WSTIAC
Weapon Systems Technology Information Analysis Center

WSTIAC Quarterly
Volume 9, Number 4

Cyber Warfare

Understanding the Threat to Weapon Systems

WSTIAC is a DoD Information Analysis Center Sponsored by the Defense Technical Information Center

http://wstiac.alionscience.com/quarterly

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 APR 2010	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
WSTIAC Quarterly, Vol. 9, No. 4 - Cyber Warfare: Understanding the Threat to Weapon Systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **WSTIAC Weapon Systems Technology Information Analysis Center, Rome, NY**	8. PERFORMING ORGANIZATION REPORT NUMBER **WSTIAC-V9-N4**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) **Defense Technical Information Center, Ft Belvoir, VA**	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
This issue of the WSTIAC Quarterly features an article on Cyber Warfare: TheThreat to Weapon Systems and Cyber This, Cyber That... So What? Included submission are the WSTIAC Directors Corner and Training Courses sponsored by WSTIAC.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**16**	

Director's Corner

The tactics, weapons, and defense materiel and systems involved in warfare have been evolving for centuries and even millennia. While the battlefield and methods of engagement of opposing forces have also been evolving, the new tactics being implemented in cyberspace are revolutionizing warfare. *Cyber warfare* is essentially the use of networks and control systems to carry out organized disruptive, disabling, destructive or malicious attacks. Methods and targets of cyber-attack range from hiding malicious software in new computer products to gaining access to secure networks and disrupting functions of critical infrastructure such as power, transportation, and communication. Cyber warfare can also entail disrupting a military force by disabling communication and control among its various weapon systems.

Weapon systems are increasingly vulnerable to cyber warfare as they become more automated and networked. Current and future weapon systems are being infused with technological advancements, many of which are electronic, including sensors, communication systems, and control systems. For instance, various battlefield systems are being networked to provide augmented command and control ability. This establishes a battlefield advantage, and even though the systems are embedded with highly advanced security, any time there is opportunity for interconnection there is potential vulnerability to foreign access. Moreover, computer processors, memory, and other hardware are ubiquitous. While scans can be run on software and hardware, there is a potential for infiltration during development or manufacturing. Infiltration can thus enable a cyber attack on weapon systems.

One of the challenges associated with cyber warfare is that it is difficult to define since it is a relatively new and rapidly evolving form of warfare. As such, the policy and doctrine surrounding it are still being developed. Yet it is becoming increasingly important to take into consideration the impact of cyber warfare when designing the next generation of weapon systems. While presumably engagements will continue to occur on the physical battlefield throughout the century, this additional dimension of warfare will continue to expand its role in coming decades.

This issue of the *WSTIAC Quarterly* is especially focused on cyber warfare as it relates to weapon systems. In particular, the first article frames the threats of cyber warfare to weapon systems against a background of cyber-related definitions and military doctrine. In addition, the article provides a brief overview of some potential cyber warfare targets. The author encourages the development of more decisive cyber warfare doctrine that can lead to more robust weapon systems.

The second article presents cyber warfare as it permeates all aspects of warfighting environments including land, air, sea, space, and cyberspace. It further addresses the concept that cyber operations are additional methods through which mission objectives can be accomplished. This is an important viewpoint as it hopefully imparts a perspective on how those involved with weapon systems technology can influence cyber operations.

The two articles address the topic of cyber warfare from slightly different perspectives. One addresses the perspective of defending against cyber attacks, while the other discusses using cyberspace to conduct military operations. The intent of these articles is to stimulate some thought and discussion about where the crossroads meet between weapon systems technology and cyber warfare. I hope this issue proves to be useful in your continued efforts to support our warfighters.

John Weed, WSTIAC Director

The WSTIAC Quarterly *is the current awareness publication of the Weapon Systems Technology Information Analysis Center (WSTIAC). WSTIAC, a Department of Defense (DoD) Information Analysis Center (IAC), is administratively managed by the Defense Technical Information Center (DTIC) under the DoD IAC Program. All data and information herein reported are believed to be reliable; however, no warrant, expressed or implied, is to be construed as to the accuracy or the completeness of the information presented. The views, opinions, and findings contained in this publication are those of the author(s) and should not be construed as an official Agency position, policy, or decision, unless so designated by other official documentation. The appearance of an advertisement, announcement, product/service review, or article in the* WSTIAC Quarterly *does not constitute endorsement by the DoD or WSTIAC.*

Inquiries about WSTIAC capabilities, products, and services may be addressed to

JOHN WEED
DIRECTOR, WSTIAC
973.770.0123
EMAIL: jweed@alionscience.com
URL: HTTP://wstiac.alionscience.com/

