Air Force Institute of Technology
AFIT Scholar

Faculty Publications

Spring 2010

Cyber This, Cyber That...So What?

Eric D. Trias
Air Force Institute of Technology

Bryan Bell [*]
Air Force Institute of Technology

Follow this and additional works at: https://scholar.afit.edu/facpub

 Part of the Infrastructure Commons, Management and Operations Commons, and the Military History Commons

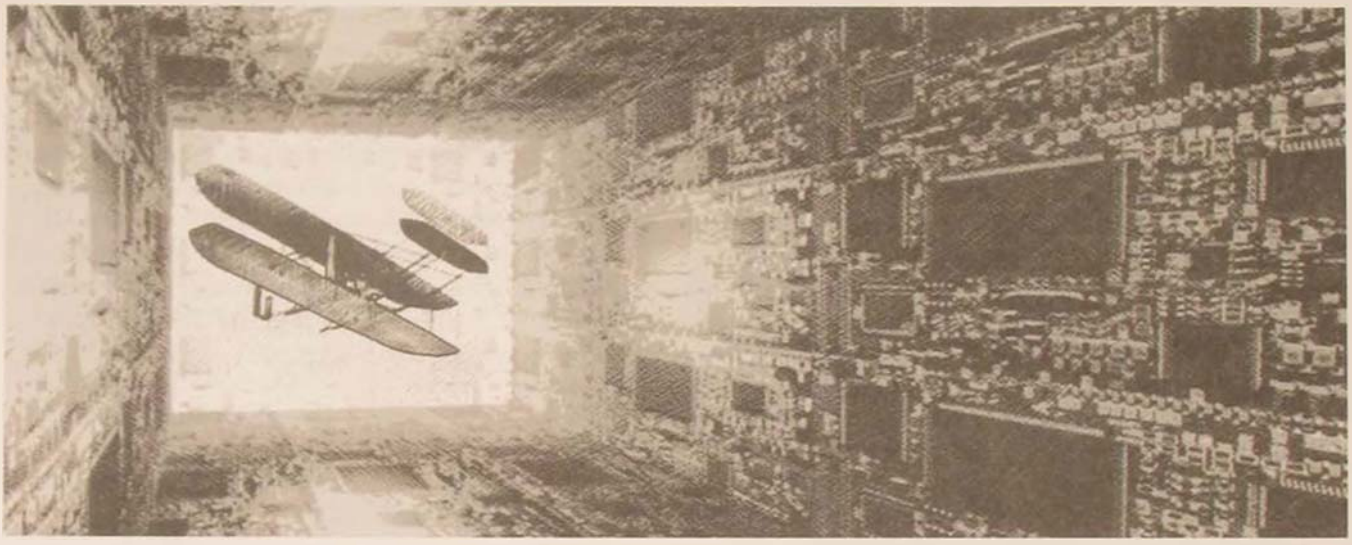
Recommended Citation

Trias, E. D., & Bell, B. M. (2010). Cyber this, cyber that ... so what? Air & Space Power Journal, 24(1), 90-100.

This Article is brought to you for free and open access by AFIT Scholar. It has been accepted for inclusion in Faculty Publications by an authorized administrator of AFIT Scholar. For more information, please contact AFIT.ENWL.Repository@us.af.mil.

Cyber This, Cyber That . . . So What?

Maj Eric D. Trias, PhD, USAF
Capt Bryan M. Bell, USAF



You have to know the past to understand the present.

—Carl Sagan

Revolutions in warfare rarely take place in one's lifetime. Rather, an evolution based on the innovative use of available technology and human ingenuity steadily occurs.[1] Is the ubiquity of cyberspace operations and technology such a revolution? Perhaps. However, any revolution should not compel us to leave behind lessons learned from the age before cyberspace. Assiduous students of warfare will still find that books on military history, theories of war, doctrines, and publications on past conflicts are invaluable. Cyberspace does not change the principles of war or the tenets of airpower from the Airman's perspective. At an even more granular level, only minor changes are required to the US Air Force's air and space (and cyberspace) functions.

