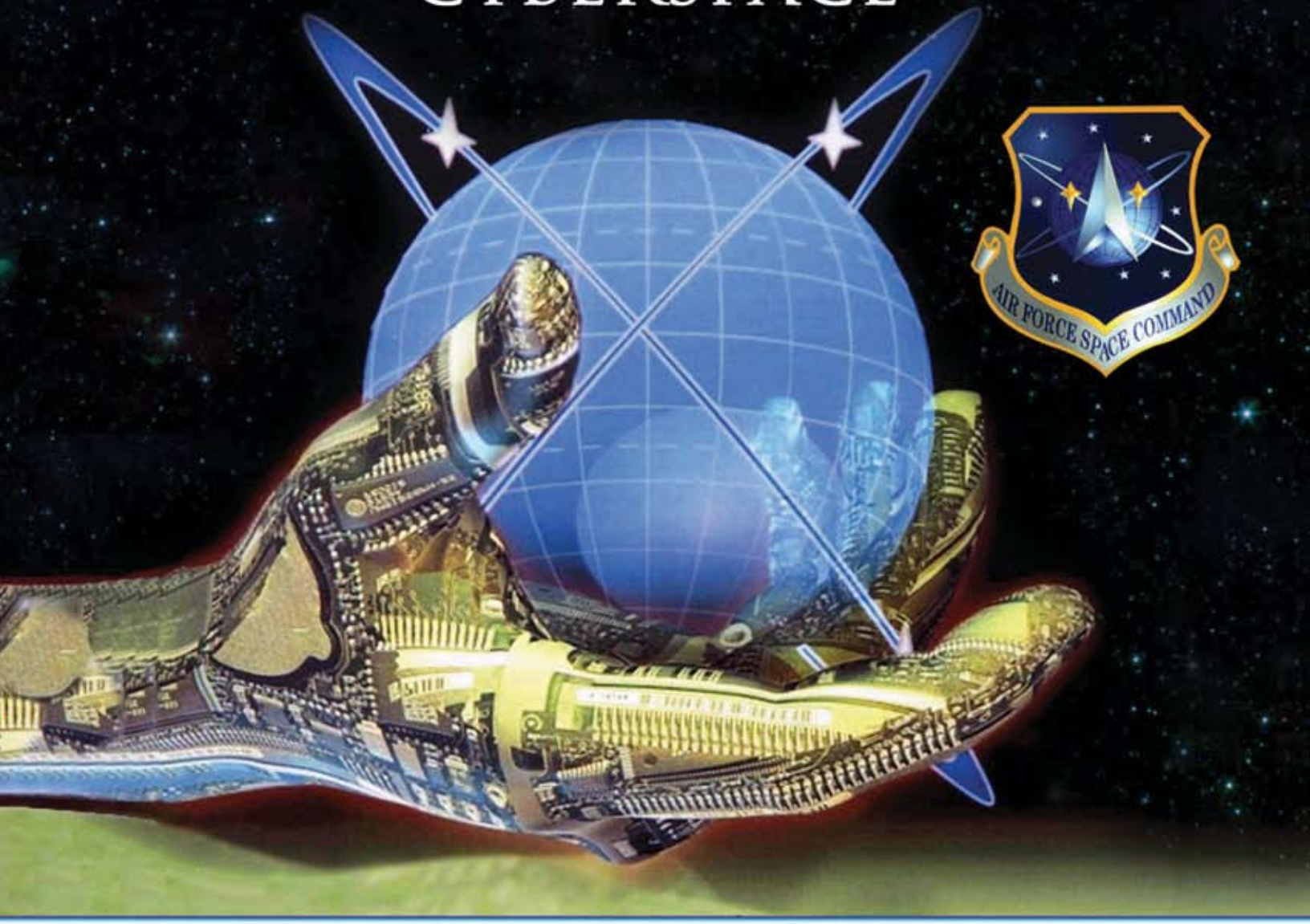
AIR FORCE SPACE COMMAND

Volume 5, Number 3

HIGH FRONTIER

THE JOURNAL FOR SPACE & MISSILE PROFESSIONALS

CYBERSPACE



INSIDE:

Published by a private firm in no way connected with the US Air Force, under exclusive written contract with Air Force Space Command. This command funded Air Force journal is an authorized publication for members of the United States military Services. The views and opinions expressed in this journal are those of the authors alone and do not necessarily reflect those of the United States Department of Defense, the United States Air Force, or any other government agency.

Editorial content is edited, prepared, and provided by the *High Frontier* staff. All photographs are Air Force photographs unless otherwise indicated.

High Frontier, Air Force Space Command's space professional journal, is published quarterly. The journal provides a scholarly forum for professionals to exchange knowledge and ideas on space-related issues throughout the space community. The journal focuses primarily on Air Force and Department of Defense space programs; however, the *High Frontier* staff welcomes submissions from within the space community. Comments, inquiries, and article submissions should be sent to AFSPC.PAI@peterson.af.mil. They can also be mailed to:

AFSPC/PA
150 Vandenberg St. Ste 1105
Peterson AFB, CO 80914
Telephone: (719) 554-3731
Fax: (719) 554-6013

For more information on space professional development please visit:
http://www.afspc.af.mil

To subscribe:
Hard copy: nsage@colsa.com
Digital copy: http://www.af.mil/subscribe

Cover: The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests—to fly and fight in air, space, and cyberspace.
Back Cover: Cyberspace. STK graphic courtesy of Analytical Graphics, Inc.

HIGH FRONTIER

The Journal for Space & Missile Professionals

May 2009 Volume 5, Number 3

Contents

Next Issue: ***Schriever V***

Introduction

General C. Robert Kehler
Commander, Air Force Space Command

"Cybersecurity is among the most serious economic and national security challenges we will face in the twenty-first century."
~ Center for Strategic and International Studies Commission

A medium encompassing the entire Global Information Grid, the cyberspace domain is interwoven throughout the physical warfighting domains and embedded in all aspects of military operations. Service members in-garrison and deployed world-wide depend on accurate and reliable information bundled and routed real-time across cyberspace to accomplish a range of missions. In the same vein, our warfighters and national leaders increasingly rely upon space-based systems to deliver data, voice, and video; position, navigation, and timing; missile warning and intelligence, surveillance, and reconnaissance; and a myriad of other information through cyberspace. Fully realizing the synergy between the space and cyberspace domains, in October 2008 Air Force leaders decided to align lead cyberspace responsibilities and stand-up a new cyberspace operational numbered Air Force (NAF) under Air Force Space Command (AFSPC). The integration of these domains allows our service to capitalize on inherent synergies found in space and cyberspace architectures, processes, skill sets and training. This quarter's *High Frontier* compiles perspectives from preeminent thinkers across the government, industry, and academia regarding potential challenges, impacts, and initiatives for consideration as we come to grips with cyberspace.

The first of four articles in the "Senior Leader Perspective" section begins with Maj Gen William Lord, commander, Air Force Cyberspace Command (Provisional), as he elaborates on AFSPC's lead role for cyberspace operations. While providing focused leadership and building on the synergies between these domains, he describes the effort and challenges in consolidating existing Air Force cyberspace organizations under 24th Air Force, the operational NAF which will present cyberspace forces to the commander, United States Strategic Command.

Next, VADM Nancy Brown, director of the Command and Control Directorate, Joint Staff, provides insight into the paradigm shift which considers the information realm as a central component of the way we fight wars as opposed to a support structure adjunct to our warfighters. Maj Gen John Maluda, director, Cyberspace Transformation and Strategy Office of Warfighting Integration and chief information officer, reflects on recent cyberspace developments. The "Senior Leader Perspective" concludes with Dr. Kamal Jabbour's discussion on the science and technology of cyberspace operations.

Progressing through this quarter's volume, we provide five articles in the "Cyberspace" section. Dr. Martin Libicki scopes the possibilities and limits of deterrence in cyberspace. Next, Dr. David Lonsdale expounds upon cyberspace's influence and impacts on strategy. Third, Mr. Timothy Thomas summarizes the views of Taiwanese specialists who focus on Chinese information warfare tactics, organization, and policy. In addition, Mr. John Vona explains the importance of seamless command and control and integration of our capabilities across geographical and organizational boundaries. The fifth and final article in the "Cyberspace" section is authored by Lt Col Patrick Clowney. He describes the "beautiful marriage" between Clausewitz and network centric warfare.

In the "Industry Perspective" section, Ms. Linda Gooden of Lockheed Martin addresses the need to protect what is considered by many to be our most powerful weapon system—information. Recognizing the escalating threat to military, civil, and commercial customers in cyberspace, Ms. Gooden socializes an initiative to return the advantage in the cyber security race to the defenders rather than the attackers.

Under the "AFSPC's Year of Leadership" section, CMSgt Richard Small, our command chief, outlines activities over the course of 2009 to improve our leadership focus and enhance skills for interacting with those we lead.

New to the *High Frontier* is the "Historical Perspective" section. Dr. Rick Sturdevant shares an entertaining view on the origin of the word "cyberspace" stemming from both the scientific work of decades past in cybernetics and the creative minds of prize-winning science fiction novelists.

We conclude this quarter's volume with a book review by Muhammad "Mac" Sharif Elatab, a Dartmouth College student, on Dr. Martin Libicki's *Conquest in Cyberspace*.

We hope you find this edition of the *High Frontier* stimulating and educational and come to realize both the importance and complexity of the cyberspace mission. Our next issue will focus on "Schriever V," our Title 10 wargame which seeks to advance issues related to space-based operations, space protection, space-related policy, as well as various partnerships and agency cooperation. We have invited a number of key Schriever V participants to submit articles on their findings and proposed solutions.

General C. Robert "Bob" Kehler (BS, Education, Pennsylvania State University; MS, Public Administration, University of Oklahoma; MA, National Security and Strategic Studies, Naval War College, Newport, Rhode Island) is commander, Air Force Space Command (AFSPC), Peterson AFB, Colorado. He is responsible for the development, acquisition, and operation of the Air Force's space and missile systems. The general oversees a global network of satellite command and control, communications, missile warning and launch facilities, and ensures the combat readiness of America's intercontinental ballistic missile force. He leads more than 39,700 space professionals who provide combat forces and capabilities to North American Aerospace Defense Command and US Strategic Command (USSTRATCOM). General Kehler will assume cyberspace responsibilities as directed by CORONA Fall.

General Kehler has commanded at the squadron, group, and twice at the wing level, and has a broad range of operational and command tours in ICBM operations, space launch, space operations, missile warning, and space control. The general has served on the AFSPC Staff, Air Staff, and Joint Staff and served as the director of the National Security Space Office. Prior to assuming his current position, General Kehler was the deputy commander, USSTRATCOM, where he helped provide the president and secretary of defense with a broad range of strategic capabilities and options for the joint warfighter through several diverse mission areas, including space operations, integrated missile defense, computer network operations, and global strike.

Cyberspace Operations: Air Force Space Command Takes the Lead

Maj Gen William T. Lord, USAF
Commander
Air Force Cyberspace Command (Provisional)
Barksdale AFB, Louisiana

"The Air Force must provide Joint Combatant Commanders tailored, innovative capabilities to secure freedom to attack and freedom from attack in and through the atmosphere, space and the electromagnetic spectrum."[1]

~ Air Force Chief of Staff General Norton A. Schwartz

In a 15 September 2008 letter to the Air Force, the secretary of the Air Force and the chief of staff of the Air Force stated, "The mission of the United States Air Force is *to fly, fight, and win … in air, space, and cyberspace*." Secretary Michael B. Donley and General Norton A. Schwartz went on to add, "The mission statement conveys our responsibility, along with other services and agencies, to develop capabilities for the warfighting domain of cyberspace."[2]

Armed with this clear mission statement and Air Force senior leadership guidance from the October 2008 CORONA conference, the Air Force Space Command (AFSPC), in concert with Air Force Cyberspace Command (Provisional), is working diligently towards the stand-up of the 24th Air Force (24 AF), a Component Numbered Air Force (C-NAF) under AFSPC organized to conduct cyberspace operations for the Air Force and our joint partners. In addition, AFSPC will assume management headquarters, component major command (MAJCOM), and lead MAJCOM responsibilities for related cyberspace operational and management tasks.[3]

Cyberspace Defined

According to the Joint Publication (JP) 1-02, cyberspace is located within the information environment, defined as "The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information …"[4]

Cyberspace itself is defined in JP 1-02 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."[5]

The Air Force considers cyberspace to be a physical domain, like those of air, land, sea, and space, and therefore subject to all physical laws of nature. In a physical sense, the Air Force considers cyberspace to include things such as the internet (Global Information Grid or GIG), telecommunications networks (combat communications, satellite communications), computer systems, network operations and command and control (e.g., Air Force Network Operations Center, Integrated Network Operations Security Centers), and embedded processors and controllers.[6]

A Contested Domain

"The full spectrum of US military capabilities on land, sea, and air now depend on digital communications and the satellites and data networks that support them."[7]

~ Secretary of Defense Honorable Robert M. Gates

Cyberspace is a contested domain. The Air Force, Department of Defense (DoD), and nation as a whole are vulnerable to threats posed in, through and from cyberspace while at the same time dependent upon free and unfettered access. Examples abound of the hostile use of cyberspace in recent history. The denial-of-service attacks on Estonian commercial and governmental web services in 2007, reports of cyber attacks preceding the August 2008 Russian incursion into Georgia, and the use of cyberspace by terrorists to coordinate the 2008 attacks in Mumbai, India, demonstrate the power, flexibility, and pervasiveness of cyberspace, serve to highlight our poten-

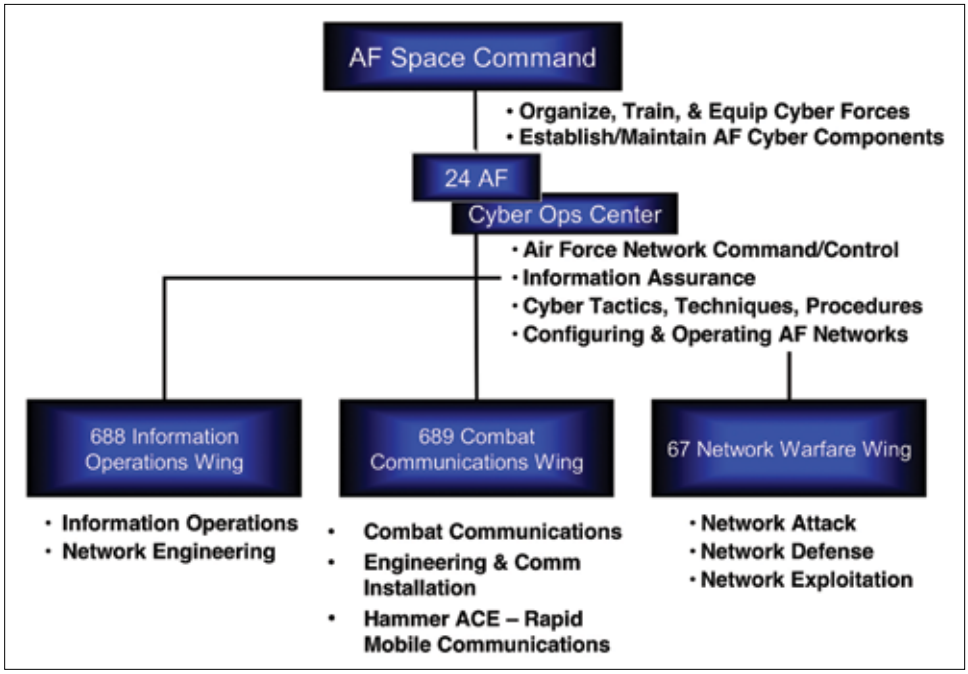


Figure 1. Air Force Space Command's new Twenty-Fourth Air Force.

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

~ Joint Publication 1-02

tial vulnerabilities and show us the nature of the operational environment. Cyber infiltrators routinely attempt to penetrate DoD, government, economic, and industrial networks to gain access to information that could be vital for activities in each of those arenas. The advantages such adversaries gain through cyberspace afford them the ability to pose a serious threat to our homeland.

Cyberspace Operations

Cyberspace Operations are defined in JP 1-02 as "The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the GIG."[8] Armed with these definitions we can draw together our Air Force capabilities in such a way as to foster unity and synergy in our cyberspace efforts.

AFSPC, via the 24 AF, will conduct cyberspace operations for the Air Force and combatant commanders. Twenty-Fourth Air Force will conduct operations primarily as a C-NAF to United States Strategic Command, through its operations center and three assigned/subordinate wings. AFSPC will be the Air Force's focal point for establishing, operating/maintaining, defending, exploiting and attacking in, through, and from cyberspace. Each wing under 24 AF will take on a piece of the cyberspace mission for the Air Force.

As the management headquarters element for Air Force cyberspace operations, AFSPC will be the leader in organizing, training, and equipping Air Force cyberspace forces.

Twenty-Fourth Air Force Mission

The mission of 24 AF will be to deliver cyberspace superiority through persistent and responsive world-class networks and cyber forces. Cyberspace superiority is the critical capability that directly enables all combat air forces ways, means and ends. Twenty-Fourth Air Force will provide combatant commanders with persistent cyber situational awareness in line with national, military, and Air Force objectives. Twenty-Fourth Air Force will also leverage technology to deliver responsive capabilities in, through and from cyberspace to meet new mission requirements in response to adversaries' emerging capabilities. Finally, AFSPC and 24 AF will provide world-class cyber professionals, trained and equipped to meet the challenges of an uncertain future.