ROBERT FITZGIBBON
BRUCE DUDLEY
TECHNICAL INQUIRIES
877.WST.USER
EMAIL: wstiac@alionscience.com

We welcome your input! To submit your related articles, photos, notices, or ideas for future issues, please contact:

WSTIAC
ATTN: BENJAMIN D. CRAIG
201 MILL STREET, ROME, NEW YORK 13440

PHONE: 315.339.7019 • FAX: 315.339.7107
EMAIL: wstiac@alionscience.com

Cyber Warfare: The Threat to Weapon Systems

Lionel D. Alford
Lieutenant Colonel USAF (retired)

INTRODUCTION

Carl von Clausewitz defined war as "…an act of violence intended to compel our opponent to fulfill our will… In order to attain this object fully, the enemy must be disarmed, and disarmament becomes therefore the immediate object of hostilities..."[1] This definition no longer describes the full spectrum of modern warfare. With today's software-intensive systems, the capability to attack a nation without the use of violence already exists, which fulfills the second half of von Clauswitz's definition of war to "disarm the enemy." The concept and use of cyber warfare has grown exponentially in recent years. Although cyber warfare is typically associated with information systems, this article describes how cyber warfare could potentially affect weapon systems.

> "Our foes have extended the fields of battle – from physical space to cyberspace."
>
> – President Clinton, 22 May, 1998

> Cyberspace is the nervous system – the control system of our country.
>
> – President George W. Bush
>
> George W. Bush, *National Strategy to Secure Cyberspace*, (The White House, February 2003)

Warfare Without Violence

The term cyber can be used to describe systems that employ mechanical or electronic systems to replace human control. In this article the term includes systems that incorporate software as a control element. Cyber warfare can be waged without executing a physical attack, and therefore the dependence on software intensive systems (cyber systems) can make nations vulnerable to warfare without violence.

Traditionally, the attacks carried out during war were focused on the physical components in a system (e.g., military personnel, weapons, facilities, and vehicles). The goal of war generally has been to disable and destroy these objects. Attacking these objects was viewed as the primary method of "disarming the enemy." From a strategic standpoint, these objects are targeted because they are part of a larger system:

- A system of manufacturing (attacked by strategic bombing)
- A supply system (attacked by interdiction bombing)
- A command and control system (attacked through blitzkrieg tactics)

In every case, the destruction of the components is intended to affect the whole, and if the attack does not disrupt the process, it at least reduces the number of combatants in the system. Though force is directed against the units in the process, the ultimate objective is to attack the process itself. These processes are potential "centers of gravity" of the enemy nation and forces.[1] By attacking the center of gravity, the enemy's capability to wage war can be "disarmed." If it were possible to attack a center of gravity without the use of force, a nation could be defeated without violence, and that capability would revolutionize warfare. For example, if an attack disrupted manufacturing without harming the machines or personnel, the effect would be the same as destroying all of the components in the system. It might be more effective because components and personnel can be replaced; the disruption of the system could result in longer lasting damage. If an attack disabled military systems, and if the nation could not detect and counter this kind of threat, it would be unable to defend itself. This kind of attack against systems and processes instead of components, if successful, would bring a nation to its knees without violence or a declared war.

Evolution of Information and Networked Systems

During the early stages of the World Wide Web cyber warfare was defined as the conduct of military operations according to information-related principles.[7] In other words, the term was being used to describe the disruption of military communication and coordination, or conversely, using information and communication systems advantageously. However, this definition no longer covers the full extent of capabilities now possible in cyber warfare. With the ever-increasing availability of inexpensive computer processors, memory, and other computer hardware, software is being used to control systems of all types, purposes, and sizes. Furthermore, as computer networks continue to expand throughout the world, all types of systems, such as infrastructure that supports civilization (e.g., electrical, oil, gas, transportation, and water treat-

DoD Cyber Warfare Doctrine

In spite of the fact that the DoD has been expanding cyber warfare doctrine and capabilities, as of November 2009 these actions are notably deficient.[2, 3] Joint Pub 3-13‡, Joint Doctrine for Information Operations, was updated in 2006, and Joint Pub 3-13.1, Joint Doctrine for Electronic Warfare was updated in 2007.[4, 5] DOD Directive O-3600.01, instituted in August 2006 still addresses cyber warfare in terms of "Information Operations."[6] As described in this article this is an inadequate approach to cyber warfare. In addition, instructions such as DOD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs handle information warfare as a discrete part of a military system. It does not address software as the major element of a weapon system; yet many software and software-controlled systems cannot be separated from the system being developed.

Table 1. Weapon system software dependencies.[8]

Aircraft	Year	Software Percentage of Functions
F-4	1960	8
A-7	1964	10
F-111	1970	20
F-15	1975	35
F-16	1982	45
B-2	1990	65
F-22	2000	80

ment systems), are being integrated or accessible via the global network.

