argument alone did not convince individuals who sought to elevate cyberspace to a full-fledged war-fighting domain. After all, no other domain was defined by the equipment used to operate within it. This ultimately led to co-opting the EMS as the physical representation of cyberspace.

Dr. Daniel Kuehl of the National Defense University—a longtime advocate of linking cyberspace closely to the EMS (he referred to such a relationship as early as 1997)—went on to have "a major role in the crafting" of the DOD's definition of cyberspace in 2006.[9] Frequently cited, he continues to advocate this physical-centric definition of cyberspace in papers and guest lectures. Possibly reflecting this early influence and desire to legitimize cyberspace, the Air Force Cyberspace Task Force of 2006 proposed a "Cyber Creed," which stated, among other things, that "cyber is a *war-fighting domain*. The electromagnetic spectrum is the maneuver space" (emphasis in original).[10]

Assigning the EMS to cyberspace is appealing for a number of reasons. First and foremost, this spectrum represents a pervasive, well-defined phenomenon in the physical world, seemingly qualified to sit at the same table with the other physical domains. Most digital communications, which intuitively seem to belong to cyberspace (if anything does), are carried on radio waves, microwaves, or lasers (either wirelessly or by fiber-optic cable), all of which belong to the EMS. Using this as a starting point, one finds that allowing the definition of cyberspace to stretch to include things like radar (an information system of sorts) and, with that, electronic countermeasures, does not appear wholly unreasonable. Suddenly, cyberspace attains an entirely new level of credibility in the mind of the traditional war fighter if it can claim the relatively venerable, proven, and effective field of EW as its own. Given the push to establish cyberspace as a new domain, one can

easily understand why the DOD initially adopted Kuehl's physical definition of cyberspace.

However, this approach quickly encounters difficulties. If radar belongs to cyberspace, then why not sonar? After all, it serves essentially the same purpose—broadly speaking—but does not leverage the EMS in any meaningful way. The airborne laser is also problematic for the opposite reason because it relies almost completely on the EMS to create effects, but any definition of cyberspace that includes laser weapons would be too broad and thus nearly useless for any practical purpose. Virtually all intelligence, surveillance, and reconnaissance; tactical sensors; and the human eye depend upon the EMS.

Although we can largely characterize cyberspace (however we choose to define it) by the use of electronics and the EMS, doing so creates some practical problems doctrinally. Associating the EMS with cyberspace leads to gathering EW and, potentially, directed energy operations under the same umbrella as computer network operations. This results in managing wholly disparate, highly specialized skill sets under one structure despite their having little to no commonality in training and doctrine. Furthermore, from a theoretical and doctrinal standpoint, electronics and the EMS are largely irrelevant in conceptually defining cyberspace, and their inclusion distracts from the truly defining characteristics of cyberspace.

Circumscribing cyberspace in terms of its use of electronics and the EMS may seem intuitively obvious, but it remains a rather superficial way to describe the domain. After all, if cyberspace primarily leveraged quantum effects to process, store, and exchange information, would it not still be fundamentally the same from an operational perspective? The physical mechanisms used by the technology employed in cyberspace to produce effects are not defining characteristics of the domain—no more so than tanks and artillery are defining characteristics of the land domain.[11]

Now that cyberspace has been successfully established as a serious military concern, forced analogies to other domains have largely out-

lived their usefulness in advancing cyberspace theory and doctrine. As noted before, the DOD and Air Force have moved away from a physically oriented model of cyberspace, as evidenced by the implementation of their new definitions, organization, and processes. We no longer treat EW as part of cyberspace, and we base training and force development on a computer-network-centric view of the domain.[12] The nascent Air Force cyber warfare career field consists primarily of former communications personnel.[13] Cyber warfare doctrine and thinking appear to be getting on the right track.