Cyberspace Force Development

"People are our most valuable asset. Their talents enable the joint warfighter to gain the utmost advantage in air, space, and cyberspace. Force Development, through experience, education and training, allows us to ensure our Airmen are agile, capable and well-prepared so that they have an absolute advantage when confronting a cyberspace adversary."[9]

~ Lt Gen Richard Y. Newton, USAF, deputy chief of staff, Manpower and Personnel, HQ USAF

No discussion of the critical operations conducted to create effects in, through and from cyberspace would be complete without touching on force development. The Air Force must produce professional Airmen with the ability to establish, control, and leverage the cyberspace domain. As stated in *The Air Force Roadmap for the Development of Cyberspace Professionals*, these Airmen will operate across a broad range of critical infrastructures, warfighting systems, and technologies and employ capabilities from airborne platforms and through space systems, from in-garrison units and from forward deployed units. By necessity and definition, these will be cross-domain professionals since it is they who will establish, control, and achieve effects within a domain upon which all forces rely.[10]

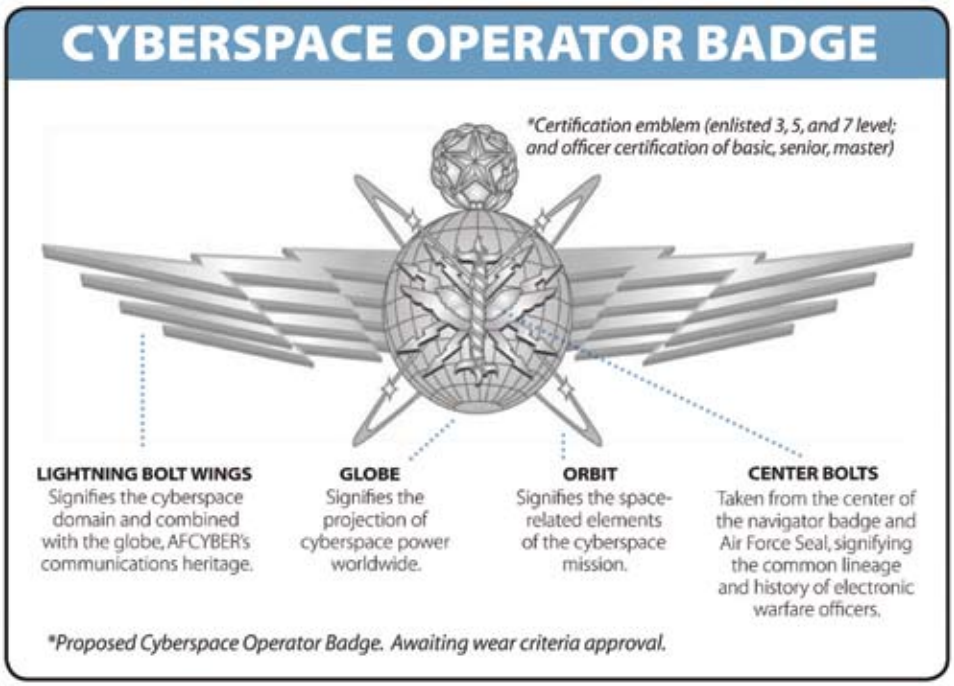


Figure 2. The proposed cyberspace operator badge.

"The bottom line is that we are at war in cyberspace … today … all the time."[11]
~ General Stephen R. Lorenz, commander, Air Education and Training Command

Figure 3. Communication and information specialists like SrA Kenneth Hawkins and A1C Ryan Gall, seen here testing cut field wires for a dial tone in Iraq, will soon see changes to their job requirements as the Air Force proposes 15 new cyberspace career fields.

Cyberspace force development will take its cues from the well established Space Professional Development Program.

Look for new, dedicated Air Force specialty codes designed to capture the core competencies of our varied current cyber-related specialties. A new badge will clearly identify both enlisted and officers with the requisite education and training as being cyberspace professionals, as with our current array of Air Force specialties. In development now are new end-to-end training and education courses for enlisted and officers including rigorous programs as part of professional military education at every level.

Final Thoughts

There are some challenges on the road ahead such as: working through complex legal boundaries between law enforcement, intelligence, and military activities; operational challenges centered on the pace at which cyberspace threats evolve and propagate; and recruiting and retaining a cyberspace savvy workforce when the requisite skills are so marketable in commercial industry. The good news is: (1) there are many dedicated professionals working these issues and, (2) now there is a MAJCOM fully committed to success in this domain. With the support and leverage of the significant experience of our total force partners, we are postured together to meet these challenges and more.

AFSPC is the right command at the right time to shepherd our service's efforts with cyberspace. The Air Force, combatant commands, and nation will make significant strides from the synergies produced by linking cyber and space … a perfect marriage.

Notes:

[1] General Norton A. Schwartz, *CSAF's Vector*, 3 September 2008, http://www.af.mil/library/viewpoints/csaf.asp?id=405.

[2] Secretary of the Air Force and Chief of Staff of the Air Force Letter, *Mission Statement and Priorities*, 15 September 2008, http://www.af.mil/library/viewpoints/jvp.asp?id=401.

[3] HQ USAF Program Action Directive (PAD) 07-08 Change 3, draft, *Phase I of the Implementation of the Secretary of the Air Force Direction to Organize Air Force Cyberspace Forces*, 19 December 2008.

[4] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 as amended through 17 October 2008, 262.

[5] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 141.

[6] PAD 07-08 Change 3, *Phase I of the Implementation*.

[7] Honorable Robert M. Gates, SECDEF, Submitted Statement given to Senate Armed Services Committee, 27 January 2009.

[8] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 141.

[9] HAF/A1 Action Group e-mail, 5 February 2009.

[10] *The Air Force Roadmap for the Development of Cyberspace Professionals,* 2008-2018, 15 April 2008, 7.

[11] General Stephen Lorenz, "General Lorenz on leadership: At war in cyberspace," *Air Force Print News Today*, 23 December 2008, http://www.af.mil/news/story.asp?id=123129337.

Maj Gen William T. Lord (BS, Biological and Life Sciences, USAFA; MBA, Chapman University; MS, National Resource Strategy, Industrial College of the Armed Forces) is commander, Air Force Cyberspace Command (Provisional), Barksdale AFB, Louisiana. He is responsible for establishing cyberspace as a domain in and through which the Air Force flies and fights. In his current duty he is responsible for establishing a new numbered Air Force under Air Force Space Command which will be responsible for the organization, training, and equipping of combat forces to operate in cyberspace.

General Lord is a 1977 graduate of the US Air Force Academy. General Lord has held various positions with tours in Europe, US Central Command and the White House. He has had multiple staff assignments, including two major air commands as director of Communications and Information Systems. General Lord has commanded at the detachment, squadron, group, wing, and joint levels. Prior to his current assignment, General Lord was director, Cyberspace Transformation and Strategy, Secretary of the Air Force Office of Warfighting Integration and chief information officer, the Pentagon, Washington, DC.

General Lord has been awarded the Distinguished Service Medal, Defense Superior Service Medal, Legion of Merit with three oak leaf clusters, Defense Meritorious Service Medal with oak leaf cluster, Meritorious Service Medal with two oak leaf clusters, Air Force Recognition Ribbon with two oak leaf clusters, and the Humanitarian Service Medal. The general is also a graduate of Squadron Officer School, Air Command and Staff College, and the Industrial College of the Armed Forces.

Difficulties Encountered as We Evolve the Cyber Landscape for the Military

VADM Nancy E. Brown, USN
Director Command and Control Directorate
Joint Staff
Pentagon, Washington DC

On 12 May 2008, Deputy Secretary of Defense Gordon England promulgated a memorandum for the military defining "cyberspace" as a "global domain" and specifying it as a "warfighting domain." This paradigm shift, considering the information realm as a central component of the way we fight wars as opposed to a support structure that is adjunct to our warfighters, requires reexamination of the entire cyber domain. This reexamination must stretch from the invisible landscape of social online communities and tools to the hardware on which the cyber world is built.

We will need to examine how we do business today in light of the historical route we have taken to get to this point, and with the understanding that we need to develop our hardware, software, and our processes with the capability to evolve into the systems that we will need to accomplish our tasks not just tomorrow, but in ten or a hundred years. We will have a number of new opportunities, and will face a number of new challenges, but first, we will need to address the challenges of today.

We have evolved the current infrastructure by buying systems to serve a current need at a given time, with the resources that were available and understood by the acquiring authority. We are now facing the immediate challenge of integrating infrastructures developed by individual commands within the services and Department of Defense agencies for the specific purposes of yesterday. We must apply this integrated whole to the problems of today and anticipate tomorrow's problems, while developing an architecture that is secure, accessible, user-friendly, and allows for both business and command and control (C2) uses. While that may seem a monumental task, it must also allow us to interface with other federal, state, and local agencies.

Difficulties of Operations in the Cyber Domain

Historically, any new weapon has been seen as an enabler before it became a true weapon. One of the most classic examples is the longbow in England which was often seen as a "peasant's weapon" until the battle of Agincourt where it proved effective against the French. A more recent example is the airplane which was originally used solely for reconnaissance and is now a powerful weapon of power projection. So too, the cyber battlefield.

Computers have been seen as adjuncts to business processes, enablers for C2, and only recently are beginning to be seen as platforms. Today our networks can be disrupted and our country's infrastructure damaged or compromised by a relatively unsophisticated adversary. While the land, sea, air, and space domains will remain concerns, we currently have good solutions for battles in those domains. Cyberspace is a domain which has yet to be defined. It has been compared to the "Wild West" because of the potential for lawlessness and the lack of control by any civil authority. It is very much within the realm of the possible that the next battle we fight will not be on land, sea, air, or space—but on the networks.

We must learn to fight and defend in this domain because our adversaries have. Otherwise we run the risk of losing a battle without a shot being fired. Naval gunfire has been used to prep the battlefield since the days of sailing ships and the cannon. Recently, prior to the invasion of Georgia, the country saw significant cyber activity. While no loss of C2 systems was published by the Georgian government, it certainly impacted their ability to spread their message, connect with sympathizers, and communicate with their populace. Even prior to that, similar activity was seen in Estonia over the relocation of a Soviet-era World War II memorial in April 2007.

The cyber world is both separate from the domains of sea, air, space, and land, and ubiquitous throughout them. What this means is that cyberspace reaches across services, cultures, nations, and ideologies. While the US is the dominant player in the land domain, unchallenged in the air, and has few near-peers on the oceans, the same is not true in a place where anyone with a computer can make their message heard and a concerted online social group may have a larger following than any elected official.

Online, our adversaries may not always be clear. We will find traditional nation-states, and we will also find transnational groups. Our defense against adversaries in this arena will have to take on an approach different from that in a traditional warfighting domain. This domain permits an adversary's message to span thousands of websites and with the power of blogs, may be repeated tenfold. In addition, we will see "flash mobs" (such as the ones that purportedly attacked Georgia) consisting of people who come together for a short time to achieve a specific purpose and then disperse. We will face additional adversaries whose form and function are not clear yet, and still others for whom the technology has not even been invented.

There are a number of solutions for the problems we face in the cyber world. Not all of them are one-for-one compatible with the physical world. Just as Cyber is a force-multiplier, so too, can it be a problem multiplier. As an example, when we destroy an opponent's anti-aircraft gun, we have limited his ability to fire projectiles at our aircraft. If we destroy an opponent's computer, we have not significantly limited his ability to fire attacks at our network. Similarly, if we note an attack from a particular Internet protocol address, there is a very good chance that the attack is not from that computer, but rather that the computer

has been compromised and the attack is from another source.

Our challenges are numerous and varied. The very architecture of the Internet was based on trust. When a computer announces its address to the Internet, all other computers trust that the computer is telling the truth. If the computer is told to pretend to be a different computer, it will do so and other computers will believe it.

Many of our internal organizations have a "Cold War" mentality when it comes to sharing information. In other words, you have to have a "need to know" before they will give you the information you need. It's done in the name of security, but it reduces the ability of organizations to collaborate and handicaps our ability to make use of the interactive social networking tools through which business is being done these days. Today's environment requires us to adopt an attitude of "requirement to share" vice "need to know." Security is still important, but we must not let our security needs stop us from taking advantage of these new tools. Rather, we must build security into our procedures for accomplishing those tasks. Collaboration and information sharing must be the new model for our military if we are to continue to be successful.

Our mission partners are never the same. From operation to operation, we may be taking unilateral action, partnering with allies, partnering with local forces, or working with other agencies in federal, state, and local governments. Each of these situations requires a non-standardized approach to sharing information. In addition, the solution must be flexible enough to be reconfigured as partners join or depart a coalition activity, and scalable enough to flex with mission requirements.

In the early days, computers were seen as a hindrance to operations since they were large, bulky, and slow. As computers have progressed, they have become a force enabler and a force multiplier. We use computers as indispensable tools with which we develop plans, orchestrate operations and execute C2 of forces. As we move even further forward, we will use them to achieve non-kinetic objectives. They will be used to prep the battlefield, attack opposition networks and communications systems, and create effects. Computers have the potential to be as strong a revolution in military affairs as maneuver warfare in World War II, the machine gun in World War I, and the longbow in the Middle Ages.

Such a change in warfare requires a corresponding change in doctrine, tactics, operations, and strategy. All of us, from the most senior down, must embrace the unlimited potential that exists in this domain and appreciate the far reaching nature of the capabilities available. We can not afford to cede this domain to our adversaries. While many of us are "digital immigrants" we must learn to understand and leverage this new world that has become critical to our national security.

In the diplomatic, information, military, and economic model of national power, the ability to carry out the information portion is dependent on our networks. In cyberspace, our networks are the platform, information, and the payload. Developing the knowledge and skills to operate effectively in this environment is the challenge. Our success will be measured by our ability to achieve and maintain the "information advantage."

Today's Environment

The premise behind joint operations is that they "identify, create and exploit effects."[1] In order to create these combined effects, we need to fight jointly. We need to have the right service capability at the right time to ensure that the various actions in an operation build on each other to achieve a synergistic effect. We must ensure that officers, enlisted, contractors, and so forth, understand how each service approaches a given problem and be able to apply their skills within that problem to fight effectively.

Contrary to this premise however, we are organized vertically. Each service and agency has their own culture and processes which explains how that organization will solve a problem. Each organization has evolved, based upon its successes, to deliver what its culture has defined as the most important part of the battle. The Navy, controls sea lanes and projects power ashore. The Air Force provides strategic bombing and close air support. The Army maneuvers and provides overwhelming force. And within these "cylinders of excellence," each service and agency has become the very best in the world at its priorities. But each service and agency will organize, train, and equip to perform its mission by itself.

No where is this more of a hindrance to mission success than when looking at a joint or coalition network. We have multiple infrastructures that have evolved to solve specific problems in a service specific way, and which may be duplicated by another service or agency to solve the same problem in a different way. The joint task force commander and even the combatant commander are then responsible for integrating these service unique networks. The combatant commander should be thinking about how to use the network to plan, attack, defend, and so forth, not thinking about how to kludge together disparate systems.

The commander is also responsible for integrating the different security postures that each of the services set for their networks. Since the networks must be integrated to collaborate and share information, differing policies restrict the flow of information. These variations insert road blocks and reduce our effectiveness. This is also true with the different ways services operate their networks—from very centralized to completely decentralized. These varying constructs put the warfighter in the seams. To be effective we must reduce these gaps and move toward a seamless environment that enhances information sharing.

For our infrastructure to be effective and efficient, we need to share information across a number of boundaries. We need to share information within our services—something that our current infrastructure has evolved to accomplish. We need to share information across service boundaries—something that our infrastructure is evolving to accomplish, but for which we have a very long road ahead. Joint, however, is no longer good enough. We must be able to operate in a coalition and interagency environment. Allies make our networks more fluid, broader, and they make us more effective in both combat and non-combat operations. Other agencies are part of our own infrastructure, and there are countless examples where we have to work together, from counter-piracy operations through humanitarian assistance

missions, to emergency response missions within our own borders.

Where We Are Going

As long as the requirement for combined effects and therefore joint operations remains; the military needs to procure, educate, and train jointly. In the cyber domain, building that infrastructure means that we have to move away from separate standards, policies, and training to a common framework which removes the barriers of information sharing between services. The Joint Staff has developed this overarching framework: the Global Information Grid (GIG) 2.0.

The GIG must be accessible and secure. To that end, the vision for GIG 2.0 includes "global authentication" which means that no matter where or how a person connects to the network, the network will recognize them and allow them to connect. It includes "access control" which means that the person connecting to the network will have access to all of the information—and only the information—that they should have access to. The GIG also provides "directory services" which means that there is a single log on for all aspects of the GIG, whether attaching via a service network, an agency portal, or a virtual private network. In the end, any authorized user must be able to access appropriate information from anywhere at any time.

The GIG provides "information and services from the edge." This means that the warfighter must have the information needed to make decisions and must have the services to apply capabilities to a given problem. That information must be trustworthy (i.e., the warfighter has to know that it has not been tampered with and that it is an accurate depiction) and available, which means it is accessible when the warfighter needs the information so that they can make a decision and can employ the proper capabilities before the opportunity has passed.

The GIG is made up of every service and agency network, coupled with those networks that are put together by field commanders, and any other network that connects. As the situation currently stands, the combatant commander or joint task force commander is responsible for integrating these diverse networks into a coherent whole that is secure, provides the required information, and can be accessed from anywhere in the area of responsibility. The vision for the GIG takes the service, coalition, combined and interagency networks and makes them seamless so that commanders are not forced to be integrators. We must bring together both the wired and wireless worlds to create the infrastructure to pass information from the edge and to the edge.

In order to make this joint infrastructure work, we will need to develop common policies and standards that apply to every network and device that connects to the GIG. GIG 2.0 must also include the operational strategies, business processes, organizational structures, policies, and culture required to implement and support that environment. We must develop standards that enable services and partners to seamlessly integrate and policies that support C2, defense, access, accreditation, and so forth.

Lastly, GIG 2.0 provides the framework for unity of command. Effective C2 relationships that support unity of command rely on authority, responsibility, and accountability. We must ensure that these elements are included in our development. We must manage and defend the network as well as the information, which means that we must manage resources such as bandwidth allocations and spectrum assignments. Without unity of effort, independent solutions waste resources, and risk success by creating seams.

We have come a long way from the days when each service could carry out its own operations and we could be successful. We have come a long way from joint operations being enough for success. The world is changing and we have to change with it, or we will become irrelevant. Cyber operations may be difficult in view of the culture of yesterday, but we must be able to operate in this domain. As I mentioned earlier, we have to learn to fight and defend in this domain because our adversaries already have. GIG 2.0 represents a fundamental shift in how we fund, build, and operate our networks. The bottom line is that when we talk about GIG 2.0 we are talking about a framework that enables the warfighter to better execute mission requirements. We are providing an enabling capability that affects each Joint Capability Area and warfighting function. Cyber operations are here to stay; they will be fought over the GIG, and GIG 2.0 will ensure our success.