Vulnerability of Weapons Platforms to Cyber Warfare

Weapon systems are also increasingly dependent on software, computer hardware, and battlefield networking, and therefore can be targeted through cyber systems. While the security of these weapon systems advance in step with the development and implementation of cyber technology, they can be increasingly affected by cyber attacks. Aircraft are a good example of the transition of cyber warfare to weapon systems.

In the past, 100 percent of an aircraft's performance and capabilities were defined by hardware (i.e., the physical makeup of the aircraft). In more recent, advanced aircraft, 75 percent or more of the aircraft's performance and capability is dependent on the software (see Table 1).[8] Without software, aircraft would not be controllable or reach the desired performance capabilities. For instance, the F-16 is unstable below Mach one, and uncontrollable without its software-based flight control system. The Boeing 777 and the Airbus 330 have software flight control systems without any manual backup; the performance of these aircraft is dependent on their digital flight control systems.

In some cases, through software, aircraft performance is gaining limited independence from physical configuration and therefore software dependence and hardware independence are growing. The F-22 in high angle of attack flight, for example, uses software controlled vectored thrust and flight controls to maneuver the aircraft. Furthermore, modern aircraft are fly-by-wire, their engines are control-by-wire, their weapons are fire- and drop-by-wire. Systems that in the past were entirely hardware with mechanical control are being replaced by software with software control.

Software also can determine the strength or effectiveness of a modern weapon system, and provides a basis for the integration of many disparate items through networking. These networked software systems, however, are now vulnerable to cyber attack, and the attacks and vulnerabilities are increasing (Figure 1).

Current doctrine (see sidebar) still does not address software as the major element of a military fighting system; yet as the above discussion shows, many software and software-controlled systems cannot be separated from the system being developed. The F-22 weapon system is an example of a software-controlled aircraft system that contains and communicates with integrated information systems (Figure 2). The F-22 is not a closed system; external information systems update and integrate F-22 combat operations during flight. Through these external connections, not just the information systems but the basic software and hardware systems of the F-22 can be attacked. Current information warfare doctrine in the

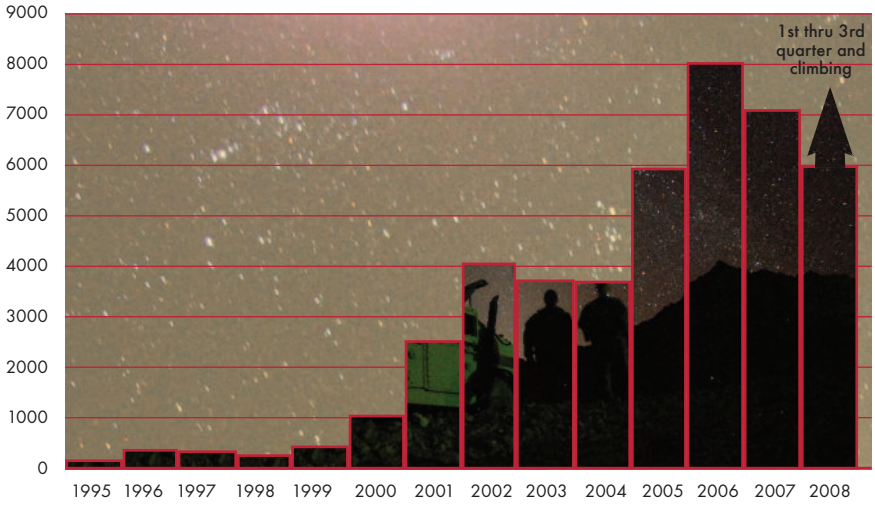


Figure 1. Number of vulnerabilities cataloged by CERT.[10]

CYBER WARFARE DEFINITIONS

The DoD Dictionary of Military and Associated Terms defines cyberspace and cyberspace operations as follows:[9]

Cyberspace – 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.

Cyberspace operations – The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

A NEW TAXONONY OF CYBER TERMS

Cyber warfare (CyW) – Any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system. CyW includes the following modes of cyber attack: cyber infiltration, cyber manipulation, cyber assault, and cyber raid.

Cyber infiltration (CyI) – Penetration of the defenses of a software controlled system such that the system can be manipulated, assaulted, or raided.

Cyber manipulation (CyM) – Following infiltration, the control of a system via its software which leaves the system intact, then uses the capabilities of the system to do damage. For example, using system's software to turn off power.

Cyber assault (CyA) – Following infiltration, the destruction of software and data in the system, or attack on a system that damages the system capabilities. Includes viruses, overload of systems through excessive data transfer.

Cyber raid (CyR) – Following infiltration, the manipulation or acquisition of data within the system, which leaves the system intact, results in transfer, destruction, or alteration of data.