Unfortunately, considerable inertia still accompanies the old models of describing cyberspace—an understandable situation, given their appeal to traditional military sensibilities. Recent papers continue to refer to and emphasize physical aspects of cyberspace that have little or no practical bearing above a technical or tactical level, despite ostensibly attempting to formulate domain-specific theory. In 2009 one such treatise on the Chinese cyber threat explicitly took issue with the updated (2008) DOD definition of cyberspace, calling back to the old physically oriented model by observing that cyberspace must also "encompass not only the actual military and civil electronics devices, but also the electromagnetic spectrum on which the information . . . travels."[14] The author goes on to stress that "strictly independent [computer network operations], Electronic Warfare (EW), and Space Operations [would] instead be incorporated within the overarching and ethereal, but 'physical,' domain of Cyberspace. Not dissimilar to the domains of Land, Sea, and Air."[15] In 2011 an article in *Joint Force Quarterly* explicitly referred to "cyberspace (that is, the electromagnetic spectrum)."[16] Even Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations* (2010), still shows the residue of overemphasizing the EMS although it follows the DOD's lead by stopping well short of equating the two.[17]

Undue emphasis on the physical aspects of cyberspace could impair clear insights by diffusing or artificially circumscribing the domain, thus potentially deflecting more profitable lines of thought. Dr. Samuel Liles, associate professor at the National Defense University, argues

that "focusing on one aspect of cyberspace (EMS) creates a strategic and conceptual blind spot to leadership. It also has a tendency to focus consideration of risk via threats and vulnerabilities on transmission mechanisms."[18] Accordingly, continued propagation of a physically oriented paradigm of cyberspace reinforces these flawed viewpoints in the academic and, to some extent, operational communities. Cyberspace clearly has a physical element, but the implications are relatively obvious, falling cleanly within existing doctrine for physical attack, EW, and other well-worn disciplines. However, cyberspace differs fundamentally from other operational domains in a number of ways that sometimes defy attempts to apply established military principles.

Identifying the truly meaningful, unique characteristics of warfare in cyberspace will help focus the minds of theoreticians, allowing them to make more efficient progress in the field by determining how cyber warfare substantively departs from established theory and doctrine. Thus, they can also clarify the principles of this relatively new and unfamiliar operational domain for the strategist and commander, helping them make more intuitive decisions as they operate within it.

The Unique Character of Cyberspace

The ability to process, store, and exchange large amounts of information rapidly, using automated systems, is the defining characteristic of cyberspace—the physical methods are superficial. In fact, its logical or virtual nature, rather than its physical mechanisms, sets cyberspace apart from other domains. This characteristic leads to a number of implications, some more obvious than others.

Perhaps the most often-cited distinguishing attribute of operating in cyberspace is its speed.[19] Indeed, the observation that cyber warfare takes place "(almost) at the speed of light" has become a cliché. For most purposes, physical distances in cyberspace are almost meaningless—only logical topology matters. Planning and preparing for an attack may take weeks or more to develop the necessary intelligence

and accesses, but, once launched, the strike may well be over in a matter of seconds. Consequently, in many cases we may not realistically be able to react to an attack in progress. Often, a defender can do nothing more than deny the most damaging avenues of attack in advance, enable detection, and respond quickly to mitigate and remediate its effects. A head-to-head confrontation between offensive and defensive forces in real time rarely occurs.

This brings up another interesting point. Cyber war is unusual in the sense that offensive and defensive forces are highly asymmetrical, compared to those in other domains.[20] Defensive forces primarily include system administrators who oversee various networks, response teams that quickly perform forensics and remediation, intrusion detection analysts, and so forth, perhaps along with software developers who hurriedly patch newly discovered flaws, and private antivirus companies that develop signatures to inoculate systems to new malware.[21] Meanwhile, highly specialized offensive forces use almost entirely different tools to attack networks, often attempting to remain undetected for the duration of the operation. Two opposing offensive cyber forces do not meet in cyberspace to wage battle, as in other "kinetic" domains; even if they did, the participants do not find themselves at physical risk—a fact that complicates efforts to erode an enemy's capacity to wage cyber war.[22]

In *Cyberdeterrence and Cyberwar*, RAND's Martin Libicki explains in detail the difficulty or impossibility of disarming an enemy's cyber capabilities: "Indeed, since hackers need only an arbitrary computer and one network connection, it is not clear that even a physical attack could destroy a state's cyberattack capabilities."[23] A state's most irreplaceable offensive assets in a cyber war are its talented hackers and its stockpile of exploits. The state can keep both of them well protected from physical and cyber attack unless it becomes so overwhelmed that the war's outcome is no longer in doubt. Even the generally expendable computer systems used by a state's cyber force are difficult to hold at risk through cyber means since they can be hardened much

more effectively than a typical workstation or server without sacrificing functionality; moreover, an assailant likely would have difficulty pinpointing them on the network in the first place. A combination of physical and flooding attacks to sever a state completely from the Internet could theoretically deny its cyber forces an attack avenue (if they cannot covertly relocate physically to an ally or unknowing third party). Doing so, however, would produce a reciprocal effect by preventing attackers from penetrating the enemy's networks.