Notes:

[1] Capstone Concept for Joint Operations Version 2.0, August 2005, 14.

VADM Nancy E. Brown (MS, Communications Systems Management, US Naval Postgraduate School; MA, National Security and Strategic Studies, US Naval War College) is the director, Command, Control, Communications and Computer Systems, The Joint Staff. She is the principal advisor to the chairman, Joint Chiefs of Staff on all C4 systems matters within the Department of Defense. Admiral Brown was commissioned through Officer Candidate School in Newport, Rhode Island in June 1974. Her initial assignment was at Naval Communications Station, Norfolk, Virginia serving as communications watch officer, followed by automation officer and personnel officer. She was then assigned to Naval Telecommunications Command in Washington, DC where she served as special projects and manpower requirements officer.

Admiral Brown has served in the Defense Commercial Communications Office at Scott AFB, Illinois; as officer-in-charge of Naval Radio and Receiving Facility Kami Seya, Japan; executive officer at the Naval Communications Station in San Diego, California; commander of Naval Computer and Telecommunications Station Cutler, Downeast, Maine; on the National Security Council staff at the White House; commander of the Naval Computer and Telecommunications Area Master Station Atlantic, Norfolk, Virginia; deputy director, White House Military Office; deputy director and Fleet Liaison, Space, Information Warfare, Command and Control; director of the first Multi-National Force–Iraq C6; the director of the C4 Directorate for both North American Aerospace Defense Command and US Northern Command; and as both vice-director and director of the C4 Directorate of the Joint Staff.

Senior Leader Perspective

On Cyberspace Developments

Maj Gen John W. Maluda, USAF
Director, Cyberspace Transformation and Strategy
Office of Warfighting Integration
and Chief Information Officer
Pentagon, Washington DC

Recent world events in Estonia and Georgia demonstrated how actions in the cyberspace domain can affect national and military objectives. Similarly, the recent lock-down on using portable devices on our own networks impacted our normal routines and operations. In some corners of the Air Force, not having access to portable devices means we have to copy powerpoint slides to a compact disk rather than carry them on a memory stick. However, at the pointy end of operations, the same lock-down denied the only means of data exchange between critical systems needed to protect lives and carry the fight to our adversaries. Clearly, we have a mission imperative to use and defend cyberspace so that we maintain the capability to conduct operations at a time and place of our choosing. This article will highlight the major Air Force efforts to develop the organizational structures and workforce competencies necessary for providing mission-ready personnel capable of operating in cyberspace.

Senior Air Force leadership recognized the need to dominate operations in the cyberspace domain, and they set us on the path toward deliberately developing cyberspace forces and capabilities by adding cyberspace to the Air Force mission statement in late 2005. As a service, we are now charged to "fly, fight, and win" in the "air, space, and cyberspace" domains. Then-Secretary of the Air Force Michael W. Wynne formed the Cyberspace Task Force under the direction of Dr. Lani Kass, and partnering with Lt Gen Robert Elder, 8th Air Force commander, worked to define the scope of what was meant by "cyberspace" and the types of operations executed in or through cyberspace. The task force got us started, and the Air Force has been pressing ahead at full throttle ever since to work through doctrine, definitions, paradigms, and constructs to deliver on senior leadership's vision for cyberspace.

A challenging aspect to operations in the cyberspace domain is that underlying technologies are always changing, and ever-changing technology drives an ever-changing set of capabilities. With the only constant being change, our efforts had to adapt to new ways of describing and implementing our vision for dominating operations in the cyberspace domain. The official joint definitions for cyberspace and cyberspace operations are as follows:

> **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.[1]
>
> **Cyberspace Operations:** The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.[2]

These joint definitions helped to clarify joint discussions on cyberspace, but these definitions were also slightly different than the working definitions the Air Force had been using—adjustments to our planning had to be made.

Factors external to the core cyberspace discussions also influenced Air Force planning. Originally, cyberspace forces were to be consolidated under the Air Force Cyber Major Command (MAJCOM) and be on par with other MAJCOMs like Air Combat Command and Air Force Space Command (AFSPC). But with renewed emphasis on our nuclear enterprise and the recognized synergies between the cyber and space mission areas, we adjusted the plan to stand-up a numbered Air Force (24th Air Force [24 AF]) reporting to AFSPC.

What has not changed is the imperative for the Air Force to provide capabilities to use and defend cyberspace to accomplish missions in and through cyberspace in support of national objectives. Air Force missions in particular rely on global connectivity through cyberspace, whether it be controlling our satellites, commanding and controlling forces from Air Operations Centers, or flying unmanned aerial vehicles from literally half a world away. Without control of cyberspace, we simply cannot achieve the battlefield effects our joint force commanders and national leaders have come to expect.

People have questions about what it means to stand-up a new cyberspace force, but the fact of the matter is we are doing (and have been doing) "cyberspace operations" for some time now; we just have not called it that nor have we necessarily done a great job of deliberately developing capabilities and core competencies for all facets of this new domain. Particularly in the area of network warfare operations, the expertise for these missions has been developed ad hoc from personnel in a number of functional areas, but the missions are being accomplished. As with the air domain, it will take some time to develop the optimum constructs for developing and employing capabilities. It has been said that in the cyberspace domain, we are at about the same stage in development as Wilbur and Orville Wright were when they delivered the first operational Wright Flyer to the Army in 1909. There is much truth in this assessment, but the important thing is to keep making progress.

One way we have made progress is the October 2008 decision to create 24 AF in AFSPC to serve as the warfighting headquarters for cyberspace operations. Creating 24 AF designates a single commander for all facets of cyberspace operations from establishing and sustaining the domain to controlling the infrastructure to leveraging the domain for active defense, attack, and exploitation operations. Having a single commander overseeing these missions is a tremendous advantage over the current organizational structures where these units report through different chains of command. Under direction of a common commander, we can leverage the strengths of network operations units and

network warfare units to close seams in our cyberspace vulnerabilities. It does not do any good to have world-class network warfare forces that can attack and exploit our adversaries in cyberspace only to leave our own infrastructure subject to the exact same vulnerabilities. Uniting the breadth of our cyberspace forces under 24 AF sets the foundation for us to galvanize our posture in cyberspace like never before.

Another advantage of consolidating cyberspace forces under a single numbered Air Force is creating a single face to the joint community for presenting forces to combatant commanders. Cyberspace transcends all of the traditional domains of air, space, land, and sea, forcing the joint community to rely on all services to provide mission-ready forces that can operate in the cyberspace domain. Creating 24 AF postures the Air Force for effective force presentation to the joint fight.

With the operational structure of cyberspace forces relatively settled by the creation of 24 AF, the Air Force can focus on the best way to develop and track personnel to meet the operational needs of 24 AF. As mentioned previously, the Air Force already operates in cyberspace and has a cadre of personnel with outstanding operational expertise. But the cadre we have today evolved from many functional areas to meet pressing needs at the unit level. We lacked a deliberate, systematic way to develop, track, and use this expertise throughout an Airman's career. Because we already have forces being trained for operations in cyberspace, albeit in an ad hoc manner, we used those training forums to begin retooling and restructuring some of our initial skills training courses for officers and enlisted to provide a better foundation for developing cyberspace operations competencies. These courses were developed through tremendous teamwork over the last 18-24 months between the MAJCOMs, career field managers, and operational units who put these skillsets to work and are set to come online over the next 18 months.

Even with new initial skills courses coming on-line, there is still much work to do. Across the spectrum of developing an Airman from accession through retirement, initial skills training is just the first step to develop Airmen for mission success. The cyberspace domain demands the same operational approach to mission accomplishment that is inherent in the air and space domains. Initial qualification training (IQT) and mission qualification training (MQT) are in varying stages of maturity across the spectrum of cyberspace operations. IQT and MQT courses need to be validated by the new operational structure (i.e., 24 AF) and then institutionalized so that all personnel taking on cyberspace operations have been properly trained and certified to perform their assigned missions.

Beyond IQT and MQT, Airmen must be able to pursue professional continuing education (PCE) to develop both operational and technical skills necessary for success at increasingly higher levels of responsibility. A framework for cyberspace PCE has already been proposed, and the Air Force Institute of Technology, in their role as the Cyberspace Technical Center of Excellence, has taken on a leadership role to help define the requirements and methodology for delivering PCE. With 24 AF standing up as the operational leaders in cyberspace operations, they will be integral participants in developing the right mix of skills to be covered in the PCE progression of courses.

While it may seem to some that developing our cyberspace capabilities and competencies has taken a long time to get off the ground, we are on the verge of putting real change into motion with newly designated operational leadership and a bevy of new initial skills training courses. It took over 80 years to go from the first operational Wright Flyer to the integrated air campaign of Desert Storm, but it will not take as long for similar milestones in the cyberspace domain. The Air Force is well postured to bring cyberspace operations into the mainstream of operational planning and deliver on the Air Force's mission to "fly, fight, and win in air, space, and cyberspace."

Notes:

[1] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 17 October 2008, 141, http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

[2] Ibid.

Maj Gen John W. Maluda (BS, Math and Physics, Troy State University; BS, Electrical Engineering, Auburn University; MS, Systems Management, University of Southern California) is director, Cyberspace Transformation and Strategy, Secretary of the Air Force, Office of Warfighting Integration and chief information officer, Pentagon, Washington, DC. He is responsible for establishing cyberspace as a domain in and through which Air Force flies and fights, to deliver sovereign options for defense of the US and its global interests. Additionally, he shapes doctrine, strategy, and policy for communications and information activities and serves as the functional advocate for 30,000 personnel.

General Maluda enlisted in the Air Force in 1973 and received his commission in 1978 as a distinguished graduate of the ROTC program at Troy State University, Alabama. The general's career highlights include serving at three major commands, with unified combatant commands, a defense agency, the White House and the Air Staff.

General Maluda's staff experience includes positions at Headquarters US Air Force, Air Combat Command, US Air Forces in Europe, Air Force Special Operations Command, US Space Command and the White House Communications Agency. He was also the director, Single Integrated Air Picture System Engineering Task Force, and special assistant for Joint Command and Control Matters, Office of the Deputy Chief of Staff for Warfighting Integration at Headquarters US Air Force. He served as director of Communications and Information for Headquarters Special Operations Command, US Air Forces in Europe and Air Combat Command. Before assuming his current position, General Maluda was vice commander, 8th Air Force, Barksdale AFB, Louisiana.

Among his many awards, General Maluda has been awarded Defense Superior Service Medal with two oak leaf clusters, the Legion of Merit with two oak leaf clusters, the Defense Meritorious Service Medal, the Meritorious Service Medal with two oak leaf clusters, the Joint Service Commendation Medal, the Joint Service Achievement Medal, and the Air Force Achievement Medal. He is also a distinguished graduate of Squadron Officer School, as well as a graduate of both Air Command and Staff College and Air War College.

Senior Leader Perspective

The Science and Technology of Cyber Operations

Dr. Kamal Jabbour, ST
Senior Scientist, Information Assurance
Air Force Research Laboratory, Information Directorate
Rome, New York

The Air Force Research Laboratory provides the science and technology (S&T) vision, leadership, and products that enable the United States Air Force (USAF) to accomplish its mission to "fly, fight, and win in air, space, and cyberspace." The dependence on cyberspace of US weapon systems, critical infrastructure, financial institutions, and our way of life creates an imperative to operate freely in this domain. The USAF vision of global vigilance, global reach, and global power depends vitally on the ability to dominate cyberspace through integrated defensive and offensive operations across blue, red, and gray cyber systems, as well as across the global cyberspace commons.

Joint Publication 1-02, Department of Defense (DoD) Dictionary of Military and Associated Terms, 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 *and* **cyberspace operations** as the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

The USAF vision of global vigilance, global reach, and global power across the full spectrum of conflict from peacetime to major combat operations drives the S&T requirements for cyber operations. Figure 1 illustrates the changing requirements for vigilance, reach, and power as tensions escalate towards combat. Within this context, cyber operations provide a necessary enabler for air and space power, while providing an additional domain where the USAF can deliver effects.

The S&T requirements for cyber operations do not focus only on conducting operations in cyberspace, but rather look holistically at the cyber S&T necessary to accomplish the USAF vision of global vigilance, global reach, and global power in all three domains of air, space, and cyberspace.

Cyberspace is viewed first and foremost as a foundational domain that enables US military superiority, and secondarily as another domain where the US can deliver effects.

Through cross-domain dominance, operations in cyberspace can guarantee freedom of maneuver and assure mission essential functions (MEF) in all warfighting domains.

GLOBAL VIGILANCE

Global vigilance is the ability to keep an unblinking eye on any entity—to provide warning on capabilities and intentions, as well as identify needs and opportunities.[1] The primary challenges of global vigilance include maintaining persistent, global, multi-domain situational awareness (SA) and using assured, trusted systems that can avoid a broad spectrum of threats. In turn, global vigilance depends to some extent on elements of global reach to support sensor positioning and forward basing of assets for SA.

We identify (1) SA, (2) assurance and trust, and (3) threat avoidance as the three main capabilities necessary to achieve global vigilance in and through cyberspace.

Situational Awareness

The strategic objective of cyber SA is to provide automated situation assessment and analysis that meet the operational requirements of all areas within the cyber domain—friendly blue networks, traversal gray networks or global commons, and adversary red networks—across the entire spectrum of conflict—from peacetime to major combat operations.

Mission awareness lies at the heart of SA. Understanding the dependence of missions on specific assets, the interdependence of assets and the interdependence of missions drives the requirements for SA.

Mica R. Endsley defines "SA as the **perception** of the elements in the environment within a volume of time and space, the **comprehension** of their meaning, and the **projection** of their status in the near future."[2]

Perception: Perception represents the transformation of a signal into an alert. Significant technical progress on the perception of the elements of an environment appears in intrusion detection systems, vulnerability assessment, network mapping, configuration management, network management, and policy management. The real-time collection and long-term maintenance of meaningful data for blue, gray, and red systems present a fundamental technical challenge for perception.

Aggregation refers to correlation and fusion of raw data into activities of interest based on factual relationships or an implied requirement for additional meaning. The set of activities of interest at any point in time describe the current situation of the environment, and depend highly on the local environment. A technical challenge of aggregation is developing the appropriate situation at the appropriate level for the appropriate operator while maintaining consistency among differing views of similar

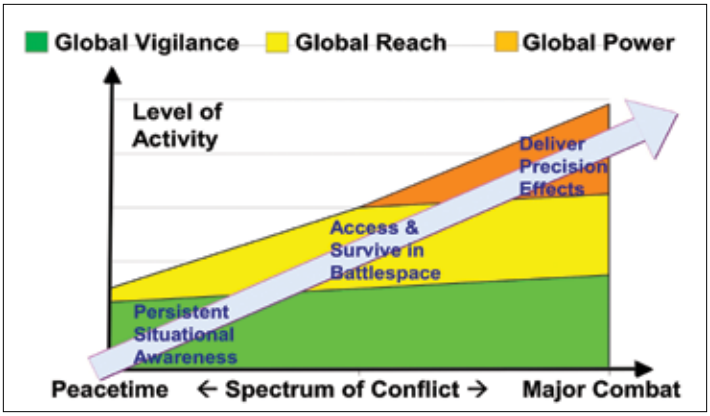


Figure 1. Level of activity across the spectrum of conflict.

situations.

Comprehension: The perception of activities of interest paves the way to their understanding and contextual placement into the environment and the comprehension of their meaning. Comprehension of meaning of a situation through assessment and analysis presents a significant technical challenge and an area of active research. Understanding a situation requires a broad range of analysis and an assessment of the impact of the situation on components, systems and missions.

Comprehension of meaning may require establishing additional relationships between activities of interest. Assessing the impact of an attack on a mission requires both attack activity and an activity that defines the relationship between MEFs and cyber assets that support those functions. The combination of these two activities can lead to deeper understanding of the impact of an attack on missions. Extending this analysis to hypothetical future situations allows reaction planning and response development.

Projection: The projection of status in the near future entails taking the current situation and analyzing plausible threats, opportunities, risks, and possible next steps. The path from the current situation to plausible future situations becomes the basis for developing courses of action (COAs) to move along a probable path and providing input into rules of engagement (ROEs).

The projection of status ranges from analyzing an attack graph to determining the existence of additional attack paths to discovering alternative solutions for fighting through an attack. Across this range of possible actions, the projection of a situation to plausible future situations presents a substantial technical challenge.

Assurance and Trust

Assuring mission and information, and trusting systems and data, provide the foundation for global vigilance across the spectrum of conflict.

Mission Assurance (MA): DoD Directive 3020.40 defines MA as "a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military Strategy."

The principal responsibility of a commander is to assure mission execution in a timely manner. The reliance of MEFs on cyberspace makes cyberspace the target of choice for an adversary who cannot, or chooses not to, face us in conventional battle. To assure these MEFs in a contested cyber domain requires mapping MEF dependence on cyberspace, mission prioritization to ensure continuity of operations, and a comprehensive risk management strategy.

Information Assurance (IA): Joint Publication 3 -13 defines IA as "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation."

Confidentiality seeks to keep secrets secret. Integrity protects information from modification or compromise. Availability ensures that information and systems remain available in a contested cyber environment. Authentication provides a mathematical mechanism for one entity to establish its identity to another entity. Non-repudiation provides attribution of transactions in cyberspace, a potential enabler to both deterrence and friendly-fire avoidance in cyberspace.

Trust: Trusting a system requires trusting its hardware, software, and information. It is necessary to maintain trust in the information that these systems handle, both the integrity of data at rest and data in motion as systems evolve in capability and technology.

Threat Avoidance

Avoiding a threat provides a strategic defensive strategy that can reduce or eliminate the need to fight that threat. We propose a three-pronged approach to cyber threat avoidance. First, we employ deterrence to prevent the initiation of attacks. Second, we seek to make most threats irrelevant by modifying the cyber domain to eliminate vulnerabilities or make them inaccessible. Third, we use real-time agility through anticipation and escape maneuvers to evade the threat.