Cyber attack – see CyI, CyM, CyA, or CyR.

Cyber crime (CyC) – cyber attacks without the intent to affect national security or to further operations against national security.

The concepts of cyber warfare also apply to cyber crime. Cyber crime is a critical consideration. To prevent international catastrophes, a nation must be able to differentiate between cyber crime and cyber

http://wstiac.alionscience.com/quarterly

Figure 2. Aircraft are more technologically sophisticated than ever, but as such are potentially more susceptible to cyber attack. (Photo courtesy of US Air Force.)

Joint Pubs is mainly concerned with security of external Command, Control, Communications, Computers, and Intelligence (C^4I) systems integrated on the F-22, but software-intensive systems make internal systems of the F-22 vulnerable to cyber warfare attack. Our doctrine must account for these vulnerabilities and provide methods of offense and defense. Although unclassified DoD publications and regulations do not adequately address cyber warfare, there is hope. The National Military Strategy for Cyberspace Operations from 2006, does correctly define and specify policy for cyber warfare.[11] Unfortunately, these policies have not permeated DoD doctrine.

CYBER WARFARE TARGETS

In general, cyber warfare targets include networks, digital systems, infrastructure, and any other element that acts as a information, communication, or control system.[12] Therefore, specifically for the DoD, any military system controlled by software is susceptible to cyber attack.

The first step in any attack is cyber infiltration; all systems that incorporate software are vulnerable to cyber infiltration. Actions following cyber infiltration can affect organizations via the transfer, destruction, and altering of records (i.e., cyber raid). Software within systems can be manipulated and the systems controlled by that software can be damaged or controlled (i.e., cyber manipulation). The software itself can be copied, damaged, or rewritten (i.e., cyber assault).

Military systems, including databases, will constantly be the targets of cyber warfare. The likelihood of a cyber attack on a weapon system is high during wartime, but relatively low during peacetime.

MILITARY TARGETS

Military Command, Control, Communications, Computers, and Intelligence

Modern military systems are dependent on Command, Control, Communications, Computers, and Intelligence. Military forces cannot fight without the coordination and communications provided through these systems. Military C^4I systems are particularly vulnerable, and are the primary focus of DoD cyber-related doctrine. JP 3-13 and JP 3-13.1 both provide doctrine for information related warfare. C^4I systems are a very complex mix – from radios to radars, mainframes to personal computers. Military C^4I uses interfaces through the Internet, base and organizational Local Area Networks (LAN), civilian and military communication systems, navigation systems, and radios in various frequency ranges. Military C^4I systems are particularly vulnerable because they interconnect. Cyber infiltration can occur at many points and potentially affect myriad systems. For instance, cyber warfare can affect the control of radars, missiles, and communications. It can potentially disable missiles, or redirect them to launch site. Furthermore it can disable or disrupt command and control networks, global positioning systems (GPS), and mobile communication systems.

These systems and their interactions are so complex that any modern military organization is unlikely to trace the full potential of any single cyber infiltration. The possibility exists for cyber attacks of

warfare. The definition of cyber crime is similar to cyber warfare, however it has two key differences. First, cyber crime is not waged between officially recognized political entities; cyber warfare is waged between entities that are governed by the laws of war. Second, the purpose of cyber crime is not to compel our opponent to fulfill our national will, while, this is the purpose of cyber warfare. Cyber crime can have as grave of ramifications as cyber war, but a key dimension of national policy is to differentiate between the two to prevent retaliations against nations when criminals are at work. A crucial aspect of cyber operations is that cyber warfare and crime are difficult to differentiate, and the warriors are not as obvious as in a shooting war. A nation will not have the political latitude to make many mistakes.

Intentional cyber warfare attack (IA) – any attack through cybermeans to intentionally affect national security (cyber warfare) or to further operations against national security. Includes cyber attacks by unintentional actors prompted by intentional actors. (Also see unintentional cyber warfare attack (UA).)

IA is equitable with warfare; it is national policy at the level of warfare. UA is basically crime. UA may be committed by a bungling hacker or a professional cyber criminal, but the intent is self-serving and not to further any specific national objective. This does not mean unintentional attacks cannot affect policy or have as devastating effects as an intentional attack.

Intentional cyber actors (I-actors) – individuals intentionally prosecuting cyber warfare (cyber operators, cyber troops, cyber warriors, cyber forces).

Unintentional cyber actors (U-actors) – individuals who make cyber attacks that may affect national security but are largely unaware of the international ramifications of their actions. Unintentional actors may be influenced by I-actors but are unaware they are being manipulated to participate in cyber operations. U-actors include anyone who commits CyI, CyM, CyA, and CyR without the intent to affect national security or to further operations against national security. This group also includes individuals involved in CyC, journalists, and industrial spies. The threat of journalists and industrial spies against systems including UA caused by their CyI efforts should be considered high.