All of this implies that "offensive counter cyberspace," a term presented without comment in AFDD 3-12, may prove meaningless or at least radically different from offensive counterair (OCA), after which it is clearly modeled.[24] Although the standard definition of OCA is rather broad (and could be construed to include cyber, at least to some extent), we commonly think of it in terms of diminishing an adversary's offensive air capability through application of our own airpower.[25] As discussed above, we may not realistically expect to substantially diminish an adversary's offensive cyber capability through offensive cyber means alone (or even by kinetic means). This does not mean that offensive cyber capability is useless—merely that these particular opposing forces may not significantly affect each other, at least not directly or in ways suggested by OCA.

Not only do offensive cyber forces remain immune to attack, for the most part, but also the defensive forces can easily grow stronger over the course of a cyber war, even if it is going badly. Specifically, network attacks reveal vulnerabilities that allow defenders to patch or otherwise mitigate these offensive avenues so that the same enemy tools may not work for very long. As Libicki puts it, an "attacker will find it continually harder to hit similar targets because they harden as they recover from each new attack."[26] Thus, "cyber weapons" are highly perishable but relatively slow and costly to develop, so the potential for attack may diminish over the course of a war.[27]

Meanwhile, a commander generally does not have to accept greater vulnerability in order to "mass forces" elsewhere. Since offensive

forces are probably separate and distinct from defensive forces, in cyberspace we do not need to consider how to allocate combat capability to "cover flanks" or trade off offensive firepower to ensure the security of lines of communication and rear areas. All of these factors combine to suggest that attrition may not exist in cyber warfare, at least not in the classic sense.

If cyber forces cannot realistically perform counterforce missions within their own domain, then the Air Force must change the way it approaches wartime objectives in cyberspace versus the air. According to AFDD 3-01, *Counterair Operations*, "Control of the air is normally one of the first priorities of the joint force. This is especially so whenever the enemy is capable of threatening friendly forces from the air or inhibiting a joint force commander's (JFC's) ability to conduct operations."[28] Replacing "the air" with "cyberspace" in this passage reveals how Airmen could draw an easy parallel and come to the conclusion that cyber forces must prioritize attaining "cyberspace superiority." This may be possible in some sense, but it may simply mean being better at attack and defense than the enemy. This statement is not quite as vacuous as it may seem at first blush.

We do not secure "control of cyberspace" by conducting cyber operations against the adversary to weaken his capabilities while protecting our own; rather, we field a capable, well-trained, and well-resourced force, relative to the adversary's. Thus, such control is no longer an operational objective but something largely determined at the outset of hostilities, a result of strategic planning and preparation during peacetime. If we engage in a cyber war with inferior forces, we cannot depend upon superior tactics to outmaneuver the opponent, inflict greater losses, and turn the tide (for various reasons described above). Thus, "cyber superiority" has little use as a doctrinal term because it is not something that we design campaigns to attain. Instead, it is a shallow descriptor of the relative quality of forces on which commanders will exert little influence in wartime. If the enemy clearly derives substantially greater military benefit from cyberspace (i.e., has "superiority"),

a commander may have only one major lever available: Take cyberspace "out of play" to an extent, either by isolating his or her forces from the Internet or by doing the same to the adversary through physical (or even logical) attack—obviously a drastic measure and easier said than done.

Conclusion

As a war-fighting environment, cyberspace differs fundamentally from the traditional physical domains, primarily due to its logical/virtual nature. It requires as much of a reexamination of basic principles as did air, relative to land and sea warfare. This unique character challenges many assumptions about waging war. If we cannot (directly) apply such elementary concepts as attrition or counterforce to cyber warfare, then we should be cautious about trying to force other principles of warfare into cyber doctrine.