Deterrence: Effective cyber deterrence requires either a credible threat of retaliation with timely detection and attribution of attacks, or a disincentive by increasing the cost of an attack and lowering its perceived benefits. Deception to influence adversary perception of costs, benefits, and the potential for retaliation also play a role in deterrence.

Effective employment of deterrence presumes a rational adversary to whom the perceptions of cost, benefit, and retaliation can be communicated. Deterrence also requires that the defender possess both the means and the will to retaliate to an attack.

Domain Modification: Modifying the cyberspace domain to eliminate vulnerabilities or make them inaccessible to an adversary provides a viable approach to threat avoidance. Sound hardware and software development practices can eliminate beforehand vulnerabilities by designing them out of a system. Since cyberspace qualifies as a man-made technological domain, we can rewrite the laws that define the domain and modify its behavior to favor protection and defense. The extension, modification, and replacement of protocols, architectures, hardware, and software are imperative to secure critical warfighting systems.

Polymorphic techniques offer a dynamic approach for continual and rapid multidimensional modification of the cyber domain. These modifications can take place many times per second if necessary, by varying protocols at multiple layers to deny an attacker SA and remove the advantages of time and preparation.

Agility: Agility in defense includes establishing indications and warning mechanisms that detect anomalous activities or entities, rapid analysis of the activity to include attribution and geolocation, anticipation of future behaviors and effects, and effective real-time provisioning of defensive measures.

Real-time threat avoidance presents an adversary with an agile moving target through evasion tactics, stealth, detection prevention, and non-identification. Self-aware defenses detect the failure of evasion tactics and confront an emerging threat with active escape tactics. In such instances, SA enables defensive agility via an accurate environmental context.

GLOBAL REACH

Global reach is the ability to move, supply and position assets—with unrivaled velocity and precision anywhere. The

concepts that support global reach in cyberspace include access technologies to position and deploy cyber assets, survival in a contested cyber environment, and cross-domain superiority for command and control of integrated mission execution.

Global reach is enabled through predominantly defensive measures when tension pushes a situation away from peace towards conflict. In turn, these predominantly defensive measures enable the capabilities that support global power in the event of conflict escalation into major combat operations.

Access

In all domains of land, sea, air, space, and cyberspace, access refers to deploying and positioning friendly forces across blue, gray, and red spaces. While traditional domains are fixed in size—the amount of available land, sea, air, and space is essentially constant—the cyberspace domain changes dynamically, and increases indefinitely in size, creating unique technical challenges for the positioning of cyber assets.

Survival

An effective defense-in-depth avoids a large percentage of threats, and defeats those threats that turn into attacks. When an attack evades detection and defeat, and disrupts US systems and networks, the defensive priority turns to survival and mission assurance. In this context, mission assurance seeks to ensure that critical MEFs fight through, and recover from, attacks against the underlying cyber infrastructure.

Survivability represents the quantified ability of a system, subsystem, equipment, process, or procedure to function continually during and after a disturbance. USAF systems carry varying survivability requirements depending on MEF criticality and protection conditions.

Fight Through: Existing approaches to information system security and survivability focus on preventing, detecting, and containing unintentional errors and intentional cyber attacks. The difficulty in automating the determination on whether a disturbance resulted from an error or an attack complicates autonomous recovery.

The concept of collaborative trusted agents that execute faithfully the commander's intent in the face of a dynamic cyber threat improves the potential for surviving and fighting through attacks. Through formal design methods and a self-protection guarantee, a class of general purpose agents can deploy special-purpose payloads to enhance the ability of a system to detect and fight through an attack, and can serve as a central launching point for system recovery.

Recovery describes the ability of a computer system to regain or even exceed its initial operating capability. While continuing MEFs, damaged systems must recover any lost services, components or data. These systems must discover their own vulnerabilities, identify the root cause of errors and attacks, and regenerate themselves with immunity to improve their ability to deliver critical services. Synthetic diversity ensures overall population survivability by removing like vulnerabilities of an otherwise vulnerable monoculture.

Since attacks in cyberspace happen in milliseconds, recovery must be automatic—not requiring human intervention. Automatic recovery requires a rapid understanding of the root cause of a failure or successful cyber attack. This knowledge must translate into the development and delivery of diverse, immune, and functionally equivalent code and components into a vulnerable system to restore it to a trusted state. Automatic recovery reconstitutes the system to its initial operating capability and decreases its vulnerability to similar attacks.

Mission-Aware Systems: The current DoD IA posture relies on solutions that seek to protect information and information systems, rather than the missions that depend on them. USAF systems must control dynamically end-to-end resources to provide mission aware service delivery and IA-enabled MA. These systems must adapt to failures and attacks by reconfiguring resources to provide an acceptable level of service and security. We must design and build systems that fight their way through attacks towards recovery, preserving MEFs while restoring system functionality and trust.

Cross Domain Operations

In Internet terminology, a domain refers to a group of computers or Internet protocol addresses that share higher-order addressing bits or higher-order naming convention. Consequently, computer security terminology calls cross-domain operations those transactions that occur across different classification levels, or across Internet domains at the same classification. In this document, we maintain consistency with the joint definition of domains as they pertain to warfighting domains, and we use the term cross-domain to represent operations across land, sea, air, space, and cyberspace.

The mission of the USAF "to fly, fight, and win ... in air, space, and cyberspace" requires an ability to maneuver through cyberspace as a means to attacking and defending from any domain against another. Effective cross domain operations require realistic modeling, simulation, and war gaming of the integrated effects among multiple domains, integrated planning of effects delivery, and cross-domain command and control.

Modeling, Simulation, and War Gaming: Robust modeling and simulation, and realistic war gaming, permit experimental pre-deployment, prototyping, and evaluation of cross-domain effects. The wartime employment of cross-domain capabilities guarantees robust and agile execution of the commander's intent, while ensuring cyber protection and MA across the command, control, communications, computers, intelligence, surveillance, and reconnaissance enterprise. Air Force warfighting systems rely on cyberspace operations, and these do not occur separately from air and space operations, but as an integrated interdependent operation.

Integrated effects modeling, simulation, and war-gaming must include the integrated delivery of effects from blue and red systems in every domain against red and blue systems in every domain. Integrated effects exercises must provide a realistic environment for cross-domain operations, in which activities in one domain have a direct bearing on activities in another domain.

Integrated Planning: Many parallels exist between operations in the more traditional domains of air and space and in the emerging domain of cyberspace. As we integrate these capabilities, planning requirements for cyber assets mirror those for tra-

ditional intelligence, surveillance and reconnaissance (ISR) and combat assets. The practice of procedural versus positive control over air assets and the time scales of the Air Operations Center do not translate well to cyberspace where decision cycles hover around a fraction of a second. Conversely, placing cyber assets under procedural control requires the incorporation into the operational tempo a set of previously agreed upon rules for a broad range of future scenarios.[3]

Integrated planning must take into consideration the challenges of cyberspace de-confliction, identification of friend or foe (IFF) procedures and the potential of cyber fratricide and cross-domain fratricide. The ability to tag and identify cyber assets and to ascertain continuously their status and integrity create technical challenges unique to cyberspace. In addition, the routine use of the global cyberspace commons necessitates extending IFF technology to individual sessions, transactions and packets.

Cross-Domain Command and Control: Cross-domain superiority enables MEF execution in a contested cyber domain and permits achieving and maintaining freedom of use of air, space, and cyberspace. Cross-domain dominance refers to the freedom to attack and the freedom from attack in and through air, space, and cyberspace. It permits rapid and simultaneous, lethal and nonlethal effects in these three domains to attain strategic, operational, and tactical objectives in all warfighting domains—land, sea, air, space, and cyberspace.[4]

The popular definition of cross-domain dominance suggests a choice among domains to deliver a desired effect against a traditional target. Under this definition, a cyber attack or a kinetic attack can deliver comparable effects against an intelligent target. Similarly, cyber countermeasures can play a cross-domain role in defending intelligent systems against a range of conventional and non-conventional threats.

GLOBAL POWER

Global power is the ability to hold at risk or strike any target, anywhere and project swift, frequently decisive, precise effects. Delivery of global power in any warfighting domain requires command and control of cyberspace, on which modern US military capability depends.

The global projection of cyber power to complement or enable kinetic power creates S&T challenges of developing precise cyber munitions, estimating first-, second-, and higher-order effects, and taking response action to external events.

Delivering Precision Effects

Precision effects are the intended outcomes of offensive operations in any warfighting domain. With conventional kinetic weapons, precision effects became synonymous with low-collateral damage, given the maturity of tools and techniques for measuring the effectiveness of munitions. In measuring the effects of cyber operations, operators rely on intuitive estimates of effectiveness that depend in large part on the experience and expertise of the operator.

Robust Effects: Cyberspace operations can produce strategic, operational, and tactical effects across the entire spectrum of conflict—from peacetime to major combat operations.

Sustained Cyberspace Operations: Second- and higher-order effects of cyberspace operations may extend beyond the immediate effects on a specific system. The complexity of estimating the duration and extent of cyber effects raises technical challenges unique to this domain.

Delivering Cross-Domain Effects: Cyberspace operations can create effects in other domains. The various effects upon adversaries and their systems are often categorized using the D-family of terminology: deter, deny, disrupt, deceive, dissuade, degrade, destroy, and defeat. Cross-domain effects delivery extends beyond the traditional warfighting domains of land, sea, air, space, and cyberspace, and includes the use of cyberspace as an auxiliary to national power to deliver diplomatic, information, military, and economic effects.

Cyber Effects-Based Assessment

Cyber effects-based assessment (EBA) refers to the process that provides the warfighter with measured effects that quantify the outcome of a cyber operation into tactical, operational, and strategic impact. This process must occur in near real-time during the prosecution of a mission by fusing multiple sensors and combining multiple means of measuring effects. This process must determine first-, second-, and higher-order effects that result from the application of cyber power.

Cyber EBA seeks to inform the commander of the mission impact of cyber operations. To this effect, cyber EBA requires a relationship between physical EBA (a router is down) and mission EBA (personnel system disruption). Mission planning geared toward EBA permits adequate pre-positioning of cyber sensors and assets and proper sequencing of operations and events. A distributed cyber sensor network provides a comprehensive multi-dimensional impact assessment capable of identifying and assessing changes to network status, system performance, and adversary behavior.

Effects on Systems: The first-level requirement for cyber EBA is to determine the effects of a cyber operation on a target system. Computers, network infrastructure, intelligent weapon systems, and critical infrastructure provide potential targets, and require specialized methods for assessing effects. Measures of effectiveness (MOE) and associated methods for measuring MOE are necessary to assess accurately the higher-order effects of a cyber operation against a target.

Effects on Users: A second application of cyber EBA includes determining effects on users. Specifically, if the intent of a cyber operation is to influence the thinking and actions of users, ranging in scope from a single user to a society of users, it is essential to develop the capability to assess the impact of cyber activity on behavior. A knowledge-based representation of human, organizational, cultural, and societal structures and behavior aids in this assessment.

Cyber Effects Assessment of Kinetic Operations: A third category of cyber EBA refers to assessing through cyber means the kinetic effects of traditional combat operations. This category includes capabilities for determining changes to network traffic and topologies before and after kinetic attacks to determine primary and secondary effects of kinetic attacks. This category includes also the seamless fusion of cyber ISR with traditional ISR collections.

Response Action

Computer network defense response action (CND-RA) refers to actions taken in cyberspace to defend blue forces against adversary attack. These response actions must take place in real time during the prosecution of a cyber mission.

Although RA focuses primarily on blue response to an asymmetric hostile cyber action that seeks to negate US superiority in a traditional domain, RA must become an integral part of operation planning in coordination with, and in response to, kinetic actions. Together, these active response actions seek to assure mission success in the last mile of force projection in the cyber domain.

Response Action for Attack Containment: Rapid forensics play an integral role in CND-RA by detecting attacks, attributing them to a source, estimating damage and enabling response COA to contain the attack and limit the damage. Additionally, rapid collateral effects estimate and battle damage assessment of contemplated RA permits automating such a response within the ROEs.

Offensive Response Action: A traditional view of cyber operations separates defensive activities from offensive activities. As attacks grow in sophistication and rapid response action requires automating ROEs, technical and legal challenges arise in using offensive operations to defeat an attack.

CONCLUSIONS

This article presented a S&T perspective on cyber operations within the focus necessary to operate in a contested cyber domain and to assure critical military missions in land, sea, air, and space against threats in cyberspace.

We recognize that the USAF depends vitally on cyberspace to achieve its vision of global vigilance, global reach, and global power. Further, the USAF projects global vigilance, global reach, and global power differently at various stages of tension across the spectrum of conflict. Consequently, the dependence of the USAF on cyberspace operations varies with the stage of conflict.

Global vigilance at peacetime requires persistent SA in all domains, mission and information assurance, and threat avoidance through deterrence and technology. Global reach requires access to the battle space, survival, and fighting through cyberspace attacks, and integrated planning of MEFs and their dependence on cyberspace.

Global Power calls for predominantly offensive combat operations, enabled through the delivery of precision effects in cyberspace, reliable effects assessment, and automated response action.

Notes:

[1] General Norton A. Schwartz, "Fly, Fight, and Win," *CSAF's Vector*, September 2008 .

[2] Definition of Situation Awareness as cited in M. R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors* 37, no. 1 (1995): 32-64.

[3] Procedural control - a method of airspace control that relies on a combination of previously agreed and promulgated orders and procedures, Joint Publication (JP) 3-01; Positive control - a method of airspace control that relies on positive identification, tracking, and direction of aircraft within an airspace, conducted with electronic means by an agency having the authority and responsibility therein.

[4] The Air Force Strategic Studies Group at CHECKMATE said "we believe superiority represents freedom to act, but dominance includes the ability to exploit." This implies that dominance exceeds superiority. However, referencing the definition of air superiority from JP 1-02, JP 3-30: "air superiority - that degree of dominance in the air battle of one force over another that permits the conduct of operations by the former and its related land, sea, and air forces at a given time and place without prohibitive interference by the opposing forces" 'superiority' is a degree of 'dominance.' Excerpts from Cross Domain Dominance brief, notes pages, Lt Col Brad "Detroit" Lyons, Lt Col Tim "Dexter" Rapp, Air Force Strategic Studies Group CHECKMATE, 10 June 2008.

Acknowledgement: This article summarizes the Strategic Vision for Cyber Operations Science and Technology developed by the Cyber Operations Innovation Team at the Air Force Research Laboratory Information Directorate in Rome, New York. The innovation team includes Scott Adams, Mark Gorniak, Todd Humiston, Patrick Hurley, Herb Klumpe, Paul Ratazzi, Paul Repak, Brian Sessler, James Sidoran, Jason Siegfried, George Tadda, Walt Tirenin and Thomas Vestal.

Dr. Kamal Jabbour, ST (BE Electrical Engineering with Distinction, American University of Beirut; PhD Electrical Engineering, University of Salford, UK) a member of the scientific and professional cadre of senior executives, is senior scientist for Information Assurance, Information Directorate, Air Force Research Laboratory (AFRL), Rome, New York. He serves as the principal scientific authority and independent researcher in the field of information assurance, including defensive information warfare and offensive information warfare technology. He conceives, plans, and advocates major research and development activities, monitors, and guides the quality of scientific and technical resources, and provides expert technical consultation to other Air Force organizations, Department of Defense, and government agencies, universities, and industry.

Dr. Jabbour began his professional career on the computer engineering faculty at Syracuse University, where he taught and conducted research for two decades, including a three-year term as department chairman. In 1999, he joined the Cyber Operations Branch at AFRL through the Intergovernmental Personnel Act, and transitioned gradually from academia to government.

In response to President Bush's National Strategy to Secure Cyberspace, Dr. Jabbour created the Advanced Course in Engineering (ACE) Cyber Security Boot Camp to develop the best ROTC cadets into future cyber security leaders. The ACE combines advanced academic training, hands-on internships, officer development, and weekly eight-mile runs into a challenging cyber security boot camp. The ACE received designation of a Special Interest Item for its role in developing officers for the new Air Force Cyberspace Command.

Dr. Jabbour has received one US patent, published more than 60 papers in refereed journals and conference proceedings, and supervised 21 theses and dissertations. An avid distance runner, Dr. Jabbour wrote a weekly column on running in the *Syracuse Post-Standard* from 1997 to 2003.

Deterrence in Cyberspace

Dr. Martin C. Libicki
Senior Management Scientist
RAND Corporation
Arlington, Virginia

For most domains, deterrence is like oxygen: little noticed when it is working and painfully obvious when it has failed. Alas, if cyber-deterrence fails and hostile states do bad things in cyberspace, it may not be immediately obvious. Corrupted data often looks like uncorrupted data. Many systems commonly malfunction all by themselves. Error may be obvious only when the system is being relied on to perform in a crisis. Even with evidence of deliberate hostile (*vice* mischievous) tampering, it is unclear who was behind it, what they were trying to achieve, or whether they had something that could be put at risk. Cyber-deterrence suffers, or depending on one's perspective, benefits from a great deal of ambiguity.

To scope the possibilities and limits of deterrence in cyberspace requires several steps. First come some definitions. Second, we make a few critical observations about how cyber-attacks take place. Third, we limn some motives for cyber-attacks. Fourth, we draw some contrasts between nuclear/conventional deterrence and cyber-deterrence.

Definitions

As William Kauffman argued,[1] "Deterrence consists of essentially two basic components: first, the expressed intention to defend a certain interest; secondly, the demonstrated capability actually to achieve the defense of the interest in question, or to inflict such a cost on the attacker that, even if he should be able to gain his end, would not seem worth the effort to him." Although the ability to ward off attack on systems would, in fact, deter someone from attacking them, we intend to use a narrower definition of deterrence: the ability to persuade others not to attack you because their doing so would result in retaliation.[2]

An attack, in turn, is an attempt to get a system to malfunction in ways that reduce its value to the user: for example, the system works more slowly or not at all, or it cannot connect to other systems, or its information and/or algorithms have been corrupted. Examples of what a major cyber-attack might do include shutting down electric power or scrambling bank records. Military effects may include disabling command-and-control systems or making integrated air defense systems fire missiles at ghosts.