Unintentional cyber warfare attack (UA) – any attack through cybermeans, without the intent to affect national security (cyber crime).

http://wstiac.alionscience.com/quarterly

every type and the results can be catastrophic. For instance, nuclear weapon control systems are incorporated into military C4I. As demonstrated by incursions in DoD networks, databases, and websites, almost any dedicated foe can engage in cyber attacks against military computer systems.[13, 14] Since military computers are the core of national C4I, successful IA and UA against such targets pose a national security peril.

> "Cyberspace is about operations, not communication. It is about operations, not a network. It is about how we do things to fight and win...We are a team of Airmen, civilians and contractors who enable joint forces to strike with precision, navigate with accuracy, communicate with certainty, see the battlefield with clarity and network with assurance."
>
> — Air Force General C. Robert Kehler
> 12 January, 2010

The US is currently executing campaigns with coalition forces, which may use equipment and systems that are not as technically advanced and do not utilize the latest security standards. Any integration or communication between forces could potentially open up additional security vulnerabilities.[15]

Weapon Systems

Current DoD doctrine does not adequately cover cyber attacks on military hardware systems, such as aircraft, vehicles, etc., that require software to operate.[16-18] As noted previously, the F-22 is a cyber-controlled aircraft (Figure 2). Infiltration and degradation of the aircraft's systems directly or via its C4I connections can be as devastating as shooting it out of the sky. Cyber infiltration of the C4I system providing data to modern aircraft allows an avenue for cyber raid, manipulation, and assault. Because many systems like the civilian Global Air Traffic Management (GATM) and the military's Tactical Targeting Networking Technology (TTNT) and the F-22 Intra-Flight Data Link (IFDL) automatically update aircraft information and intelligence, they can allow undetected infiltration of the aircraft.[19] Intelligence, navigation, and communication systems are integrated to each other and input and output to a host of other aircraft systems, including the flight control system (through the autopilot), propulsion system (through the autothrottles), radar system, master warning system, and environmental control system. Using the correct control sequences, inputs, or reprogramming, an infiltrator could produce any level of systems damage, from driving the aircraft off-course to overwriting the flight control software. UAVs are controlled from thousands of miles distance, and therefore the controls could be potentially hijacked. Many other weapon systems utilize similiar equipment and controls, and therefore are just as susceptible.

New Doctrine

What the above shows is that the DoD and the United States require a strong doctrine to address cyber warfare in all its potential forms including attacks on weapon systems. Taxonomy and cataloged security threats go a long way to build a framework for this doctrine. That is the first step in the development of a doctrine that includes all the dimensions of current and future cyber warfare threats. The challenge is to put the required effort and funding forward to ensure a strong level of security for all software-controlled systems.

NOTES & REFERENCES

‡ Joint Pub 3-13 provides the doctrinal foundation for the conduct of IO in joint operations.

[1] von Clausewitz, Carl, On War, Book I, translated by Michael Howard and Peter Paret, Princeton University Press, 1976.
[2] Jackson, W., "The Nation Needs a Clear Cyber War Doctrine," *Government Computer News*, 2009.
[3] Waterman, S., "Analysis: A New USAF Cyber-war Doctrine," UPI.com, 2007.
[4] "Information Operations," Joint Publication 3-13, Joint Chiefs of Staff, February 2006.
[5] "Electronic Warfare," Joint Publication 3-13.1, Joint Chiefs of Staff, January 2007.
[6] DOD Directive O-3600.01, Information Operations (IO), 14 August 2006.
[7] Arquilla, J. and D. Ronfeldt, "Emergent Modes of Conflict," *Cyberwar is Coming*, The RAND Corporation, 1992.
[8] US Air Force, "Bold Stroke" Executive Software Course.
[9] "Department of Defense Dictionary of Military and Associated Terms," Joint Chiefs of Staff, Joint Publication 1-02, April 2001.
[10] "CERT Statistics," Carnegie Mellon Software Engineering Institute, http://www.cert.org/stats/cert_stats.html, (accessed March 2010).
[11] "National Military Strategy for Cyberspace Operations," Chairman of the Joint Chiefs of Staff, November 2006.
[12] Dobitz, K., B. Haas, M. Holtje, A. Jokerst, G. Ochsner, and S. Silva, "The Characterization and Measurement of Cyber Warfare," USSTRATCOM Global Innovation and Strategy Center, May 2008.
[13] Lemos, R., "DoD Confirms Hacker Boast," ZDNN, 1998, http://www.zdnet.com/zdnn/content/zdnn/0421/309056.html
[14] Vatis, M.A., "Cybercrime, Transnational Crime, and Intellectual Property Theft," Statement for the record before the Congressional Joint Economic Committee, 1998.
[15] O'Hara, T.F., "Cyber Warfare/Cyber Terrorism," US Army War College, May 2004.
[16] Joint Publication (JP) 3-13, Joint Doctrine for Information Operations, 13 February 2006.
[17] Joint Publication (JP) 3-13.1, Joint Doctrine for Command and Control Warfare, 7 February 1996.
[18] DOD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, 27 February 1998.
[19] Trimble, S., "Seamless airborne networks are becoming a reality thanks to bridging technology," Jane's Defence Weekly, 2007. http://integrator.hanscom.af.mil/2007/January/01252007/01252007-15.htm