When the chief of staff and secretary of the Air Force added cyberspace to the service's mission statement in December 2005, it became powerfully clear that the Air Force was serious about its role in providing capabilities in cyberspace operations to the joint fight.[2] As a result, the Air Force community, along with its counterparts in other services, has been busy developing supporting documents and guidance to define and focus what the fledgling mission area means to the force. Cyberspace is everywhere we turn; it is an essential part of our daily mission and activities. However, we must remember that our fundamental functions as an Air Force have not changed.

This article endorses the idea that cyber operations may be conducted in all warfighting domains: air, space, cyberspace, land, and sea. In addition, despite the immaturity of cyberspace operational doctrines, the doctrines from air and space remain relevant and applicable to the cyberspace domain. Cyber operations are just another set of tools in the commander's toolbox. Although cyber operations have distinct ways of achieving effects, from an Air Force perspective they are similar to other air and space operations that support air and space (and cyberspace) functions. Known and established cyber operations provide war fighters with viable options to kinetic means. This article highlights the role of cyber operations in supporting the air and space functions.

Lastly, we add a new function, *countercyberspace*, to the 17 Air Force functions (see table). Past Air Force doctrine has used different nomenclature but has not made the importance of countercyberspace completely clear until recently. For this reason, the new function necessitates adjustments to the existing information operations (IO) function to account for duplication. By showing that cyber operations are just another set of tools, we can integrate previously defined supporting operations in an initial development of cyberspace operations doctrine. Eventually, a more concrete Air Force cyberspace doctrine will evolve as prescribed by lessons from history and future events.

Doctrine is an integrated collection of lessons learned from experiments, exercises, and past engagements that we accept as the *best practices* for conducting warfare.[3] Still in their infancy, cyberspace operations consequently lack the history of experience vital for establishing sound doctrinal statements. Dr. David Lonsdale remarked that "new or developing methods of warfare require doctrinal and theoretical development [that] should be grounded in, and informed by, experience, historical knowledge, and the work of the universal theorists, most especially Carl von Clausewitz and Sun Tzu."[4] Air Force strategists are struggling to create doctrinal principles for cyber warfare in the form of Air Force Doctrine Document (AFDD) 2-11, "Cyberspace Operations," now several years in draft. However, we must be careful to derive cyber doctrine and strategy from the proven methods of previous documents and must examine how we can employ cyberspace operations in support of Air Force functions.

The Air Force functions defined in AFDD 1, *Air Force Basic Doctrine*, are those specific responsibilities that enable the service to fulfill its legally established roles as noted in Title 10, *United States Code*, section 8013. The operational functions listed in the table are the "broad, fundamental, and continuing activities" of air, space, and cyberspace power.[5] "They are not necessarily unique to the Air Force . . . but together they do represent" how the service fulfills its assigned missions.[6] The following sections address each of the air and space functions, discussing how cyberspace operations can provide the same effects and serve as the appropriate foundation for cyberspace doctrine.

Strategic Attack

The goal of strategic attack is to apply force systematically against enemy centers of gravity in order to produce the greatest effect for the least cost in dollars and lives.[7] As illustrated by Col John Warden's five strategic rings, these centers may be material (infrastructure) or nonmaterial (populace support) in nature. He further advocates attacking the three elements of command—information gathering, decision making, and communication (e.g., bombing

Table. Air Force air, space, and cyberspace functions

Function	*General Definition*	*Air and Space Example*	*Cyber Tasks*
Strategic Attack	Systematic application of force against enemy centers of gravity	Destroying leadership, power, and communication hubs	Attack on supervisory control and data acquisition and Internet traffic
Counterair, Counterspace, Counterland, Countersea	Operations conducted to attain and maintain a desired degree of superiority within a domain while denying an adversary use of that same domain	Air interdiction, close air support, suppression of enemy air defenses, jamming satellite up/ downlink frequencies	Manipulating databases, images, power/controls of a weapon system
Information Operations	Actions to support commanders' ability to assess the operational environment and enhance their observe-orient-decide-act loop	Influence operations, electronic warfare, military deception, counterintelligence	Manipulation of Web content, e-mail "leaflets"
Airlift, Air Refueling, Spacelift	Activities that extend the reach of personnel and materiel in order to provide rapid, functional, flexible, timely, and responsive options	Intratheater airlift, operational support airlift, deployment launch	Messaging e-mail, Web pages, remote network administration
Intelligence, Surveillance and Reconnaissance	Activities that contribute to the creation of the intelligence preparation of the battlespace in order to provide commanders detailed knowledge that helps them better understand and know the enemy	U-2s, remotely piloted aircraft, national assets, human intelligence	Search engines, network enumeration, honey pots, packet sniffing
Special Operations	Operations that use mobility in denied territory, surgical firepower, and special tactics to conduct low-visibility, covert, or clandestine military actions	Special reconnaissance, psychological operations, counterterrorism	Address masking, Internet cafes, botnets
Combat Support, Command and Control, Combat Search and Rescue, Navigation and Positioning, Weather Services	Actions that enable the war fighter to focus on and successfully carry out those operations related to the above functions	Aircraft maintenance, air and space operations center, global positioning system satellites, National Oceanic and Atmospheric Administration satellites	Net-centric operations, command and control, and network terrain packets
Countercyberspace	Operations conducted to attain and maintain a desired degree of cyberspace superiority by destroying, degrading, denying, deceiving, disrupting, or exploiting the enemy's cyberspace capability	Bombing server buildings	Software exploits