Should breaking into a system and copying its files (computer network espionage) be considered an attack? Such an act alters the target computer in the sense of getting it to send information to a place it should not go—but it otherwise does not keep the computer from operating and even generating correct information and commands. Espionage ought not be encouraged even by default, but, historically, the rules of war tended to distinguish conflict from espionage and the latter is not usually considered an actionable legitimate *casus belli*. As a practical matter, one can expect that the intelligence services of every competent state are busy trying to read each others' mail. One must also imagine that the ones you *do not* hear about are doing a better job of it than the ones you do hear about. Thus, evidence that someone has penetrated a network may be a better indicator of their incompetence than malice.

We further assume that cyber-deterrence is retaliation in kind. The reason for this exclusion is not because it makes sense to do so but because it illustrates more of the conundrums of cyber-deterrence.[3] Some of these conundrums apply to retaliating for cyber-attacks by kinetic means; others apply to retaliating for, say, kinetic attacks with cyber means.

Finally, we assume that nothing seriously kinetic is taking place at the time with the putative attacking country. If war is going on, deterrence in cyberspace would be impossible to discuss without reference to how the rest of the conflict is governed.[4]

What Permits Cyber-Attacks

Although cyberspace, like everything else, is rooted in the material world, it is, for all practical purposes, man-made. The cyber world is a virtual medium over which the user has, at least in theory, a great measure of control. A system that is disconnected from the rest of the world's networks and built with trustworthy components, and manned by trustworthy individuals is likely to be quite secure even against the most determined of attacks. These characteristics can or should describe most classified military systems (which is to say, most warfighting equipment).[5] However, many systems *are* connected to the outside world, and so users must devise ways to scrutinize packets that come into it from the outside world so as to block harmful content. This is the case because everything that gets into a system gets in because the system has allowed it to and because the system only does what its designers and operators let it do—thus, in theory there is no forced entry in cyberspace. In practice, of course, bad things do get in all the time. The software that makes systems run is exceedingly complex, often opaque to the user and inevitably imperfect. Even when software is completely transparent (as it is in the open-source world), it is still quite complex. Ensuring that no combination of bytes can cause a system to malfunction is a daunting challenge.

Indeed, complexity is ultimately the primary source of nearly all computer malfunctions, both inadvertent and malevolent.[6] The system viewed by designers may be capable of warding off mischief. But users and systems administrators may carry a completely different and incomplete perspective on the system; the difference between the two can lead to security breaches.[7] Last, there is the actual code, which is the definitive word on

how the system actually reacts to inputs and what it puts out. In any conflict between perception, design, and code, code always has the last word. Divergence between the security model as designed and used, and the security features resident in the code, is the primary source of vulnerabilities. Taking advantage of such vulnerabilities is, in turn, how hackers get systems to do what they want rather than what the designers, administrators, and users think the system should have done.

The fact that almost all attacks come from taking advantage of vulnerabilities has several implications.[8] First, attacks themselves may be self-limiting. Users who are aware that their systems are not working correctly may, with effort, learn why. Knowing why, they may also understand how far to trust their systems, and may even know how to fix the problem or (if the problem is in acquired software) seek help from those who know. If the fix works and the system is cleaned, the attacker has to come up with some other trick to wreak similar harm. Even if the nature of the vulnerability cannot be discerned, the facts are that rarely is physical equipment destroyed and a competent organization should be backing up its data and retaining clean copies of its software. This would mean that almost all of the damage from any attack is temporary.[9] Second, attacks require guile rather than brute force. Persistent rather than desultory attempts to look for vulnerabilities are more likely to find one, but a thousand networked hackers working independently may be just as likely to find a vulnerability as a thousand employees of a state intelligence agency.[10] Third, for this reason, there are essentially no distinguishing physical requisites for launching an attack—and correspondingly, almost nothing of theirs that can be destroyed or disabled in order to prevent an attack from taking place.[11]

Motives for Cyber-Attacks: One is tempted to ascribe secondary status to the divination of motives for attack when considering how to deter them. After all, the message of deterrence in any mode is "Don't—or else!" irrespective of how reasonable or rational the attacker's motives are. Conversely, it is rarely wise to conclude that deterrence is unnecessary because no rational person would see net gains from a particular form of attack.

Nevertheless, some attention to motive is important because it shapes the nature and credibility of the response and suggests how well the fear of failure or the threat of punishment can deter attacks. Essentially, one can divide motives into four categories: errors, coercion, preemption, and spite.

- Errors are many and various: for example, a self-induced system flaw, an attempt to crack a system in order to spy on it but which veers off unexpectedly; a response by the attacker to what it erroneously thought was an earlier strike by the target; and attack that looks as if it came from a state but actually came from unauthorized sources. Understood correctly, errors may not merit retaliation.
- Coercion exists to warn the attacked country to respect the attacker's interests—to act in a certain way. Sometimes an attack is tantamount to a dare; sometimes, the attacker can make the point and stay hidden since its interests may be shared by other state and non-state actors. Here, retaliation sends a warning of its own back.
- Preemption targets national defense/security systems on the hope that a crippled response capability gives freer rein for the attacker to operate in the kinetic domain. If the attacker refrains from follow-on kinetic operations, however, one might guess that the cyber-attacks did not work or that they were not sufficiently coordinated with kinetic options—or else had been mischaracterized by the target. In such circumstances, warding off kinetic threats during the window when cyber systems are malfunctioning is the first priority, retaliation in kind might follow, but later.
- Spite (as a motive) is a way to classify attacks intended to harm the target but without significant benefit to the attacker. Retaliation can be appropriate, but so is figuring out a plausible reason for such an attack in the first place.

Eight Difficulties of Cyber-Deterrence

Deterrence has become so commonplace a notion during the Cold War period (and afterwards) that its pre-requisites are often overlooked. The importance of these pre-requisites, however, returns when the subject of cyber-deterrence is raised.

Do We Have an Actionable Basis for Deterrence?

Returning to the Kaufmann criteria for deterrence, the interests we would defend must have some precision; it will not do for the US government to unilaterally assert the right to police all behaviors in cyberspace. Most would agree that the nation's interests extend beyond its government systems to include critical infrastructures (e.g., banking, electric power). Beyond that, lies foggy terrain. Hostile activity in cyberspace takes place constantly. Hackers vary from the curious and careless, to political demonstrators, cynical businessmen, shysters, criminals, nihilists, and state actors. Only a picayune fraction of such attacks are investigated. Of these, only some can be traced behind the borders of a hostile state and not all of *those* are state-sponsored. So what kind of threshold should make mischief in cyberspace actionable? To avoid retaliation in error and avoid consuming the gross national product in investigating every breach in cyberspace, there probably has to be some discernible difference in magnitude between our threshold for retaliation and the magnitude of damage that might be ascribed to background noise (whose level and composition varies over time). Although most state-created mischief in cyberspace is spying, is spying actionable?[12] Loss of life makes a tractable threshold but we have yet to see the first casualty from hacking; most of the highly interesting targets can crash without people being killed in the process. If some dollar threshold makes an attack actionable, how would it be communicated and how would it be measured to the understanding if not necessary the satisfaction of the attacker who would then face retaliation?

Do We Know Who Did It?

For nuclear and massed conventional attacks the source is usually immediately obvious. This is not true in cyberspace.

Because almost all forms of retaliation require the target have a vulnerability to take advantage of, the ability to predict what retaliation will do depends on one's ability to predict what vulnerabilities the target has.

Even if one could trace back incriminating packets to (the Internet protocol address of) the computer that sent them, one cannot really be sure if the attack is the fault of the computer's owner (it could be an implant that the real attacker placed in someone else's computer and then activated). Even if the attacker *is* the system's owner, one cannot know if such an attack was authorized by the state. Attacks can be launched from literally anywhere (including by trusted insiders) and only states that were truly brazen or feckless would launch an attack from their own networks. Counting on technology to yield attribution forensics is swimming against the tide flowing towards greater digital anonymity.[13] Intelligence on the attacker may help, but starting a war, even one limited to cyberspace, based solely on intelligence has its problems. Otherwise, one will not be able to make reasonable attribution unless the attacker virtually announces its role. Needless to add, without solid attribution, the case for retaliation has to overcome the non-zero probability that one may hit the wrong party back.

It does not help that unlike most forms of combat (but like terrorism) it is not always clear at the outset whether any one cyber-attack is a glitch, a crime or an act of war. If a glitch, its elucidation is the owner's responsibility; if a crime, it is a matter of law enforcement; only if it is an act of war would national security entities (e.g., Department of Defense) get involved. The three communities have quite different standards of evidence and thresholds for proof. The international nature of cyberspace adds further complexity. All this introduces seams in the systems and authorities to detect, classify, and respond to "attacks." Figuring this out, however, and agreeing on an appropriate response may take time, causing a potential hostile actor to time-discount (or to dismiss altogether) the possibility of a punitive retaliatory response.

Can You Deliver on a Response?

Because almost all forms of retaliation require the target have a vulnerability to take advantage of, the ability to predict what retaliation will do depends on one's ability to predict what vulnerabilities the target has.[14] Forecasting is possible but difficult and chancy. One may know about vulnerabilities that remain publicly undisclosed (aka 'zero-day' vulnerabilities) and thus *presumably* undiscovered by the other side.[15] Through assiduous exploration, one might find that key systems of the target are vulnerable in specific ways. Unfortunately, while such knowledge gives one confidence in being able to make some response on any given day, a deterrence posture requires the ability to predict that one can respond as long as the deterrence policy is operative—a period of years or decades. Zero-day vulnerabilities, in general, or specific vulnerabilities, in particular, can be discovered and patched (indeed, they may already be patched unbeknownst to the unwary hacker). The effects of the attack may also be speculative. Many kinetic weapons (e.g., nuclear bombs) tend to work much the same way against any target; a test in Alamogordo (New Mexico) can predict what happens to Hiroshima. Not so for attacks on information systems. Furthermore, a great deal of the damage to any information system is strongly related to how its human operators react: for example, how quickly faults can be found and fixed; how easily damage can be routed around; how frequently the data is backed up; extant contingency plans; or whether customers have a great deal of faith in the systems to begin with. Again, without observing how the other side reacts to an attack, one can only guess at the response. Finally, what puts targets at risk from cyber-attack is precisely the complacency of their owners and the belief that their systems face no serious threats apart from those that have been anticipated and dealt with. Thus they can rely on systems with only nominal fall-back capabilities. Once such targets are put at obvious risk, operators may no longer be so complacent and thus targets may not be so vulnerable. Note a key paradox: the more complacent the target operators are—and hence the more vulnerable they really are—the less likely threats against them will be taken seriously, a *sine qua non* of deterrence.

And Do It Again?

By this point the alert reader can probably guess the answer—not without difficulty (note that people rarely worried about the difficulties of re-establishing nuclear deterrence after a nuclear war). The first time a state retaliates in cyberspace (especially if infrastructure is seriously disrupted or corrupted), the aforementioned complacency will vanish. Targets will become much harder to hit with new attacks.[16] To be sure, the retaliator may have laid in several potential attacks all of which breached defenses while defenders were complacent. However, one can expect that the alert defender will be reviewing existing systems for anomalous behavior and unexplained code and may well unearth follow-up attacks in waiting.[17] Worse, for those wishes to re-establish deterrence, operators may convince themselves that they had installed the necessary fixes and *so this time* their defenses would be adequate and that they therefore have nothing to fear from retaliation.

Can Deterrence Capabilities at Least be Used for Counter-Force Ends?

Counter-force can sometimes have the character of a second prize: we built a capability; it did not deter; we had to use it, but at least, by using it, we reduced the other side's ability to hurt us. No such second-prize exists in cyber-deterrence. Unless the other side foolishly builds its cyber-strike capability on its own network, which can then be disabled, it is nigh-impossible to disable its ability to strike. Cyber-attacks rely on clever hack-

ers, exquisite intelligence, useful tools, and some connectivity to the target—only the latter can be disabled through cyber-attacks. The latter response, disconnection, suggests yet another paradox. To disconnect attackers from the target requires disconnecting the target from the world since the attackers could strike from literally anywhere. So while cyber-warriors have to worry about second-strike capability, such a capability is more surely diminished by the after-effects of their own strikes than by the effects of the adversary's strikes. The contrast with nuclear war needs little elaboration.

Can We Keep the Fight Limited to the Two Contestants?

Deterrence rests on communications, and communications requires enough clarity to separate the consequences of good behavior (being left alone) from the consequences of bad behavior (being hurt).[18] The harder it is to measure causes and consequences, the fainter the message, to the point where every decision is judged not on the response it brings, but on the smaller issue of whether its results (of violence) merit the effort (to generate it). Once third parties, with their various agendas, get into the mix, clarity of message suffers greatly. An act of retaliation that puts a target into play may engender follow-up attacks from third parties. Third parties are less likely than states to have the deep intelligence that allows them to target specific sites, but they may well have clever individuals who can find vulnerabilities. Third party attacks, if nothing else, will make it difficult for the retaliator to signal the target that punishment has ended and the counter has been reset ("We'll stop and see if you've learned your lesson not to do this again.") Conversely, the inability to control escalation does send a message of: "don't start, because no one knows where this will end."

Is Deterrence Sending the Wrong Message to Our Own Side?

Most of the infrastructures that the US public depends on—for example: banking, power, and telecommunications—are privately owned and operated. Making sure that the information systems that run these are safe from disruption and corruption is a responsibility that can only be discharged by system operators. A policy of deterrence puts the focus on the attackers rather than the system owners who failed to meet their public obligations. Although untested in the courts, system owners may be able to shield themselves from lawsuits by arguing that cyber-attacks were acts of war and thus merit *force majeure* protection against third parties—even though there is no such thing as forced entry in cyberspace.[19]

Can One Avoid Escalation?

It is generally believed that a nuclear exchange already puts all parties at the top of the escalation ladder.[20] Not so, of course, for every other form of conflict. Indeed, violence of any form might be considered an escalation from cyber-attacks, however painful. Hence the concern: if one actually responded to a cyber-attack with retaliation in cyberspace in order to indicate great displeasure without losing control over events, can one be confident that the other side feels a similar need for restraint? Russia, for one, has said the reverse: any cyber-attack against it that rises to the strategic level may be responded to with other strategic (hint: nuclear) means.[21] One might argue that the answer to escalation threats is to maintain escalation dominance, but such a posture, while logical, does not completely erase the risks associated with cyber-retaliation, however justified it may seem to be ("seem" whenever there is doubt about who carried out the attack or whether it crossed a reasonable threshold).

Conclusions

Deterrence is tough, and it is even tougher when dealing with the ambiguities of cyberspace. Historically, war can, in large part, be measured in terms of land taken and enemies disarmed. Deterrence, by contrast, works or fails by affecting what others believe. It calls on at least one side to generate rules, communicate them to the adversary, and convince the adversary that you intend to enforce them both positively ("don't, or I'll …") and negatively ("since you didn't, I won't …"). With nuclear deterrence and even predecessors such as the threat of massive air raids, deterrence involved no small element of primitive fear. The threat of retaliation in cyberspace puts no one directly at corporeal risk; the fear factor is muted.

Influencing another's calculus effectively requires a high degree of clarity since one is trying to impart a dual message: bad behavior will be punished and good behavior rewarded (or at least not punished). Ambiguity is noise; noise damages the message. Difficulties in detecting the true damage from, or the perpetrator of a cyberspace attack, do not help. Doubts, on both sides, about whether retaliation will have the right level of effect—enough to be noticed but not so much as to be seen as escalatory—do not help. Uncertainty as to what motive any one attack, and thus what the other side's calculus really is, does not help.

None of this is to say that deterrence, as such, is not a valid concept. It can be. There may be circumstances where some attempt to establish deterrence in cyberspace in hard to avoid, notably where the attacker virtually dares you to strike back. But here the gap between theory and practice is wide and must be carefully bridged: measure twice, cut once.

Notes:

[1] W. W. Kaufmann, *The Evolution of Deterrence 1945-1958*, (Santa Monica, CA: RAND, 1958).

[2] This is not to denigrate the usefulness of deterrence-by-denial. Indeed, implicit in our argument that deterrence-by-punishment is problematic is the conclusion that one must rely on deterrence-by-denial, which, although difficult, is not burdened with the complications and ambiguities of retaliation. Indeed, the two are synergistic. A good defense weeds out minor attacks and thus minor attackers—making it easier to focus on major attacks and, for attribution purposes, major attackers. Conversely, if one would retaliate with confidence, it helps to know that the impact of counter-retaliation (by the original attacker) would be blunted by dint of having good defenses.

[3] Since individuals or groups (e.g., the Russian Business Network) are responsible for almost all of what we define as cyber-attacks, detection and prosecution of individuals rather than states is the primary use of government power in deterring attacks. Sometimes one can deter governments by threatening plausibly to prosecute their employees (e.g., as was done to Libyan agents because of the destruction of the jet over Lockerbie). Re-

taliation-in-kind, rather than something more violent, is also a statement by the retaliator that what happens in cyberspace stays in cyberspace. If the attacker believes as much, the risk of escalation outside cyberspace may be muted, but there is no guarantee that forbearance will be mutual.

[4] The role and effectiveness of cyber deterrence in the context of an ongoing conventional war has many but not all of the same elements present when conflict is confined to cyberspace. The prospect of casualties, for instance, may complicate or even supersede the gain/loss calculus that characterizes the decision to retaliate in cyberspace. If one retaliated against the wartime foe for a cyber-attack carried out by someone else, few tears would be shed.

[5] This is not to minimize assessment issues and risks associated with software and firmware performance validation and security assurance, but this is a complex concern that deserves more attention than we can give it here.

[6] This is less true for insider attacks—such as those facilitated by being able to put hands (literally) on a targeted computer, conniving insiders, or the ability to compromise hardware or software at its source (aka "supply-chain attack"). Insider attacks are insidious but very difficult to create *en masse*.

[7] For example, until recently users probably assumed that thumb drives were passive containers of data. Most personal computers, however, can be programmed to look for boot-up instructions on thumb drives, and some of them are so programmed. Such computers can thus be infected on boot-up by infected thumb drives.

[8] Distributed denial-of-service attacks (or flooding attacks in general) are a primary exception to this rule, since they can cut systems off from the rest of the world without the systems, themselves, being otherwise affected. Uniquely, they do not arise from the target system's vulnerabilities as such, although their effects can be mitigated by more commodious network routing architectures.