Comment on this article, email: wstiac@alionscience.com

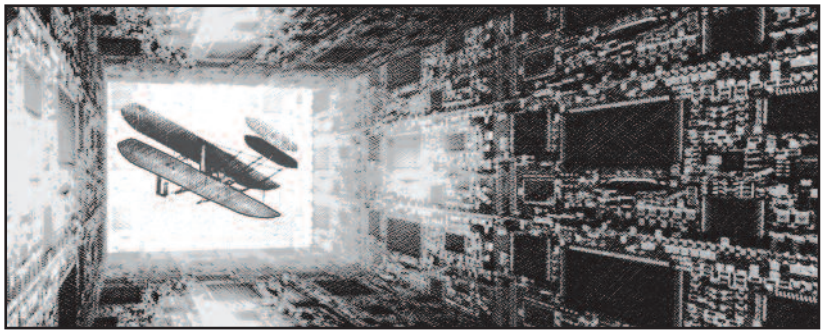
Lionel D. Alford, Jr. is an independent design engineer, program manager, and experimental test pilot currently working with and consulting for Defense Research Associates, Flint Hills Solutions, EG&G, AirLaunch Systems, the University of Dayton Technical Institute, and the University of Dayton. He has designed five Uninhabited Aerial Vehicles and holds a patent for the Capped Helix Winglet (CHeW). Mr. Alford is a retired US Air Force Lieutenant Colonel and an experimental test pilot with over 6300 hours in more than 60 different kinds of aircraft. He is an active member of the Society of Experimental Test Pilots and Daedalians. During his Air Force career, Mr. Alford served in four operational Air Force combat squadrons and led missions in North America, South America, Asia, Europe and Central America. He is a prolific writer and a dynamic speaker who has published and presented over 40 papers and articles in international forums and journals. He is the author of three historical fiction novels, *Centurion* 2008, *Aegypt* 2008, and *The Second Mission*, 2003, and three science fiction novels, *The End of Honor*, *The Fox's Honor*, and *A Season of Honor*, published as a series in 2008. Mr. Alford writes "Military Aviation Adventures" and an aviation blog for www.WingsoverKansas.com.

Cyber This, Cyber That . . . So What?

Major Eric D. Trias
Captain Bryan M. Bell
US Air Force

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.* 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 tothe joint fight.[1] 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.



You have to know the past to understand the present.
—Carl Sagan

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 1). 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.[2] 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."[3] 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.[2] "They are not necessarily unique to the Air Force... but together they do represent" how the service fulfills its assigned missions.[2] 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.[4] As illustrated by Colonel 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–

This article is reprinted in part from Air & Space Power Journal, *Vol. XXIV, No. 1, Spring 2010. The full article is available at http://www.airpower.au.af.mil.*

Table 1. Air Force air, space, and cyberspace functions.[2]

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

information gathering, decision making, and communication (e.g., bombing Iraq's communications infrastructure during Operation Desert Storm, as shown on Cable News Network).[5]

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."[6] 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.[7] 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.[8]

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.[2] 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.[9] 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.[9] 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."[2]

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."[10] 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.[11] 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 cyberenabled 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*, 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.† 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.** "In Operation ALLIED FORCE... multiservice 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."[12] 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 counter information 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 counter information activities such as information assurance and operational security protocols are already in place at all Air Force installations, some in noncyber form.

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.[2] 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).[13] 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.[14] CSAR is the method that the Air Force uses to support joint personnel recovery in "uncertain, denied, or hostile environments."[15] Personnel recovery operations are essential to sustaining unit morale, preserving critical combat resources, and preventing the enemy from gaining intelligence.[2] 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."[13]

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. Netcentric 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 counterdomain 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."[16] Air and space superiority is characterized by freedom of action and simultaneous freedom from attack. Freedom of action is a characteristic of cyberspace 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). General 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."[17] We can be certain that cyberspace will remain a contested environment, but this should not constrain our ability to operate within the domain.

continued on page 14

WSTIAC
Weapon Systems Technology Information Analysis Center

Technical Expertise to Advance Your Mission

Train With Our Experts

- Improvised Explosive Devices (IEDs)
- Rocket-Propelled Grenades (RPGs)
- Smart/Precision Weapons
- Weaponeering
- Performance Based Logistics (PBL)
- Systems Engineering
- Supply Chain Design

What We Offer

- Onsite Training
- Custom Course Development
- Open Registration
- Tailored Content

About Our Training

Our program is designed to give you a professional foundation in weapons technologies. Courses are designed as two and three day intense sessions and are the perfect fit for hectic schedules. For current course offerings and pricing visit our website.