Few, if any, strong examples of "cyber war" exist from which we can draw combat-proven lessons learned.[29] Consequently, individuals who craft new doctrine will naturally gravitate to the tried and true in other domains and attempt to graft those bits of wisdom to this new arena. However, even if we can rationalize a way to link cyber operations to some venerated theoretical framework, doing so may prove pointless if it yields no greater insight into waging war effectively. Rather than ask ourselves how a certain tenet applies to cyber, we should first inquire about whether it pertains to cyber in any meaningful way. Only by honestly assessing the idiosyncrasies of cyberspace can we usefully apply established wisdom and forge ahead with new doctrine. ✪

Notes

1. Jeff Boleng, Dino Schweitzer, and David Gibson, "Developing Cyber Warriors" (presentation, Third International Conference on i-Warfare and Security, US Air Force Academy, Colorado Springs, CO, September 2007), http://www.usafa.edu/df/dfe/dfer/centers/accr/docs/boleng2008a.pdf.

2. Any observations about the conference not cited in the notes are the recollections of the author, who attended it.

3. Department of Defense, *The National Military Strategy for Cyberspace Operations* (Washington, DC: Department of Defense, December 2006), ix, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.

4. Maj Gen Bill Lord, "Air Force Cyber Command (P) Update" (presentation, Armed Forces Communications and Electronics Association, Boston [Lexington-Concord chapter], 23 January 2007), slide 17, http://www.afceaboston.com/documents/events/nh08/Gen_Lord.pdf.

5. Chairman of the Joint Chiefs of Staff, memorandum 0363-08, July 2008. See also Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 August 2012), 77, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

6. It is difficult to prove a negative assertion since the Air Force evidently has no official statement that explicitly excludes combat systems officers from the cyber career field or EW in general from the cyberspace domain. However, references to such officers in recent Air Force literature on cyberspace seem to be very rare, sparse, and undeveloped; furthermore, the service generally seems to treat cyberspace as virtually synonymous with information systems and data networks—especially computer networks based on Internet protocol. We can state with assurance, though, that the 12R career field (EW combat systems officer) remains separate, not wholly subsumed into the cyber officer career field as initially planned—unlike the 33S (communications) career field. Headquarters Air Force Personnel Center, *Air Force Officer Classification Directory* (Randolph AFB, TX: Headquarters Air Force Personnel Center, 1 August 2012), 48.

7. The White House did issue guidance in March 2011 curbing public references to cyberspace as a military operational domain fully on par with land, sea, air, and space. But the very existence of such high-level guidance is a good indicator that the field of cyber warfare is getting far more attention than it ever has before. White House, memorandum, subject: White House Guidance Regarding the Use of "Domain" in Unclassified Documents and Public Statements, 14 March 2011.

8. Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), 17.

9. "Information as an environment may be a difficult concept to grasp, but there is no arguing that there is a physical environment to which information is uniquely related: cyberspace. Cyberspace is that place where computers, communications systems, and those devices that operate via radiated energy in the electromagnetic spectrum meet and interact." Dan Kuehl, "Defining Information Power," *Strategic Forum*, no. 115 (June 1997): 3, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA394366. See also Kuehl, "The Information Revolution and the Transformation of Warfare," in *The History of Information Security: A Comprehensive Handbook*, ed. Karl de Leeuw and Jan Bergstra (Amsterdam: Elsevier, 2007), 823n6.

10. Lani Kass, "A Warfighting Domain," 26 September 2006, slide 14, http://www.au.af.mil/info-ops/usaf/cyberspace_taskforce_sep06.pdf.

11. "Explosive chemical reactions" is probably a truer analog, albeit perhaps less intuitive. Much like the EMS vis-à-vis cyberspace, it is a key physical phenomenon conspicuously exploited in operating not only within the land domain but also across the other domains.

12. The Undergraduate Cyber Training curriculum offers evidence of the focus on data-network-centric training. Julie R. Karr, "Cyberspace Force Development," 18 May 2011, slide 8, http://www.safxc.af.mil/shared/media/document/AFD-110614-028.ppt.

13. "30 Apr 10: 33S [communications] personnel/billets convert to 17D [cyber officer]. . . . Re-aligned 15 [communications and information] AFSCs [Air Force specialty codes] into 11 3DXXX [enlisted cyber] AFSCs." Brig Gen David Cotton, "Cyberspace Workforce Transformation Update," May 2010, slides 14, 15. Despite efforts to identify talented members of other AFSCs, particularly in the officer corps, to transition them into the cyber career field, former communications officers still dominate numerically since converting en masse to the new AFSC, and the emphasis remains on computer network skills.

14. LCDR Jorge Muñiz Jr., USN, "Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors" (thesis, US Army Command and General Staff College, 2009), 2, http://www.hsdl.org/?view&did=11694.