[9] In 2007, DHS blew up an electrical generator as part of a simulated cyber-attack (www.cnn.com/2007/US/09/26/power.at.risk/index.html). So, it is possible. Nevertheless, a long-standing tenet in machine control is that no software failure (whether accidental or induced) should lead to hardware failure; see Nancy Leveson, *Safeware: System Safety and Computers* (Reading, MA: Addison-Wesley, 1995).

[10] Brute-force code-breaking with expensive machinery is one part of breaking into a system for which state intelligence agencies do have an edge (even though an RSA encryption code was famously cracked by the volunteer effort of thousands of personal computer owners).

[11] Sometimes, one can interrupt an attack in progress if it is coming from a single source. But foes can use other attack methods that are harder to interrupt: e.g., attacks from coordinated redundant sources, or preprogrammed attacks implanted within the target network and triggered months or years later.

[12] The means by which systems are jimmied in order to let information flow out from them may, it is argued, also make systems heir to commands that can disrupt or corrupt such systems. But taking such activities more seriously than might be warranted by the 'espionage' label does not mean that they are actionable prior to actual harm taking place.

[13] Although the transition to Internet Protocol version 6 (IPv6) should make it easier to trace packets back to their source, the attacking machine can use Wi-Fi to piggyback onto a completely innocent machine, to one that the incriminating packets would be traced to. A sufficiently sophisticated cell-phone/SIM card combination—both purchased anonymously—could also be used to carry out an attack and would be effectively untraceable if used no more than a few times and each call is over before someone can get to the caller.

[14] If the retaliator wants a calibrated response, it also has to know how much collateral damage may come from retaliation. Attacks of all types risk *some* collateral damage. The complex, interconnected nature of cyberspace and the poorly understood interdependence of critical infrastructures suggest that our ability to bound much less estimate collateral damage is highly underdeveloped.

[15] By contrast, the great majority of malware reported in the quasi-technical press (e.g., CNET) exploits vulnerabilities that have been announced and patched but whose patches have not been entirely implemented within the global user base. These days, the really large infections are meant to recruit computers to form networks of zombies (computers under the control of someone else; aka botnets). Such purposes are well satisfied by picking on the most weakly defended computers. Attacking a serious infrastructure measures often means penetrating systems that are or at least should be strongly defended.

[16] A first attack may facilitate a second by getting inside and opening up a back door for further intrusion. Yet, the first attack had better be undetected if its effects are to remain hidden—precisely the kind of retaliatory strike that cannot convey deterrence. Since the most likely effect of a detectable attack is to shut down or isolate the affected network, such an attack is immediately inimical to creating a second attack.

[17] A defender who finds such code may alternatively elect to patch the system, or route around the corrupted code without touching it, thereby leaving the retaliator unjustifiably confident that a second attack is possible.

[18] In classic deterrence theory, this is called positive deterrence or assurance. An adversary is unlikely to be deterred from some action if he's likely to be punished regardless.

[19] A somewhat more legitimate case for shielding system owners from lawsuits may exist if it was government regulation (e.g., mandating open interconnect) that unavoidably exposed system owners to vulnerabilities that they could do nothing about—something hard to prove.

[20] That noted, Herman Kahn's *On Escalation*, New York, Praeger, 1965, identified 29 steps on the nuclear rung (out of 44 total steps, the first 15 being non-nuclear).

[21] How ironic that it is that Russia is the only state that can credibly be accused of having attacked another in cyberspace (perhaps Estonia in 2007, but with more certainty, Georgia in 2008 and Kyrgyzstan in 2009).

Dr. Martin C. Libicki (PhD, U.C. Berkeley, 1978) has been a senior management scientist at RAND since 1998, focusing on the impacts of information technology on domestic and national security. This work is documented in commercially published books, *Conquest in Cyberspace: National Security and Information Warfare*, and *Information Technology Standards: Quest for the Common Byte* as well as in numerous monographs, notably *Cyber-Deterrence and Cyber-War, What is Information Warfare, The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, and *Who Runs What in the Global Information Grid*. He was also the editor of the RAND textbook, *New Challenges New Tools for Defense Decisionmaking*. His most recent assignments were on the subjects of organizing the Air Force for cyber-war, exploiting cell phones in counter-insurgency, developing a post-9/11 information technology strategy for the US Department of Justice, using biometrics for identity management, assessing Defense Advanced Research Projects Agency's Terrorist Information Awareness program, conducting information security analysis for the FBI, and evaluating In-Q-Tel. Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years as a policy analyst for the General Accounting Office's Energy and Minerals Division. He has also received a master's degree in city planning from U.C. Berkeley (1974).

The Impact of Cyberspace on Strategy

Dr. David J. Lonsdale
Lecturer, Strategic Studies
University of Hull
Hull, United Kingdom

As with any environment in warfare, the true significance of cyberspace can only be understood in how it relates to, and affects, strategy. When faced with the latest development in military affairs, the strategic analyst must always pose the question: so what? This article seeks to provide some initial analysis on this very stark, but crucial question in relation to cyberspace. In the first instance the work will define strategy and its complex nature. Particular attention will be given to the multidimensional nature of strategy. Indeed, the dimensions of strategy provide us with a useful conceptual framework, within which we can begin to understand the reach and influence of cyberspace. Of course, what follows can be only a cursory examination of the impact of cyberspace on each of the dimensions of strategy. How each dimension of strategy fares in the cyberspace age deserves detailed analysis. Nonetheless, the breadth of this article will provide an indication of the reach of cyberspace's influence, and therefore will give us an indication of its significance. The article will conclude that 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.[1]

STRATEGY DEFINED

Strategy is best defined as the art of using military force towards the attainment of policy objectives. Although this simple definition identifies the core relationship within strategy (that between policy and military force), it does little to highlight the inherent complexity of the process. The word process is deliberately used to underline the fact that strategy is an active pursuit, both practically and conceptually, within which military force is translated into political effect. The complexity of strategy, which is the result of many factors, can be described in many different ways. One approach may focus attention on the nature of war, whilst another may highlight the paradoxical logic or disharmony among the levels of strategy.[2] One of the most useful and comprehensive discussions on the subject is to be found in Colin S. Gray's work on the dimensions of strategy.[3] Gray has identified 17 dimensions of strategy, and argues that success in strategy requires a level of competence in each of them. The current article will assess how cyberspace affects, or is affected by, each of the 17 dimensions. At the end of the analysis, we should have a fairly good understanding of how significant cyberspace may prove to be in the conduct of strategy.

Gray delineated the 17 dimensions into three categories: people and politics (which includes people, society, culture, politics, and ethics); preparation for war (economics and logistics, organization, military administration, information and intelligence, strategic theory and doctrine, and technology); and war proper (military operations, command, geography, friction, adversary, and time). The following analysis will show that although cyberspace has a place in all of them, its influence is more pronounced in some than in others.

CYBERSPACE AND THE DIMENSIONS OF STRATEGY

People

Gray persuasively argues that 'people matter most' in strategy.[4] From the fact that war comes into existence to serve the interests of human communities, through to the harsh reality of the frontline where human beings do the fighting, strategy is fundamentally a human activity. Will cyberspace in any way alter this basic truth? Since a form of strategic power can be exercised through cyberspace (for example via attacks against information infrastructures), it is plausible that people may become somewhat removed from the physical act of warfare. However, this statement is only valid if so-called 'strategic information warfare' proves to be a war-winning instrument.[5] If information attacks do not prove independently decisive, then more traditional physical forms of force will have to be employed. The 2007 denial of service attacks against Estonia indicate that significant levels of disruption can result from information attacks. However, the rapid recovery of Estonia's information infrastructure suggests that the strategic effects of such an attack may be limited. This argument is strengthened when one conducts an analysis of conventional strategic bombing campaigns. The air campaign analogy is valid since both forms of war share important characteristics. Most importantly, both methods of war seek to undermine the capability and will of the enemy to resist via attacks against perceived centers of gravity. They both rely upon perceived vulnerabilities within industrial or information age societies and economies. Although the air campaigns waged against Germany, Japan, and Iraq (both in 1991 and 2003) made significant contributions to the respective war efforts, they can hardly be described as decisive. Indeed, a number of common obstacles to the campaigns can be detected. Particularly worthy of mention are: operational difficulties, institutional friction, doctrinal limitations, intelligence shortfalls, political restrictions, poor strategy, and enemy resilience.[6] It is highly plausible that information attacks will fail to achieve strategically decisive results for the same reasons as conventional bombing campaigns.

In the final analysis it is hard to deny the fundamental point that human affairs are normally decided on land, where humans live and work. Thus, at some level most strategic issues are decided by 'the man on the scene with a gun.'[7] In which case, people will still be required to face the harsh realities of the

frontline. Nonetheless, operations in cyberspace (including information operations within the battlespace) could make a significant contribution to the war effort, just as air campaigns have.

Society

Modern armed forces are recruited from, and at some level supported by, a society. In turn, society is governed by some form of executive decision making body. The complex set of relationships among society, government, and the armed forces find theoretical form within Clausewitz's remarkable trinity.[8] For our purposes, Clausewitz's most important thought on the subject was his advice to ensure that a balance is established among the different actors and their respective needs within the trinity. Whether such a balance can be maintained, at least to some degree, increasingly depends upon events within cyberspace. As mentioned in the previous section, modern society can be directly attacked through its information infrastructure, thereby potentially striking at its support for a war. In addition, cyberspace can act as the medium through which an enemy can wage a propaganda campaign to undermine relationships within the trinity. However, we must not fall into the trap of technological determinism. Just because the trinity can be targeted through cyberspace, it does not automatically follow that such attacks will translate into strategic effect. Information infrastructures can be defended and governments can use cyberspace for their own propaganda efforts to strengthen the trinity. Within cyberspace, as in the other environments of strategy, relationships among belligerents will be dynamic and somewhat unpredictable.

Politics

Politics is fundamentally about human interaction. Cyberspace in no way changes that fact. Rather, it merely acts as another medium within which those interactions occur. Nonetheless, cyberspace does appear to influence politics in certain ways. Certain actors in both domestic and global politics owe their existence or influence to cyberspace. Certain groups and political movements have achieved a certain degree of power (the ability to influence the behavior of others) thanks mainly to cyberspace.[9] Thus, certain actors now play a role on the strategic stage mainly through the opportunities afforded by cyberspace. This is noteworthy, but not significantly so. The main actors in the global system are still nation states, and their dominance is primarily a result of their military power and the economic resources upon which it is based. In addition, although cyberspace may enable more effective promotion of certain political causes, it does not change the fundamental relationship between politics and military force. Strategy is still strategy in the information age.

Ethics

At some level the behavior of societies engaged in strategy is framed by ethical norms and values. Depending upon the context (especially what is at stake), societies will not tolerate certain actions in the pursuit of policy objectives. Cyberspace acts as a medium through which messages and/or images can be transmitted to play upon these norms and values. The transmission of images from the battlespace clearly has an impact on the societies and polities engaged in strategy. In addition, norms and values can be disseminated via cyberspace. It is tempting to suggest that western liberal norms pertaining to human rights will increasingly dominate the global strategic environment. However, groups that promote especially brutal forms of war (such as certain terrorist organizations) are proving to be adept at spreading their own perspectives on moral values. Thus, it is difficult to predict whose norms and values will achieve primacy. On the issue of ethics, it is also worth noting that certain methods of information attack appear to offer the promise of less lethal forms of war. Thus, from an ethical perspective, cyberspace appears to offer greater flexibility to the strategist. However, this is dependent upon the operational and strategic efficacy of these methods. It is doubtful that information attack will ever prove decisive enough to make war a more humane activity.[10]

Economics and Logistics

Cyberspace appears to offer the promise of more efficient forms of supply and thereby smaller logistic tails. An improved sensor-to-shooter relationship, resulting in a greater chance of assured kill, should reduce logistical requirements for a cyberspace-savvy force. In addition, just-in-time (JIT) logistics should result in more efficient forms of supply. Taken together these developments suggest that cyberspace may produce forms of strategic activity that are less draining economically on the respective societies taking part. Also, forces should have less vulnerable lines of communication. However, cyberspace is not immune from the paradoxical logic of strategy. More efficient forms of warfare and their related logistical elements present new opportunities for enemy counters. JIT logistics may be especially susceptible to disruption precisely because they are so finely balanced. In this sense, the efficiency that makes them so attractive is also their greatest vulnerability. We should also be careful not to assume that attritional forms of warfare have disappeared, in which case large logistical requirements may have a future.

Organization and Military Administration

These two dimensions can be discussed together since they are both affected by cyberspace in similar ways. The process of strategy, and the organizations that conduct that process, may gain certain advantages from the exploitation of cyberspace. In particular, more efficient flows of information provide opportunities for more effective organizational styles and structures. Indeed, quite correctly new organizations and units are being created, such as the 24th Air Force, to rationalize activity in this area and to develop the required expertise. At a structural level, the most prominent organizational change facilitated by cyberspace is the rise of the network.[11] The adoption of network structures offers the promise of more streamlined bureaucracy and the delegation of decision making to those most effectively placed to use it. While these are clear advantages that need to

be exploited, they do little, if anything, to solve the problems associated with the interface of politics and military force. Disjuncture between these two different worlds is more cultural than organizational in nature.

Information and Intelligence

If cyberspace is the medium that underpins much of modern strategy, then information is the key resource. Many of the advantages wrought by cyberspace emanate from the ability to move information around more effectively. Although a total lifting of the fog of war is unlikely, certain forms of uncertainty can be reduced through the application of information age technologies. Thus, some form of information dominance or dominant battlespace knowledge is both desirable and perhaps possible. However, notions that the battle for information will become decisive are overstepping the mark.[12] Many obstacles stand between the exploitation of information and victory. In an age of plentiful information, friction in the form of information overload will be close at hand. And, as the war for Kosovo revealed, cyberspace is just as likely to transmit the enemy's intended acts of deception, as it is to transmit genuine and useful information.[13] Finally, as Gray notes, important though information undoubtedly is, alone it does not destroy a single piece of enemy equipment.[14]

Strategic Theory and Doctrine

The maturation of cyberspace has exerted significant influence over modern doctrine and strategic theory. One only has to read doctrine related to information operations to find evidence of how powerful that influence has become. It is undoubtedly wise, especially in an age of plentiful information, to produce detailed institutional doctrine on the use of information and exploitation of cyberspace. Indeed, Gray persuasively argues that doctrine performs an important role as the nexus between ideas and action.[15] However, it is vital that modern doctrine does not become overly prescriptive, attempts to reinvent the wheel, or produces mantras from fairly empty concepts. For example, effects based operations (EBO) are defined as 'a process for obtaining a desired strategic outcome or effect on the enemy through the synergistic and cumulative application of the full range of military and nonmilitary capabilities at all levels of conflict.'[16] This appears to be a prime example of reinventing the wheel, as the definition just given represents nothing more or less than good strategy. This is not to say that operational concepts such as EBO are empty of value or content. It is merely to note that they represent nothing new in strategy and that they should not be mistaken for a new dawn in strategic performance or understanding. Although new or developing methods of warfare require doctrinal and theoretical development, these 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. An unfounded sense of living through an age of revolutionary change can lead one to discard past traditions and ideas without good cause. In addition, the constant development of new operational concepts can overly complicate strategy, and thereby ride roughshod over Clausewitz's advice concerning the value of simplicity.[17]

Technology

Like the other environments of war, perhaps with the notable exception of land, the strategic utilization of cyberspace requires the development and application of technology. In fact, cyberspace is largely constructed of technology. Thus, a keen appreciation of the place of the technological dimension of strategy is an important consideration in the exploitation of cyberspace. However, the significance of cyberspace does not just relate to the fact that it enables or requires the development of new technologies. One of the main benefits of this developing environment is that it acts as a force multiplier to existing forces. In theory, and often increasingly in practice, the exploitation of cyberspace enables more efficient and precise use of force. Nonetheless, it is worth pointing out that although technology normally represents a vital dimension of strategy, it is only one among 17. Theorists and practitioners alike should resist the temptation to reduce strategic performance down to the technological level.[18]

Military Operations

Gray correctly identifies military operations as one of those dimensions of strategy so obvious that it is often overlooked. Well-versed in the Clausewitzian tradition, Gray is also quick to identify how vital this dimension is: 'Strategy, no matter how apparently brilliant, is moot until somebody does it.'[19] The impact of cyberspace in this dimension is pervasive. There is little a modern, regular force does that does not rely upon cyberspace to some extent. Indeed, it has long been postulated that new operational concepts will be born out of the development of cyberspace. Dominant battlespace knowledge, network-centric warfare, and swarming, to name but three, typify potential cyberspace-enabled forms of warfare. However, important though they may be, it is not clear exactly how new, revolutionary, or realizable these operations will prove to be. At the opening of the Second World War, German blitzkrieg appeared both new and decisive. However, in many important respects, blitzkrieg was an operational level example of a tactic used by Alexander the Great.[20] In addition, the early promise of rapid, maneuver-based victories was eventually countered by the enemy or neutralized by geography. Thus, the Second World War became characterized, at least to some degree, by attritional forms of warfare.[21] Similarly, limited war theory, given operational reality with the most advanced technology of the day, was found wanting in Vietnam against a wily foe and in the face of poor strategy. Context is everything in strategy. Cyberspace may promise much, and therefore deserves study and development. However, those looking for quick and easy victories are likely to be disappointed.