Derived from Air Force Doctrine Document 1, *Air Force Basic Doctrine*, 17 November 2003, 39–58, http://www.dtic.mil/doctrine/jel/service_pubs/afdd1.pdf (accessed 8 December 2009).

Iraq's communications infrastructure during Operation Desert Storm, as shown on Cable News Network).[8]

The cyberspace domain provides adversaries a new environment to conduct offensive and defensive operations. In addition, cyber operations offer the means to expedite other operational functions previously conducted through other domains. "In the effort to influence—whether focused on an individual, an organization, or an entire society—cyberspace is a key operational medium via which 'strategic influence' is conducted."[9] However, considering modern organizations' and nations' dependence on the world's cyberspace infrastructure, new sources of vulnerabilities are tempting targets for strategic attack, especially from an asymmetric form of warfare.

Over the past few years, the ability to use cyber operations as an avenue for strategic attack has become evident. In 2007 the Idaho National Laboratory for the Department of Homeland Security simulated a cyber attack on a test power station. The simulation demonstrated an exploitation of a software vulnerability in Supervisory Control and Data Acquisition (SCADA) systems, the computer systems that control electric, water, and chemical plants throughout the United States. Designed with minimal security protection, many of these systems remain vulnerable to cyber attacks. Even terrorist organizations are interested in the vulnerabilities of strategic systems like SCADA.[10] Examples include the virtual shutdown of the Estonian government via its Internet infrastructure and the Russian-Georgian conflict of 2008, during which Russian military forces orchestrated a wave of cyber-related operations against Georgia prior to an invasion. Coordinated through a Russian online forum, the online assault appeared to have been prepared with target lists and details about vulnerabilities. The cyber attacks were carried out before the two countries engaged in a five-day ground, sea, and air war.[11]

Counterair, Counterspace, Counterland, Countersea

These operations are conducted "to attain and maintain a desired degree of superiority" within any of the physical domains by destroying, degrading, denying, deceiving, disrupting, or exploiting the enemy's capability within that same domain.[12] They are characterized by actions that are either offensive or defensive in nature. Offensive counteroperations inhibit the enemy from exploiting a particular domain to his advantage.[13] One goal of offensive counterair involves destroying the enemy's offensive air and missile assets before he can do the same in order to establish freedom from attack for friendly forces. Defensive counteroperations "preserve US/friendly ability to exploit" a domain in order to protect friendly capabilities.[14] During Operation Iraqi Freedom, coalition forces conducted a defensive counterspace operation to destroy an adversary's "ground-based global positioning system (GPS) jammers to preserve freedom to employ GPS-aided munitions by friendly forces."[15]

US military assets across all operational domains are infused with cyber technologies, as is the case for most modern militaries. The *Quadrennial Roles and Missions Review Report* of January 2009 outlines the Department of Defense's (DOD) desire to seek "strategic, operational, and tactical cyberspace capabilities that provide . . . warfighting effects within and through the cyberspace domain that are synergistic with effects within other domains."[16] Cyber-related tools and operations have become commonplace, if not prerequisites, in military operations. Systems such as data links shared among platforms and command and control (C2) centers, the Blue Force Tracker utilized by the US Army, and GPS-aided carrier-landing technologies employed by the US Navy have changed the execution of specific operations. However, they exist to support the same service functions.