Advance Your Knowledge

Visit http://wstiac.alionscience.com/training or call us at 315.339.7135

WSTIAC
Weapon Systems Technology Information Analysis Center

Technical Expertise to Advance Your Mission

Today's warfighters depend on technology as never before.

Technical Inquiry Service

Funded by DoD, WSTIAC provides a technical inquiry service to answer your weapon systems technology questions.

Free Research Fast Answers

Start benefiting from:

- **FOUR FREE HOURS** for each inquiry
- **Experts** ready to answer your questions quickly
- Access to multiple **databases** and resources
- **Library** containing over 100,000 publications
- We'll help jump-start or **support** your project

Meet your research needs and your deadline.

What is the inquiry service?
Who is eligible?
How are answers obtained?

Advance Your Research

visit http://wstiac.alionscience.com/experts or call us toll-free at 877.978.8737

Flexible Contract Vehicle

- Already competed, single award, task order contract vehicle
- Weapon systems technology scope
- Avoid common procurement costs and time
- Competitive rates
- Easy funds transmittal (MIPR, IAA, etc.)

WSTIAC is an already competed, delivery order contract that can get your requirements on contract quickly, and it does not require your common procurement costs. The comprehensive scope of WSTIAC gives us the flexibility to handle your weapon systems needs with competitive costs and shorter lead time schedules – and – access to data and subject matter experts that can save additional time and money.

Advance Your Project

visit http://wstiac.alionscience.com/getoncontract

To learn how WSTIAC can work for you, please contact:

Steve Ashford
Deputy Director
703.259.5238
sashford@alionscience.com

Bernard Radigan
Contracts Facilitator
315.339.7059
bradigan@alionscience.com

or visit http://wstiac.alionscience.com/getoncontract

continued from page 9

As a function, countercyberspace is comprised of various types of cyber and noncyber-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, President 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.[18] 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.[18]

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.[18]

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.[18] To attain cyberspace superiority, we must execute successful offensive, defensive, and maintenance 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.[16] 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 *manmade* 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.[6] 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.‡ 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."[1] 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."[3]

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 & REFERENCES

* "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]).

† 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.

** "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,* Vol. 31, No. 9, September 2008.

‡ 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.

[1] Wynne, M.W., "Flying and Fighting in Cyberspace," *Air and Space Power Journal,* Vol. 21, No. 1, Spring 2007, http://www.airpower.au.af.mil/airchronicles/apj/apj07/spr07/spr07.pdf (accessed 8 December 2009).

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

[3] Lonsdale, D.J., "The Impact of Cyberspace on Strategy," *High Frontier,*

Vol. 5, No. 3, May 2009, http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf (accessed 8 December 2009).
[4] "AFDD 2-1.2," *Strategic Attack*, 12 June 2007, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_1_2.pdf (accessed 8 December 2009).
[5] Warden, J.A., *The Air Campaign: Planning for Combat*, National Defense University Press, 1988, http://www.au.af.mil/au/awc/awcgate/warden/warden-all.htm (accessed 8 December 2009).
[6] Kuehl, D., "From Cyberspace to Cyberpower: Defining the Problem," *Cyberpower and National Security*, Potomac Books, 2009.
[7] Zetter, K., "Simulated Cyberattack Shows Hackers Blasting Away at the Power Grid," *Wired*, 26 September 2007, http://www.wired.com/threatlevel/2007/09/simulated-cyber/ (accessed 8 December 2009).
[8] Krebs, B., "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *Washington Post*, 16 October 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forus_f.html (accessed 8 December 2009).
[9] "AFDD 2-1.1," *Counterair Operations,* 1 October 2008, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_1_1.pdf (accessed 8 December 2009).
[10] *Quadrennial Roles and Missions Review Report*, Department of Defense, January 2009, http://purl.access.gpo.gov/GPO/LPS108437 (accessed 8 December 2009).
[11] "Hacker Forces 1,500 Pentagon Computers Offline," Associated Press, 21 June 2007, http://www.msnbc.msn.com/id/19358920/ (accessed 15 August 2009).
[12] "AFDD 2-5," *Information Operations*, 11 January 2005, http://www.carlisle.army.mil/DIME/documents/afdd2-5InformationOperations.pdf (accessed 8 December 2009).
[13] "AFDD 2-1," *Air Warfare*, January 2003, http://www.dtic.mil/doctrine/jel/service-pubs/afd2_1.pdf (accessed 8 December 2009).
[14] "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).
[15] "AFDD 2-1.6," *Personnel Recovery Operations*, 1 June 2005, http://www.e-publishing.af.mil/shared/media/epubs/AFDD2-1.6.pdf (accessed 15 December 2009).
[16] AFDD 2-11, "Cyberspace Operations," draft, 4 February 2008.
[17] Chilton, K.P. "Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities," *Air and Space Power Journal,* Vol. 23, No. 3, Fall 2009, 10, http://www.airpower.au.af.mil/airchronicles/apj/apj09/fal09/fal09.pdf (accessed 8 December 2009).
[18] Harris, S., "The Cyberwar Plan," National Journal Magazine, 14 November 2009.