Command

With an enhanced flow and utilization of information, cyberspace can have a significant impact on the way modern command is undertaken. Network command structures may enable even greater, more efficient, delegation of command author-

ity. In so doing, cyberspace may enable the creation of more flexible forms of command and thereby facilitate more agile military operations. In this respect, cyberspace holds the potential to radically alter the structure and process of command. However, cyberspace will make no difference to the cognitive and emotional qualities required for successful command. The Clausewitzian 'military genius,' a template for good command, requires such characteristics as moral courage, an appreciation of the politics/military nexus, and certain intellectual abilities. These, and other attributes are not possessed by many. Therefore, cyberspace is unlikely to represent much more than a fine-tuning of the art of command. As Winston Churchill wrote, '[war's] highest solution must be evolved from the eye and brain and soul of a single man … nothing but genius, the demon in man, can answer the riddles of war.'[22]

Geography

Geography is an interesting dimension of strategy when considering the impact of cyberspace. Cyberspace is largely a new man-made geographic environment where strategy is played-out. The development and maturation of this new environment has strategic implications. However, the existing forms of geography (especially the land environment) represent an abiding background for the conduct of strategy. In some respects, cyberspace appears to diminish the impact or relevance of certain terrains. For example, global positioning system navigation has all but eliminated the chances of getting lost in featureless desert terrain. Some analysts, like Dr. Martin C. Libicki, have even suggested that the coming dominance of information operations will eventually neutralize the significance of physical geography entirely.[23] This is unlikely, in the first instance, because information operations will rarely be decisive. Secondly, as Clausewitz argued (although of course not using such terms as information dominance), even if information dominance coerces one side to capitulate, it is not information dominance per se that acts as the coercive force. Rather, it is the prospect of what would happen if physical battle took place that represents the true coercive element.[24] Finally, it is an inescapable truism that people live on the land and at some point control has to be exerted on the ground.

Nonetheless, the obvious dominance of the land environment does not seriously undermine the significance of cyberspace as a new or developing geography for strategy. Thus, it is important to understand the nature of cyberspace and to train and equip oneself to operate effectively within it. The current article is not the place to undertake a detailed analysis of the nature of cyberspace. The one point that is worth making, and indeed the most significant strategic characteristic of cyberspace, is the fact that command of the environment will be difficult to achieve. Therefore, akin to the air and sea environments, the best one can hope for is to achieve control of a certain aspect of cyberspace for long enough to achieve one's goals.

Friction, Chance, and Uncertainty

Cyberspace has something of a dichotomous relationship with friction. In some important respects the exploitation of cyberspace helps to reduce uncertainty and thereby diminishes an important source of friction. Some form of control of cyberspace enables one to exercise a more efficient sharing of information among friendly forces. Control does, however, have other positive effects. Either by acts of deception, or by interrupting the flow of enemy information, friction for the adversary can be increased. Despite these positive effects, friction is so varied in its causes that it can never be entirely removed. Uncertainty may be reduced, but it can never be eradicated. Although information can be collected and disseminated on a wide range of relevant topics, some knowledge is much more difficult to acquire and quantify. For example, the morale and quality of enemy forces are somewhat intangible factors in warfare. The exploitation of cyberspace also has the potential to create new sources of friction. Most obviously, the increased flow of information can overwhelm intelligence and command processes, leading to information overload. In addition, networks may be attacked and the flow of information disrupted. This could have particularly serious consequences for a force accustomed to an information-rich operating environment. In the final analysis, it is certainly worth exploiting cyberspace in order to help reduce certain causes of friction. However, it must be remembered that friction acts upon cyberspace, just as much as cyberspace acts upon friction.

Adversary

From an internal perspective the process by which military force produces positive political outcomes (strategy) is challenging enough. The task is further complicated by interaction with an intelligent and active foe. And yet, as Gray notes, it is easy to overlook this fundamental dimension when one is lost in the many difficulties associated with producing strategy at home or within an alliance.[25] The significance of the enemy's role is no more simply and effectively expressed than by the Confederate General George Pickett, who, when asked why they had lost the battle of Gettysburg replied, 'I think the Union Army had something to do with it.'[26] As noted in relation to a number of the dimensions already discussed, cyberspace creates a range of opportunities to increase one's chances against the enemy. Either by attacking enemy information systems, or by increasing the efficacy of one's own forces, cyberspace is a significant force multiplier. However, an intelligent and resourceful enemy will soon understand the basis for such an imbalance in capabilities. He can then either operate in a manner that diminishes the significance of one's cyberspace-enhanced force, or he can attack the system and processes upon which one's forces rely. As Gray notes, what works today will not work tomorrow, precisely because it did work today.[27] This does not mean that the advantages to be gained from cyberspace will be quickly negated. It is merely to note that strategy is a competitive and dynamic activity and advantages have to be constantly fought for and maintained.

Time

Although time is essentially a constant, perceptions of it can be manipulated for strategic effect.[28] In one sense, cyberspace

enables one to operate at the speed of electrons. A fairly simple information attack can be completed within the same timeframe it takes an email to reach its destination. Even if we assume that a war will include physical military forces, cyberspace still offers the potential to conclude one's operations more rapidly than in the past. Precision-guided munitions suggest that an air campaign can hit all of its main targets within minutes and well-coordinated networked surface forces should be able to operate with an increased tempo of operations. Therefore, at least in theory, the exploitation of cyberspace brings with it the promise of shorter, more decisive forms of war. However, such possibilities, when added to the social and political impact of images from the battlespace, may produce an intolerance to protracted wars. In such circumstances, the advantages of a protracted war, long recognized by irregular forces, may have even greater potency. Thus, although cyberspace may enable a modern force to compress the time dimension, enemies may be able to counter that, and thereby exploit a new Achilles' heal.

Conclusion

As anticipated at the beginning of this analysis, the influence of cyberspace reaches into all of the dimensions of strategy. This has substantial significance at both theoretical and practical levels. Theoretically, the role of cyberspace must become embedded in our thoughts and thereby be accepted in the same way that we accept the air and space environments for example. In turn, this must be represented in doctrine, so that ideas can be translated into practice in the most effective manner possible. At a practical level, it is essential that strategic actors prepare adequately for war in the cyberspace age. This has significant implications for the development of military culture, organization, and capability requirements. The further rationalization of cyberspace commands and operations is therefore to be welcomed. However, at the same time we must resist the temptation to assume that the maturation of cyberspace has fundamentally changed the nature of strategy, or indeed enabled the development of radically new operational concepts. War will remain a violent, competitive political act, laden with friction. The man on the scene with a gun will continue to be the ultimate arbiter in war. The exploitation of cyberspace is merely a means to support that man in his role.

Notes:

[1] This is a reference to Clausewitz's distinction between the character and nature of war. The former is changeable, whereas the latter is not. See Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1989).

[2] For discussions on the paradoxical logic and disharmony within the levels see Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge: The Belknap Press of Harvard University Press, 1987). For a general discussion on the nature of war see David J. Lonsdale et al., 'Strategy,' *Understanding Modern Warfare* (Cambridge: Cambridge University Press, 2008).

[3] Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999). Gray's work on the dimensions of strategy builds upon earlier work on the subject by both Clausewitz and Michael Howard. For the latter, see Michael Howard, 'The Forgotten Dimensions of Strategy,' *Foreign Affairs* 57 (1979): 976-986.

[4] Gray, Modern Strategy, 26.

[5] For a discussion of strategic information warfare see, for example, G. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001).

[6] For a detailed analysis of these obstacles see David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004) especially pages 151-166.

[7] J. C. Wylie, *Military Strategy: A General Theory of Power Control* (Annapolis: Naval Institute Press, 1967).

[8] Clausewitz, *On War*, 89.

[9] For a discussion of these issues see J. T. Mathews, 'Power Shift', *Foreign Affairs* 76, no. 1 (1997), and J. Arquilla and D. Ronfeldt, *The Advent of Netwar* (Santa Monica: RAND, 1996).

[10] For a discussion of humane warfare see C. Coker, *Humane Warfare* (London: Routledge, 2001).

[11] Leading exponents on the rise of the network are Arquilla and Ronfeldt. See John Arquilla, and David Ronfeldt, *The Advent of Netwar* (Santa Monica: RAND, 1996).

[12] Such claims are evident in the work of Martin Libicki. See, for example, Martin C. Libicki, 'The Emerging Primacy of Information', *Orbis* 40, no. 2 (1996).

[13] B. Lambeth, *NATO's Air War for Kosovo: A Strategic and Operational Assessment* (Santa Monica: RAND, 2001).

[14] Gray, *Modern Strategy*, 39.

[15] Ibid., 36.

[16] US Joint Forces Command, *Effects-based Operations White Paper Version 1.0* (Norfolk, VA: Concepts Department J9, 2001), 5.

[17] Clausewitz, *On War*, 271.

[18] J. F. C. Fuller, *Armament and History: A Study of the Influence of Armament on History from the Dawn of Classical Warfare to the Second World War* (London: Eyre and Spottiswoode, 1946).

[19] Gray, *Modern Strategy*, 38.

[20] David J. Lonsdale, *Alexander the Great: Lessons in Strategy* (London: Routledge, 2007).

[21] This argument is strongly made in John Ellis, *Brute Force: Allied Strategy and Tactics in the Second World War* (London: Andre Deutsch Limited, 1990).

[22] Winston S. Churchill, quoted in M. Carver, 'Montgomery,' *Churchill's Generals*, ed. J. Keegan (London: Weidenfeld and Nicolson, 1991), 148.

[23] M. Libicki, 'The Emerging Primacy of Information'.

[24] Clausewitz, *On War*, 97

[25] Gray, *Modern Strategy*, 42

[26] Quoted in R. L. DiNardo and J. Hughes, 'Some Cautionary Thoughts on Information Warfare,' *Airpower Journal* 9, no. 4 (1995), 76.

[27] Gray, *Modern Strategy*, 42.

[28] Whilst on the Earth and operating at normal speeds time is essentially constant. However, it is recognized by this author that time is actually relative. The relative nature of time is influenced by changes in distance from large masses and speed of travel.

Dr. David J. Lonsdale (MA, Aberdeen; MA, Hull; PhD, Hull) is a lecturer in Strategic Studies at the University of Hull. Prior to this he worked at the University of Reading, and was a lecturer in Defence Studies at King's College London, based at the Joint Services Command and Staff College. His primary area of research is strategic theory and its application to contemporary and historical issues. Dr Lonsdale's publications include *The Nature of War in the Information Age: Clausewitzian Future, Alexander the Great: Lessons in Strategy,* 'Clausewitz and Information Warfare,' in *Clausewitz in the Twenty-First Century*, and 'Strategy,' in *Understanding Modern Warfare*.

Taiwan Examines Chinese Information Warfare

Mr. Timothy L. Thomas
Senior Analyst
Foreign Military Studies Office (FMSO)
Fort Leavenworth, Kansas

This article summarizes the views of several Taiwanese specialists who focus on Chinese information warfare (IW) tactics, organization, and policy.

Taiwanese military specialists have studied Chinese IW topics for over two decades. Due to their common language, culture, and close proximity with the mainland, the Taiwanese are capable of discerning nuances in the People's Liberation Army's (PLA's) approach to IW that might escape a Western analyst. Some of the interesting PLA IW concepts that Taiwanese military professionals have discussed, for example, include:

- Acupuncture war
- Highly-controlled war
- Strategic information war
- Political work Web sites
- Intangible war
- Net force
- Surgical war

Understanding the PLA's potential use of information technology and IW theory is key to the future security strategy of the Republic of Taiwan. It is mandatory for Taiwanese government and civilian professionals to study Chinese IW intensely and be able to predict and foresee the PLA's potential use of IW against Taiwan in both peacetime and wartime.

This article will examine Taiwan's analysis of several issues (asymmetric war, IW theory, political work and psychological war, media war, and PLA IW institutes) associated with PLA IW. Also covered in this article will be Taiwan's view of the PLA's focus on the revolution in military affairs and how that revolution has transformed the PLA from a mechanized to an informationized force. These developments impact the PLA's policy, organization, education, structure, and theory of IW.[1]

A Taiwanese View of the People's Liberation Army's Revolution in Military Affairs

The Chinese military has studied the meaning and impact of the revolution in military affairs (RMA) for more than two decades. While it might be assumed that China's understanding of the RMA would be similar to that of the US or other nations, it is not. For example, in 2001, retired Chinese Maj Gen Wang Baocun defined the term as a process of military informationalization where theory and practice are the focus. He added that Chinese progress toward an RMA is signaled by its command, control, communications, computers, and intelligence modernization, network-based war-gaming, IW personnel training and field exercises, and informationalized equipment.[2] Thus Wang's Chinese perspective indicates that the information revolution is the key component of the current RMA. US analyst Richard O. Hundley of RAND defined the RMA in 1999 as "a paradigm shift in the nature and conduct of military operations which either renders obsolete or irrelevant one or more core competencies of a dominant player; or creates one or more new core competencies, in some new dimension of warfare; or both."[3]

The US and Chinese differences most likely are a direct reflection not only of capabilities but also of culture. The US lead is in technology while the Chinese rely on theory and strategy to enable (in their opinion) their inferior force to overcome US superiority. Further, Wang is not the only Chinese military figure with an opinion on the RMA. One Chinese author noted that the RMA is really a cognition system revolution and a new phase in military strategy research. Another author added that the RMA involves a series of changes to military theory, methods of operations, weaponry, systems organization, command organization, and so on; an understanding closer to most US RMA concepts.

One thing is certain: the Chinese hope to develop an RMA concept with "Chinese characteristics." A Chinese general noted that "Only with superior thought processes and superior moves, and by seeking a developmental strategy of 'imbalance' will we truly be able to avoid traveling the 'path that the enemy expects.' In the realm of IW, trying to keep up with the Jones' by developing whatever they possess will lead to falling into traps set by others…"[4]

Taiwan's understanding of the Chinese RMA does not necessarily coincide with these views completely. Maj Li An-yao, who was serving in the Air Force Command of the Ministry of National Defense of Taiwan when he wrote about this topic, stated that the revolution in military affairs has changed China's strategic views on international security and on constructing fast response and projection capabilities. He listed five characteristics of the Chinese communist's revolution in military affairs that concern Taiwan: the gap in military technologies has affected China's national security and forced the PLA to place priority on technological development; the transformation has forced adjustments in battle thought, theory, equipment, and training (this point coincides with Chinese theorists noted above); a "show of weakness" by the PLA can help thwart the China threat theories being developed; the study of asymmetrical and unrestricted warfare has developed deterrents and counters to Western developments (currently such thinking includes the use of a preemptive strike); and IW can help win a future war in the Taiwan Strait since it is marked by high technologies, a brief time period, and few casualties.[5]

Li was impressed with the contributions of former Chinese leader Deng Xiaoping to new thinking and its impact on current projections. Deng emphasized People's War (PW) under

modern conditions and he recommended a shift in the center of gravity in Chinese decision-making to economic construction and the development of science and technology. Today top-level decision-makers in China understand fully the importance of economic modernization alongside military modernization. Modernization helps China change its way of conducting a war. Li writes that the Chinese link IW to a technical form of war defined by the widespread use of information technologies. PW refers to a political form of war defined by the righteous nature of a war. China's RMA must be laced with such Chinese characteristics in accordance with the societal shift in the forms of technology and war from the mechanized to the information age.[6]

However, Li also pointed out China's RMA weaknesses. First among them is the age of the military leadership. Next are obstacles in the development of new weapons and equipment such as increased costs, the lag in domestically produced weapons, the technical integration of weapons purchased from foreign nations, and the reliability of precision guidance components. Finally, China lacks experience in offensive operations and in Navy and Air Force operations. Li concluded by noting that Taiwan "must pay close attention to the direction of China's army building, study the course and results of PLA military reform, and draw upon the experience of the rise of the Chinese communists following the path of overcoming strength with knowledge as soon as possible."[7]

Maj Hsu Hsieh-jung was another Taiwanese officer who wrote about China's RMA concept. While noting that the PLA must expedite its "military reform with Chinese characteristics," Hsu believes China must also take into account the recent successes of the US and its coalition partners in Iraq, Afghanistan, and elsewhere. In those locations, decapitation operations were utilized against the leadership of the regimes. These actions indicate one must innovate (the soul of the RMA to Hsu) and learn from other experiences such as those of the US if it wants to avoid perilous situations.[8]

One of those lessons, Hsu writes, is that China must be adept at "highly-controlled warfare" since it was a special characteristic of the war in Iraq. The PLA's Academy of Military Science noted that the 2003 US-Iraq war was characterized by "a high control level, high demand for control, and a high degree of control." War is evolving from general war to highly controlled war. This change is felt not only in military affairs, but also in the emphasis on control over political, economic, and other sectors to include psychological control. Highly-controlled war is a new form of warfare in which "the direct purpose is to control a political regime and in which political, economic, diplomatic, and other resources are integrated effectively to control the scale, form, means, and results of the war, with the backing of absolute military superiority."[9] War is expanding from tangible to intangible war as a result.[10]

Other ways in which China's RMA differs from Western countries include:

- Pursing a different strategic purpose than the West (which pursues world hegemony in China's opinion).
- Utilizing different motivations than the West to stay in line with the profound changes in modern warfare.
- Starting from a different technological point than the West, since China is still going through the late stages of mechanization.
- Utilizing different operational RMA forms, such as leap-frog developments instead of the West's gradual development.[11]

For these reasons, Hsu notes, the PLA cannot copy the model of advanced Western countries. It must be familiar with the laws of the RMA and apply their contextual situation to it in order to avoid being trapped in an arms race with the West as happened to the former Soviet Union. Study of the Iraq war and US successes in Kosovo convinced China that the idea of winning local wars under high-tech conditions had evolved to that of winning informatized war based on high-tech conditions.[12]

A Taiwanese View of the People's Liberation Army's Asymmetric War Concept

In the information age, stratagems and psychological operations of all types can play havoc with an opponent especially when combined with the use or even potential use of exotic weapons. Chinese asymmetric warfare operations fit this description and they are not restricted by time and space. Stratagems used in the time of Sun Tzu are equally applicable in the virtual environment of today.