Hackers have already demonstrated their ability to break into the DOD's and contractors' networks.[17] Gaining access to C2 databases on the Internet presents an opportunity to affect the timing of launching forces from garrison, the direction they take, and their actions upon arrival. A successful breach of weapon system communication/data-link architectures would easily allow us to disrupt the enemy's ability to execute his mission. Infiltration of the enemy's cyber-enabled systems would also let us manipulate his operating picture or influence the delivery of electric power or the operation of satellite control systems.

Information Operations

As defined by AFDD 2-5, *Information Operations*, IO exists to support commanders in determining the situation, assessing threats and risks, and making timely and correct decisions. Reliance upon accurate information and its speed of travel make dominating the information spectrum more important than ever. Currently, IO consists of influence operations, network warfare operations, and electronic warfare (EW) operations.[18] With the advent of cyberspace operations, it is apparent that network warfare operations fall under this new concept. However, a debate continues over the future of EW. After the publication of a doctrine for cyberspace operations, AFDD 2-5 must be revised to incorporate these changes.

This does not mean that the two are mutually exclusive. IO can be conducted in the cyberspace domain, as it has been for decades in other operational domains. However, not all IO can be considered cyberspace operations. For example, influence operations seek to achieve effects resulting in a change in the enemy's observe, orient, decide, act loop. Traditional means include dropping leaflets or using human messengers to conduct psychological operations (PSYOP). EW operations seek to achieve effects across the electromagnetic domain, including radio frequencies as well as optical and infrared regions of the spectrum. Traditional EW operations conducted by aircrews over the past 50 years are considered noncyber by entire communities.[19] "In Operation ALLIED FORCE . . . multi-service capabilities were combined in the form of 'jam to exploit,' demonstrating how opponent communications users can be herded to frequencies which intelligence may collect and exploit."[20] IO often consists of nonkinetic actions to defend our decision cycle and influence the adversary's, but it can also take the form of physical attack against tangible information infrastructures.

The offensive counterinformation activities of PSYOP, military deception, and information attack all have a place in the cyber realm. Well-trained cyber forces can influence enemy decision cycles by presenting misleading Web content or even changing information presented by reputable sources. Defensive counterinformation activities such as information assurance and operational-security protocols are already in place at all Air Force installations, some in noncyber form.

Airlift, Air Refueling, Spacelift

Airlift, air refueling, and spacelift extend the reach of personnel and materiel to provide rapid, functional, flexible, timely, and responsive options necessary to apply strategic global power to various crisis situations worldwide. Airlift capabilities are vital for delivering expeditionary forces and infrastructure with minimum delay.[21] These assets link theaters and locations within the same theater. Air refueling broadens the range of employment options available to the joint force commander. It enables fighter, bomber, cargo, and rotary aircraft to operate from bases safe from attack and conduct multiple missions without having to return to base when they are low on fuel. Spacelift deploys space systems to establish operational capability, sustains failed satellite constellations or replaces failing satellites, and augments constellations to in-

crease capability when the demand of current global operations is on the rise.[22]

These three functions are characterized by their ability to increase the range of military assets and deploy materiel to the fight. They are a measure of our capacity to project air and space power abroad. Operations within the cyberspace domain achieve the same effect with information as the payload. *Cyberlift* occurs regularly among computers connected via the Internet or other network infrastructures. That is, packets of data pass over Ethernet cables and wireless connections as messages communicated among users. Network administrators who frequently push patches and software updates are exercising cyberlift operations. Images and intelligence information are communicated globally. Just as airlift, air refueling, and spacelift are the physical assets of our forces, so are cyberspace operations the information enablers. Cyberlift permits the precision delivery of information. Getting the right information to the right person at the right time is critical in today's operational environment, whether for conducting time-sensitive targeting or air-dropping supply pallets to locations "outside-the-wire." The logistics behind focused information flow represents a challenge that we can answer by using appropriate cyberlift tactics, techniques, and procedures.