15. Ibid., 5.

16. Benjamin S. Lambeth, "Airpower, Spacepower, and Cyberpower," *Joint Force Quarterly*, issue 60 (1st Quarter 2011): 46, http://www.ndu.edu/press/lib/images/jfq-60/JFQ60_46-53_Lambeth.pdf.

17. "[Cyberspace] requires . . . emphasis on the electromagnetic spectrum. . . . Systems may also be designed to change frequencies (the places where they operate within the EMS) as they manipulate data. Thus, physical maneuver space exists in cyberspace." Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, 15 July 2010 (incorporating change 1, 30 November 2011), 2, 3, http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf.

18. Samuel E. Liles, "An Argument for a Comprehensive Definition of Cyberspace," *Selil* (blog), 18 November 2011, http://selil.com/archives/2712.

19. There is no shortage of references to this idea, but, to take one example, AFDD 3-12 notes that "in cyberspace, the time between execution and effect can be milliseconds" and that "operations can take place nearly instantaneously." AFDD 3-12, *Cyberspace Operations*, 29, 9.

20. One must note the possible exception of space, which has its own idiosyncrasies that fall outside the scope of this article.

21. This is an interesting aspect of cyberspace in its own right—that independent, private companies could legitimately be considered part of national military defense forces in some regard.

22. One might observe that certain access operations could require that team members put themselves in physical proximity to an adversary's network, thus placing them at risk. The author argues that this actually constitutes special operations support to (or conduct of) cyber operations rather than actual "offensive cyber forces." Furthermore, the forces that would place them at physical risk certainly are not offensive cyber forces.

23. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 60, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

24. AFDD 3-12, *Cyberspace Operations*, 52. Offensive counter cyberspace is also identified as the seventh of nine prioritized "key cyber capability areas for the Air Force." *Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012–2025* (Washington, DC: AF/ST [Science and Technology], 15 July 2012), 19.

25. OCA involves "operations to destroy, disrupt, or neutralize enemy aircraft, missiles, launch platforms, and their supporting structures and systems both before and after launch, and as close to their source as possible. The goal of OCA operations is to prevent the launch of enemy aircraft and missiles by destroying them and their overall supporting infrastructure prior to employment." JP 3-01, *Countering Air and Missile Threats*, 23 March 2012, I-3, http://www.dtic.mil/doctrine/new_pubs/jp3_01.pdf. "OCA includes targeting enemy . . .

command and control, communications, cyberspace, and intelligence nodes." AFDD 3-01, *Counterair Operations*, 1 October 2008 (interim change 2 [last review], 1 November 2011), 5–6, http://www.e-publishing.af.mil/shared/media/epubs/afdd3-01.pdf.

26. Libicki, *Cyberdeterrence and Cyberwar*, 59.

27. Libicki explores this concept in more detail in ibid., 56–59. He raises the possibility of a cyber war's "petering out" as attacks become less effective over time (ibid., 135).

28. AFDD 3-01, *Counterair Operations*, 1.

29. In several isolated instances, cyber operations have taken place (e.g., allegedly during Operation Orchard and the Stuxnet worm, also known as Olympic Games). However, these fall short of open warfare in the cyber domain (although they very well might serve as the model for how cyber attacks are most commonly used in actuality—surgical covert operations). Some individuals may argue that Russia's cyber attack on Georgia in 2007 represents a "strong example of cyber war"—perhaps the strongest one to date. Nevertheless, in this case the disparity between the two sides makes it hard to say whether the cyber aspect of the attack had any meaningful impact on the conflict. One would have difficulty advocating this example as a foundation for cyber warfare doctrine.

Maj Sean C. Butler, USAF

Major Butler (BS, University of Southern California; MS, Air Force Institute of Technology) is a member of the faculty at Air Command and Staff College, Maxwell AFB, Alabama. He earned his commission through the Air Force Reserve Officer Training Corps at the University of Southern California. Major Butler served in the 23rd Information Operations Squadron, Lackland AFB, Texas, developing network warfare tactics. As an assistant professor who directed and taught the US Air Force Academy's network security course, he guided the cadet team to a win over the other service academies in the 2004 Cyber Defense Exercise. At the academy, he was one of a group of Air Force subject matter experts selected to "ops test" the Undergraduate Network Warfare Training course in 2007, and he helped develop the curriculum that became the foundation of the Air Force's current cyber force training.