Comment on this article, email: wstiac@alionscience.com

Major Eric D. 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.

Captain Bryan M. 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.

WSTIAC Directory

WSTIAC Director
John L. Weed
100 Valley Road, Ste 102
Mount Arlington, NJ 07856
973.770.0123; Fax: 973.770.1808
Email: jweed@alionscience.com

WSTIAC Deputy Director
Stephen E. Ashford
50 West Corp Center
3975 Fair Ridge Drive, Ste 320 South
Fairfax, VA 22033
703.259.5238
Email: sashford@alionscience.com

Defense Technical Information Center
Attn: IAC Program Office (DTIC-I)
8725 John J. Kingman Road, Ste 0944
Fort Belvoir, VA 22060-6218
703.767.9120; Fax: 703.767.9119
Email: iac@dtic.mil
URL: http://iac.dtic.mil/

Technical Inquiries
Robert Fitzgibbon
Bruce Dudley
201 Mill Street
Rome, NY 13440
877.WST.USER; Fax: 315.339.7002
Email: wstiac@alionscience.com

Training Course Coordinator
Mary Priore
201 Mill Street
Rome, NY 13440
315.339.7135; Fax: 315.339.7002
Email: mpriore@alionscience.com

http://wstiac.alionscience.com/quarterly

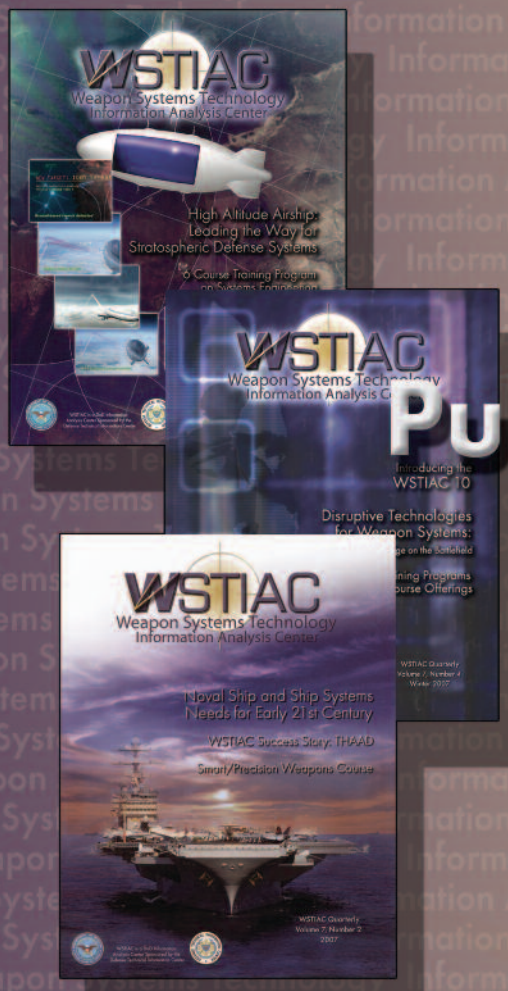
WSTIAC
Weapon Systems Technology
Information Analysis Center
1901 N Beauregard Street, Suite 400
Alexandria, VA 22311-1705

Prsrt Std
US Postage
Paid
Utica, NY
Permit No. 566

Please update...
and verify your subscription information at: **http://wstiac.alionscience.com/certify**

Inquiry Line/Ask the Experts
877.WST.USER

Free Subscription
http://wstiac.alionscience.com/subscribe



WSTIAC Quarterly

Publish Your Work

Increase Visibility
Reach more than 18,000

Transfer Technology
Higher ROI to DoD

Increase Access
Articles preserved on our website
for future researchers

http://wstiac.alionscience.com/authors
email: wstiac@alionscience.com