Intelligence, Surveillance, and Reconnaissance

Information collected by intelligence, surveillance, and reconnaissance (ISR) assets, such as the U-2 Dragonlady, satellites, and/or undercover personnel, contributes to creation of the intelligence preparation of the battlespace (IPB), which provides information to commanders to help them understand and know the enemy.[23] The easiest, and often most overlooked, way to conduct cyber ISR is merely to make use of Internet search engines. Operations-security practices to safeguard critical information are often disregarded or loosely implemented, giving us an opening to collect required intelligence easily. Network enumerating, another activity of cyber ISR, involves scanning an adversary's networks for vulnerabilities in his security architecture, allowing us to build plans for exploiting those networks during wartime. Additionally, establishing decoys within our own networks grants US cyber forces a facility for learning the type of information that our enemies look for and the techniques they employ for undermining our security protocols. By utilizing packet sniffers, we can capture and analyze packets that travel our networks. All of these activities allow us to characterize enemy capabilities with our cyber means, thus providing additional information to the IPB. Once inside our adversaries' networks, we can leverage cyber-ISR operations to conduct IPB.

Special Operations

Special operations use airpower operations to conduct actions that include, but are not limited to, unconventional warfare, special reconnaissance, PSYOP, and counterterrorism.[24] The difference between special operations and conventional operations lies in the degree of physical and political risk, overtness, operational techniques, mode of employment, independence from friendly support, and dependence on detailed operational intelligence and indigenous assets.[25]

The inherently clandestine nature of special operations parallels the ease of conducting stealthy cyber operations. In 2007 cyber attacks assailed the nation of Estonia. Newspaper, banking, and governmental agencies were subjected to a distributed denial-of-service attack by almost one million computers enslaved by cyber terrorists. National servers, routers, and switches were flooded with traffic and rendered essentially useless. Many fingers pointed to the Russian government. Attacks poured in from all over the world, but computer security officials say that some of the attackers were identified by their Web addresses, many of

them Russian and some from Russian state institutions.[26] However, a major issue with network attacks has to do with pinpointing the source. As Dr. Martin Libicki notes, "One will not be able to make reasonable attribution unless the attacker virtually announces its role."[27] Thus, one cannot respond without reasonably attributing the attacks. Even then, the attacks may come from allies or one's own systems.[28] This bodes well for those able to exploit the vulnerabilities of their enemies without leaving a cyber trail.

Combat Support, Command and Control, Combat Search and Rescue, Navigation and Positioning, and Weather Services

Combat support, C2, combat search and rescue (CSAR), navigation and positioning, and weather services are the backbone of the previously mentioned air and space power functions. Without the success of these functions, other functions cannot and will not succeed. Combat support is the product of successful logistical, medical, and force-support operations, whose synergy with other operations is essential for creating combat capability across the range of military endeavors.[29] C2 encompasses motivating forces into action to carry out the mission (command) and regulating those same forces to execute operations aligned with the commander's intent (control).[30] Effective C2 enables the joint force commander to utilize available Air Force platforms at the right place and time, despite the fog of war, and degrade the enemy's capability to intercede.[31] CSAR is the method that the Air Force uses to support joint personnel recovery in "uncertain, denied, or hostile environments."[32] Personnel recovery operations are essential to sustaining unit morale, preserving critical combat resources, and preventing the enemy from gaining intelligence.[33] By providing accurate location and time of reference, the navigation and positioning function enables military forces to maneuver precisely, synchronize actions, locate and attack targets, and locate and recover downed Airmen. Weather services offer timely and accurate information regarding the space and atmospheric environments. This information is critical in timing, planning, and conducting air and space operations, thus influencing "the selection of targets, routes, weapon systems, and delivery tactics."[34]

Cyberspace operations enable these functions, and communication over the cyberspace domain facilitates them. For the most part, precise navigation and timing rely on the cyberspace domain for signal transmission and dissemination of GPS data. Net-centric operations have made way for continued, efficient support of war fighters from bed, bullets, and beans to the C2 elements required. The weapon system represented by the Air Force air and space operations center consists of hundreds of servers running various information systems, each one operating in cyberspace.

Countercyberspace

We propose the following definition for *countercyberspace: a function consisting of operations to attain and maintain a desired degree of cyberspace superiority by the destruction, degradation, or disruption of an enemy's capabilities to use cyberspace.* This definition is similar to those of the other counter-domain functions listed above. Although it does include the requirement of superiority within the domain, this differs considerably from how we view air or space superiority. The draft version of AFDD 2-11 defines cyberspace superiority as "the degree of advantage possessed by one force over another that permits the conduct of operations in cyberspace at a given time and place without prohibitive interference by the opposing force."[35] Air and space superiority is characterized by freedom of action and simultaneous freedom from attack. Freedom of action is a characteristic of cy-

berspace superiority; however, due to the ubiquitous nature of the Internet, freedom from attack cannot be assured and thus is not a requirement for cyberspace superiority. An appropriate summary of cyberspace superiority would be "freedom of action through attack" (i.e., the ability to act even while under attack and after an attack). Gen Kevin P. Chilton, commander of US Strategic Command, concluded that "we went out in our mission-oriented protective posture (MOPP) gear and fixed airplanes, loaded airplanes, and flew airplanes. We conducted operations in a hostile environment. That's what operating under attack in cyberspace is going to be like."[36] We can be certain that cyberspace will remain a contested environment, but this should not constrain our ability to operate within the domain.

As a function, countercyberspace is comprised of various types of cyber and non-cyber-related operations. For example, if the desired effect is to disrupt Internet service, then physical attack or destruction of cyber-related equipment (e.g., routers and buildings housing Internet service providers) can be considered operations in support of countercyberspace. The effect also may be delivered in the form of a software exploit to disrupt legitimate Internet traffic from flowing properly. Consider one unclassified example. In May 2007, Pres. George W. Bush ordered the National Security Agency to conduct a cyber attack against cell phones and computer networks that Iraqi insurgents used to plan roadside bombings.[37] The agency's efforts helped US forces commandeer the Iraqi fighters' communication system. Former Bush administration officials involved with the decision to execute the attack "credit the cyberattacks with allowing military planners to track and kill some of the most influential insurgents," eventually helping turn the tide of the war.[38]

Both physical and cyber operations may produce the same direct effect in support of the countercyberspace function, but they have varying levels of indirect effects that must be considered. On the one hand, like any other attack, strikes against structures housing physical cyber assets have the potential to result in collateral damage. On the other hand, attacks through cyberspace against cyber assets can also result in cascading collateral damage. The fear of such side effects had kept American leadership from pulling the trigger of cyber weaponry. Prior to the recent US invasion of Iraq, DOD leaders considered a plan to disable the Iraqi banking network. However, they subsequently abandoned it after determining that it could also hinder the French banks so closely tied to Iraqi institutions and could potentially migrate to the other allies, including the United States.[39]

We propose the following definition for *countercyberspace: a function consisting of operations to attain and maintain a desired degree of cyberspace superiority by the destruction, degradation, or disruption of an enemy's capabilities to use cyberspace.*

We must give serious consideration to employing a cyber "munition" because it is not usually destroyed during an attack. Once released, such a weapon is easy to capture. Cyber forces can then deconstruct and analyze its code to determine appropriate countermeasures for future attacks and for use as a weapon against its sender.[40] To attain cyberspace superiority, we must execute successful offensive, defensive, and mainte-

nance operations through network attack, network defense, and network operations, respectively, in order to attain the level of control required to operate unimpeded while preventing the enemy from gaining advantage from the use of cyberspace.[41] Elevating countercyberspace operations as an Air Force function will help provide focus and set boundaries for the service and joint community.

Conclusion

Any cyberspace operational doctrine must take into account the similarities between and relationships with air and space operations. Many people agree with the draft cyberspace operations doctrine's statement that the cyberspace domain is a *man-made* virtual domain. Further study reveals its *natural* similarities to the other domains, as defined by the electromagnetic spectrum environment. Viewing the cyberspace domain as the fifth dimension (to air, land, sea, and space), more people conclude that it is no different than the other four dimensions, where we develop and use man-made technology to enter, maneuver, and exploit those domains.[42] In addition, the unique characteristics of the cyberspace domain dictate how we operate within it.

Cyberspace is a loaded term that invokes various definitions from different organizations and people.[43] Having limited operational experiences in cyberspace, the Air Force must use its experience in other warfighting domains in order to develop sound doctrine. After all, cyberspace operations support the same functions as air and space operations. As former secretary of the Air Force Michael W. Wynne wrote, "All aspects of air war will have some equivalent role in cyber war."[44] With the advent of cyberspace operations, some changes do need to take place, to include differentiating cyberspace operations from IO. Further, a new countercyberspace function should be added to underscore its importance as a separate Air Force function in the cyberspace domain. As Lonsdale points out, "Although cyberspace has a part to play in all of the dimensions, it does not fundamentally alter anything of real significance in strategy. Thus, like the air dimension before it, cyberspace affects the grammar of war, but not its logic."[45]

With time, our experience in conducting cyberspace operations and working in the cyberspace domain will grow and become embedded in our daily operations; we will accept those operations in the same way we do air and space operations. Cyberspace doctrine will evolve so that we can translate ideas into practice in the most effective way possible. In the meantime, we must examine and learn from the similarities and differences among air, space, and cyberspace operations in support of air, space, and cyberspace functions. ✪

Notes

1. "Observers constantly describe the warfare of their own age as marking a revolutionary breach in the normal progress of methods of warfare. Their selection of their own age ought to put readers and listeners on their guard. . . . It is fallacy, due to ignorance of technical and tactical military history, to suppose that methods of warfare have not made continuous and, on the whole, fairly even progress." Cyril B. Falls, *A Hundred Years of War* (London: Duckworth, [1953]), 13.

2. Hon. Michael W. Wynne, "Flying and Fighting in Cyberspace," *Air and Space Power Journal* 21, no. 1 (Spring 2007): 3, http://www.airpower.au.af.mil/airchronicles/apj/apj07/spr07/spr07.pdf (accessed 8 December 2009).

3. Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, 17 November 2003, 3, http://www.dtic.mil/doctrine/jel/service_pubs/afdd1.pdf (accessed 8 December 2009).

4. Dr. David J. Lonsdale, "The Impact of Cyberspace on Strategy," *High Frontier* 5, no. 3 (May 2009): 23, http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf (accessed 8 December 2009).

5. AFDD 1, *Air Force Basic Doctrine*, 39.

6. Ibid., 39–40.

7. AFDD 2-1.2, *Strategic Attack*, 12 June 2007, 2, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_1_2.pdf (accessed 8 December 2009).

8. Col John A. Warden, *The Air Campaign: Planning for Combat* (Washington, DC: National Defense University Press, 1988), http://www.au.af.mil/au/awc/awcgate/warden/warden-all.htm (accessed 8 December 2009).

9. Dr. Dan Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 6.

10. Kim Zetter, "Simulated Cyberattack Shows Hackers Blasting Away at the Power Grid," 26 September 2007, *Wired*, http://www.wired.com/threatlevel/2007/09/simulated-cyber/ (accessed 8 December 2009).

11. Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *Washington Post*, 16 October 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (accessed 8 December 2009).

12. AFDD 1, *Air Force Basic Doctrine*, 41.

13. AFDD 2-1.1, *Counterair Operations*, 1 October 2008, 5, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_1_1.pdf (accessed 8 December 2009).

14. AFDD 2-2.1, *Counterspace Operations*, 2 August 2004, 3, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_2_1.pdf (accessed 8 December 2009).

15. AFDD 1, *Air Force Basic Doctrine*, 43.

16. Department of Defense, *Quadrennial Roles and Missions Review Report* (Washington, DC: Department of Defense, January 2009), 16, http://purl.access.gpo.gov/GPO/LPS108437 (accessed 8 December 2009).

17. Associated Press, "Hacker Forces 1,500 Pentagon Computers Offline," 21 June 2007, http://www.msnbc.msn.com/id/19358920/ (accessed 15 August 2009).

18. Joint Publication 3-13, *Information Operations*, 13 February 2006, and DOD Directive 3600.01, *Information Operations*, 14 August 2006, more specifically list electronic warfare, computer network operations, psychological operations, military deception, and operations security as the five core capabilities of IO.

19. "Simply stated, EW is not part of Cyberspace. Cyber is a customer of EW. It certainly uses limited aspects of EW, but EW serves four other Domains—Land, Sea, Air and Space—that also need to achieve Spectrum Control. Within the Joint Service, the prevailing sentiment would indicate that EW will indeed remain an articulated mission area to exercise the critical care for and protection of the Spectrum, and not to be assimilated by any new peer mission area, such as Cyber." Lt Col Jesse Bourque, "Does EW + CNO = Cyber?" *Journal of Electronic Defense* 31, no. 9 (September 2008): 34.

20. AFDD 2-5, *Information Operations*, 11 January 2005, 23, http://www.carlisle.army.mil/DIME/documents/afdd2-5InformationOperations.pdf (accessed 8 December 2009).

21. AFDD 2-1, *Air Warfare*, 22 January 2000, 17, http://www.dtic.mil/doctrine/jel/service_pubs/afd2_1.pdf (accessed 8 December 2009).

22. Ibid., 18–19.

23. Ibid., 20–21.

24. AFDD 1, *Air Force Basic Doctrine*, 53.

25. AFDD 2-7, *Special Operations*, 16 December 2005, 3, http://www.fas.org/irp/doddir/usaf/afdd2-7.pdf (accessed 8 December 2009).

26. Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian*, 17 May 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (accessed 1 July 2009).

27. Dr. Martin Libicki, "Deterrence in Cyberspace," *High Frontier* 5, no. 3 (May 2009): 18, http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf (accessed 8 December 2009).

28. Shane Harris, "The Cyberwar Plan," *National Journal Magazine*, 14 November 2009, http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php (accessed 14 November 2009).

29. AFDD 1, *Air Force Basic Doctrine*, 47.

30. AFDD 2-1, *Air Warfare*, 14–15.

31. AFDD 2-8, *Command and Control*, 1 June 2007, 4–6, http://www.fas.org/irp/doddir/usaf/afdd2-8.pdf (accessed 8 December 2009).

32. AFDD 2-1.6, *Personnel Recovery Operations*, 1 June 2005, 10, http://www.e-publishing.af.mil/shared/media/epubs/AFDD2-1.6.pdf (accessed 15 December 2009).

33. AFDD 1, *Air Force Basic Doctrine*, 57.

34. AFDD 2-1, *Air Warfare*, 24.

35. AFDD 2-11, "Cyberspace Operations," draft, 4 February 2008, 13.

36. Gen Kevin P. Chilton, "Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities," *Air and Space Power Journal* 23, no. 3 (Fall 2009): 10, http://www.airpower.au.af.mil/airchronicles/apj/apj09/fal09/fal09.pdf (accessed 8 December 2009).

37. Harris, "Cyberwar Plan."

38. Ibid.

39. Ibid.
40. Ibid.
41. AFDD 2-11, "Cyberspace Operations," draft, 13–17.
42. Kuehl, "From Cyberspace to Cyberpower," 4.
43. In a Deputy Secretary of Defense memorandum of 12 May 2008, the DOD defines *cyberspace* as "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." Air Force doctrine defines it as "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." AFDD 2-11, "Cyberspace Operations," draft, 1.
44. Wynne, "Flying and Fighting in Cyberspace," 8.
45. Lonsdale, "Impact of Cyberspace on Strategy," 21.

Maj Eric D. Trias

Major Trias (BS, University of California–Davis; MS, Air Force Institute of Technology [AFIT]; PhD, University of New Mexico) is an assistant professor of computer science in the Department of Electrical and Computer Engineering at AFIT, Wright-Patterson AFB, Ohio. He enlisted in 1988 and was nominated for the Air Force Twelve Outstanding Airmen of the Year award in 1994. In 1998 he received his commission through the Airman's Education and Commissioning Program and Officer Training School. As a communications officer, he has served operationally at Osan AB and Camp Humphreys Army Installation, Republic of Korea, and at the Distributed Mission Operations Center, Kirtland AFB, New Mexico. He is a graduate of Squadron Officer School and Air Command and Staff College. Major Trias's current research interests include knowledge discovery and data mining, information systems security, digital forensics, and various cyberspace-related topics.

Capt Bryan M. Bell

Captain Bell (BS, University of Florida) is studying for a master of science degree in space systems in the Department of Aeronautics and Astronautics at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio. In 2005 he received his commission through the Reserve Officer Training Corps and joined the space and missile operations career field. Prior to attending AFIT, he served with the 7th Space Warning Squadron, Beale AFB, California, as a missile warning crew commander and instructor. He is a graduate of the Air and Space Basic Course. Upon graduation from AFIT, Captain Bell will serve as the officer in charge of component plans, US Strategic Command Joint Intelligence Center, Fort Meade, Maryland.