Asymmetric warfare is a method for China to deal effectively with its current potential superpower opponent, the US. Surgical war, paralyzing war, and unrestricted warfare operations are all examples of asymmetric warfare operational measures that the Taiwanese ascribe to the PLA. Taiwanese author Chen Wei-K'uan used the definition of a PLA military strategist, Kuo Yung-bing, to define asymmetric warfare as "operations in which any two opposing parties in a war can try their best in using their own advantages in strategy, weapons technology, and applications of their arms and services as much as possible to locate and attack the vulnerabilities of the opponent fiercely and overwhelmingly."[13]

Chen states that stratagems are one of the most typical ways that China uses asymmetric warfare. He notes that a stratagem is used "to force an enemy to make mistakes which can then be taken advantage of." He quoted from a few Chinese military classics to demonstrate this point:

- In the art of warfare, a psychological offense is better than capturing a city, and a psychological war is preferable to an armed war. ~ Zhu Ge Liang
- A whole army may be robbed of its spirit; a commander in chief may be robbed of his presence of mind. ~ Chapter VII: Maneuvering, Sun Tzu's *Art of War*
- All warfare is based on deception. ~ Chapter I: Laying Plans, Sun Tzu's *Art of War*
- In war, the way is to avoid what is strong and to strike at what is weak. ~ Chapter VI: Weak Points and Strong, Sun Tzu's *Art of War*
- In all fighting, the direct method may be used for joining battle, but indirect methods will be needed in order to secure victory. ~ Chapter V: Energy, Sun Tzu's *Art of War*

- Attack him where he is unprepared; appear where you are not expected. ~ Chapter I: Laying Plans, Sun Tzu's *Art of War*
- In war practice dissimulation and you will succeed. ~ Chapter VII: Maneuvering, Sun Tzu's *Art of War*
- Thus the highest form of generalship is to frustrate the enemy's plans. ~ Chapter III: Attack by Stratagem, Sun Tzu's *Art of War*
- The key to overcome an enemy relies more on the use of strategy to deceive the enemy than the use of force. Thus, people who are good at commanding the troops are those who can deceive and who also can avoid being deceived. ~ Chapter on Deception, Jie Xuan's *100 Stratagems of War*

Chen focused on technological aspects of asymmetric warfare operations that aim to paralyze an opponent before their destruction, if the latter scenario was even needed. First are soft-kill weapon systems, which include electronic jamming equipment, computer viruses, directed-energy weapons, laser beam weapons, and non-directed-energy weapons. Second are precision and remote tactical missile attacks, not only aimed at troop assembly points or hardware construction targets, but also aimed to paralyze command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), radar reconnaissance systems, and command center targets. Third is the development of an electronic warfare (EW) capability, electromagnetic pulse weapons, and the ability to construct a comprehensive surgical warfare infrastructure (based on importing weapons from Russia at an increased tempo). Surgical warfare aims to attack the vulnerability of high-tech weapons systems to achieve final victory, namely, attacking one point to cripple the whole system. Finally, the development of a space warfare capability puts the crowning touch on China's asymmetric warfare capability: the ability to sabotage or destroy an enemy's space systems.

Chen's conclusion was that China is headed quickly in the direction of winning a regional war under high-tech conditions via asymmetric warfare operations. It is unfortunate that he did not go into more detail as to how the two areas he covered (stratagems and technology) might be integrated.

Another author, Chung Chien, wrote that a symmetric war involving the PLA and other nations may last for a long time and is not an option sought by China. An asymmetric warfare operation, on the other hand, has the opportunity to last but a matter of hours or weeks and would be a preferred operation, one "without bloodshed." Two types of operations that Chung mentioned the PLA might enact were: a PLA long range blockade of Taiwan's sea lines of communication, cutting Taiwan's logistic life-line through the Spratlys; and an electromagnetic pulse attack that would shut down all services in Taiwan and make command and control impossible.[14]

A Taiwanese View of the People's Liberation Army's Information Warfare Concept

Taiwanese professor P'an Chin-chang wrote in 2007 that the PLA views informatized warfare (another way of saying IW) as "a war pattern which refers to that included under nuclear deterrence in the information age, where two sides in a war use information as the lead, comprehensively use information to integrate platforms and informatized weapons, and conduct joint combat efforts by multiple services and branches in all-dimensional space, including land, sea, air, space, and electronics."[15] Informatized warfare includes precision combat, network combat, special operations, and space combat. Such combat includes direct attacks that "jump over time and space" and aim to take multi-dimensional control of battlefields and to destroy and paralyze the opponent's combat system.[16] Informatized warfare will require the comprehensive integration of four capabilities: sensing the battlefield, information transmission, rapid mobility, and accurate strikes.[17] The PLA's IW focus is on the control of information. The ability to manipulate information and seize information supremacy is the preeminent quality in future war, according to P'an.[18]

This was not always the view that Taiwan took of PLA IW theory and practice. In fact, Taiwan's views of the PLA's IW capability have evolved over time. In the late 1990s, Lin Chin-ching, director of the Telecommunications Bureau of the Ministry of National Defense (MND) in Taiwan, served as a prominent spokesman for IW issues and continued to do so for several years. He listed three ways that China might strike at Taiwan's digital infrastructure. First, he stated that China's goal was to paralyze Taiwan "by destroying its command and control system using an electromagnetic device the size of a briefcase."[19] Second, citing EW theory, he said China would use "acupuncture-point-prodding," the ancient Chinese martial art theory of taking out an enemy with a strike on a pressure point. Finally, he noted that China would try to steal Taiwan's military secrets via the Internet or the use of computer viruses.[20]

In response to the Chinese IW threat, Lin says Taiwan set up a Strategy Planning Committee for IW. He noted that Taiwan had also established computer emergency response teams; established a telecommunication and information security committee; stipulated laws and relations concerning telecommunications and information security; improved procedures to access computers; and installed warning devices on all networks to strengthen the awareness of computer personnel about potential threats.[21] Taiwan is also trying to make people aware of the Chinese potential to spread false news about the stock market through the mass media and cause confusion or panic in society.[22]

In 2000 Lin predicted that the next five years would be crucial for the development of IW capabilities on both sides of the strait. He noted that China had established an IW simulation center, developed viruses to be used in attacks against networks, and imported foreign information technology and equipment. By 2005 he believed the PLA could establish a neural network center to execute joint simulations; develop battlefield command systems to provide better troop mobility; develop a tactical data link system; digitize and mobilize command and control systems; strengthen satellite communications research and development; and establish an optical fiber communications network. As a "communist totalitarian nation," China will also use the entire nation's effort to mobilize IW's development.[23]

Also in 2000, Taiwan Defense Minister Wu Shih-wen stated that a military unit in charge of cyber warfare would be established. The unit would be responsible for protecting Taiwan's computer systems from hackers and for denying access to unauthorized individuals. Lin Chin-ching added that all officers under the rank of lieutenant general would be tested on their knowledge of IW and computer information and that their test results would be taken into consideration when their files are reviewed for promotion.[24] The initial military cyber unit would be a battalion sized unit of specialized troops with a focus on the development of IW and EW capabilities, especially C4ISR. These areas will account for 23 percent of the defense budget according to Lin.[25]

In 2005 another Taiwanese author with the last name of Lin, Lin Tsung-ta, who by reputation is one of Taiwan's most outstanding scholars on Chinese IW, wrote a book titled *All Out War on the PRC's Information Warfare*. He focused on Chinese IW's asymmetric character, its use of civilian entities and applicability to PW theory, and its preemptive and deterring qualities. Chinese IW requires "attacking vital points," words that are conceptually similar to Lin's focus on acupuncture war.[26]

Lin noted that China's National Defense Science and Technology Information Center divides IW into three parts. The first is EW/command and control warfare equipment. The second is offensive information weaponry, described as: computer virus weapons, nano-machines, chip microbes; hackers; high energy radio frequency guns; and power damaging munitions. The third type of weaponry is defensive weapons, to include: network sentries; information defense encryption systems; firewalls; and multi-layer Internet defense networks. Further, Lin added that combat power in the opinion of many Chinese scholars lies in the control and counter-control of information since those who control information control the initiative on the battlefield in future wars.[27]

There are new types of PW, Lin stated, such as hacker force and propaganda force PW. Like military forces they can obtain military intelligence, bolster morale, and interfere with an enemy information system. Combat goals can be reached simply by damaging another side's economy. People's IW is an asymmetric and non-violent type of national war. China is deepening the study of "Network PW" mobilization education to make every Netizen (Internet citizen) a "network combatant." Mobilizing IW talent in the military and in society will be the key to future successes. As of 2005, the PLA had carried out deliberations on organizational institutions for PW, civilian mobilization plans, strategies and tactics, and training for Network PW. Strategies provide an intangible combat power asset that compensates for insufficiencies in material conditions according to Lin. Legal systems, secrecy, market competition, and intellectual property rights are other ways to add intangible power to the PLA's arsenal.[28]

People's IW uses asymmetric operational methods to enable opening up a second battlefield for the PLA far from the combat zone and in the enemy's rear area. Moreover the goal of Chinese PW "is to proactively protect international information infrastructures while attacking enemy rear political, economic, and military information systems, damaging the enemy's economic order in the rear, weakening the enemy's combat potential, and further influencing the progression of war. During this process, enterprises and individuals nationwide use their computers, communications equipment, and other information systems' signals and resources to provide sustained support to the nation's information infrastructure in the strategic rear."[29]

Finally, PW strategy relies heavily on military modernization. Economic growth is crucial and a high-tech national defense industry must be developed. Lin notes that China intends to pursue international exchanges to increase its national defense economic potential.[30]

In September 2007 Maj Gen Tschai Hui-chen, the director of Information Assurance for Taiwan's Ministry of National Defense and deputy chief of the general staff for communications, electronics, and information, spoke at a conference at Fort Leavenworth, Kansas. Tschai noted in a section of her report to conference attendees that with regard to threats and challenges before Taiwan, China remains the greatest concern in both areas. She discussed general information security threats, strategic IW threats, and general security threats posed by China's emphasis on IW. Of interest is that in her report, she covered many of the topics listed in Taiwan's view of Chinese IW from the mid-1990s: deterrence, paralysis, network force, asymmetric war, strategic information war, long-range precision war, and network psychological war.[31] Thus it appears that Taiwan's concerns with regard to Chinese IW have not changed much over the years other than to stress that the Chinese are more advanced in both their budgetary spending on and development of information technology.

Naturally, even though the general categories have remained basically the same, each is much more sophisticated and advanced than it was in the 1990s.

A Taiwanese View on the People's Liberation Army's Political Work and Psychological War

The PLA has always been expert at the use of psychological warfare techniques, particularly the application of psychological pressure. The firing of missiles near Taiwan into the Taiwan Strait in 1996 and the development of an Anti-Secession Law in 2005 exerted both psychological pressure on Taiwan to "toe the line" and abandon any thoughts of independence from the mainland. A recent episode of psychological pressure involved the former Russian Kuznetsov class aircraft carrier Varyag. Chinese sailors and civilians refurbishing the carrier state that it will soon be renamed the Shi Lang (after the Chinese general who took possession of Taiwan in 1681, which was the first time China paid attention to the island).[32]

Mr. P'an Chin-chang, a teacher at Taiwan's National Defense University in 2007, wrote a few excellent articles on the PLA's "informatized" political work and use of psychological warfare techniques. P'an described the PLA's political work database and political work Web site that enhances the combat functions of informatized political work. The PLA believes, he writes, that informatized warfare is not just competition in weapons and equipment but also in ideology, will power, political strength,

spiritual factors, and psychological capacity. Information "includes not only military information transmitted by digitized weapons and equipment but also political and ideological information to be used to launch psychological offensives against the enemy. Informatized warfare involves not only the competition of military force but also non-military competition of political and psychological power."[33]

P'an stated that on 20 October 2005 the PLA inaugurated its political work Web site. No longer would paper be the only way to convey teaching materials. The Web site's operations center is located at the General Political Department in Beijing. The six major functions of the Web site are operational guidance, news and information dissemination, propaganda and education, study and training, culture and entertainment, and communication and interaction. The site offers online lectures, distance learning, and even psychological counseling.[34]

The site is carrying "some 3,000 items per day, the Web site is updated every minute, there are 44 channels, including nine interactive and online-posting channels, which carry 382 second-level columns, 2,530 third-level columns, 53 large-sized databases, numerous books, videos, and games, more than 1,000 kinds of newspapers and journals, and every article document can be opened and refreshed instantly."[35] National Defense University has developed six types of software for political work command platforms for the site and is researching over thirty projects concerning the informatization of political work.[36]

The PLA is studying other aspects of political work as well. A symposium held at Nanjing's Academy of Political Science in December 2004, for example, highlighted eight aspects of the informatization of political work. P'an described the findings as: developing the theory of informatization of political work; training professionals; applying information technology to political work; developing and enriching information resources; allocating information equipment and facilities to political work; constructing political work for an information network; formulating policies, laws, ordinances, and standards for the informatization of political work; and enhancing information-related capabilities of political work cadres. The Nanjing Academy stressed the importance of political competition in future wars, citing competition in political stratagem, media propaganda, and psychological manipulation as well as legal competition.[37]

Psychological warfare, a major aspect of informatized warfare and political work, is now a part of the PLA's state strategy, P'an added. This has resulted in the development of the following categories: political psychological warfare, economic psychological warfare, military psychological warfare, diplomatic psychological warfare, religious psychological warfare, cultural psychological warfare, propaganda psychological warfare, and deterrent psychological warfare. All of these types of psychological warfare can be used to enhance "beheading" an enemy force instead of attacking it with conventional forces.[38]

Regarding the future development of psychological warfare, the PLA proposes:

- Establishing psychological warfare command institutes
- Creating psychological warfare specialty troops
- Setting up psychological warfare research institutes
- Cultivating a team of psychological key members
- Developing psychological warfare technologies and devices
- Establishing special psychological warfare training venues
- And establishing psychological warfare platforms with computer networks[39]

The use of these facilities will enable the PLA to stealthily substitute one thing for another, to replace and edit people and landscapes in a virtual world, and to produce some false and shocking scenes to deceive and incite discontent. Network confrontation training is required to improve the conduct of network psychological warfare and help develop countermeasures against its use by enemy forces. Troops are developing and conducting simulated training using sound, light, electronics, and information technologies.[40]

When fighting an enemy force, the deputy director of the Political Work Research Institute of the PLA's Academy of Military Science, Gong Fangbin, wrote that:

> A study by the PLA General Staff Department also concluded that the actual cases of the several high-tech wars in recent years have shown that information technology, when applied to the psychological warfare battlefield, has promoted: the development of instant psychological warfare propaganda operations; the invention of intellectual equipment for psychological warfare; the diversification of the means of psychological warfare; and the integration of psychological warfare and armed warfare.[41]

Political cadres must be capable of buttressing local opinion and demoralizing enemy attitudes. With regard to local opinion, cadres must be able to manipulate information and launch the "three types of warfare" (legal, public opinion, and psychological) before a military operation begins. This will ensure that the people are on the side of the armed forces and that they will trust that the war being fought is a just war, according to P'an's interpretation of the PLA's work. With regard to demoralizing the enemy, P'an cites PLA Professor Zhang Zhaozhong, who noted that it is necessary to "distort the enemy's cognition system through IW and psychological warfare, and thus win a war without really fighting a battle, or by fighting fewer battles, or by fighting only small-scale battles."[42]

Zhang also stressed the importance of strategic IW as a new form of war that can take on an independent posture and even be launched several months or years before an armed invasion takes place. Targets of strategic IW include national political, monetary, communications, and other crucial sectors down to single weapon systems such as aircraft carriers. Developments can lead to the use of strategic deception, strategic psychological warfare, strategic deterrence, or strategic information attacks.[43]

Not all is well with political work in the PLA, however, according to P'an. He notes that duplicate organizations still exist, coordination is difficult, lateral communication is not as prevalent as top-down communications, and communication equipment is still susceptible to damage. These constraints continue to limit the effectiveness of the PLA's political work Web site. However, the PLA will continue to use military force alone in

the absence of other psychological factors to continue to intimidate Taiwan.[44]

A Taiwanese View on the People's Liberation Army's Media Warfare

Closely related to political work and psychological operations is the concept of "media warfare." A relatively new field of research in terms of terminology, media warfare appears to be an updated version of "propaganda work" whose importance, the PLA ascertains, has not diminished. As Mao noted, "the Red Army's priority in conducting its propaganda work is to expand its political influence and win the trust of the majority of our people … the Red Army's propaganda work is the first and most important work for the Red Army."[45] In a high-tech environment, the PLA is concerned that its officers and soldiers will have to overcome a psychology of fear, panic, isolation, and pessimism. Solid media warfare prepared ahead of time can help alleviate some of these concerns.[46]

Taiwan researcher Liu Wan-lin discussed how China had closely followed the two Gulf Wars and drawn several important conclusions. The PLA believes that the media must be managed and controlled to establish an effective propaganda system that puts pressure on an opponent. The true nature of a war must be publicized, as well as world opinion about the war and the PLA's policy. World opinion should be prepared ahead of time since modern war is a political and diplomatic process as well as a military process, according to Liu's analysis of Chinese media. Media warfare can create opportunities and conditions that help win a war by influencing national strategy and military strategy simultaneously.[47]

Media warfare is an aspect of former Chinese President Jiang Zemin's three warfare concept for political work that includes media war, legal war, and psychological war. Due to media wars strategic significance, the General Political Department of the PLA issued a new "PLA Political Work Regulation" and directed military educational organizations to increase their focus on this topic. More than 50 software suites on political work, battlefield propaganda methods, and so on have been created. The Academy of Military Science created a "Research Center for Cross-Strait Issues" and a "Research Institute for Political Work."[48]

At the regional level, the Nanjing Military Region's officers and soldiers were provided a booklet titled "Concise Handbook of Law-Abiding Combat Operations" and the Nanjing Political Academy opened a new course called "Media Warfare." The PLA's Xi'an Political Academy handed out materials on "100 Questions and Answers on Media Warfare, Psychological Warfare, and Legal Warfare." They prepared a course on "Political Warfare Operational Command Automation" and established more than 10 new research and teaching divisions to include a psychological warfare department, a military security protection department, a wartime political warfare work division, and an information technology and political warfare work division.[49]

Media warfare measures can help China win the consent and support of the international community. The PLA hopes to offset the use of deceptive propaganda by a potential opponent and thereby assure that the direction of the media and public opinion is on the side of the PLA. The PLA will also continue to contain Taiwan, in Liu's opinion, via the use of the US while promoting its "One China" policy.[50]

A Taiwanese View of the People's Liberation Army's Electronic Warfare Assets

Taiwanese officers and professors frequently write on the PLA's electronic warfare capabilities. They cover topics such as the PLA's capabilities, troops, EW attack potential, and Taiwanese responses. Navy Commander Hsu Keng-wei wrote on the PLA's EW attack options in 2008 and his article will be highlighted here.[51]

Hsu stated that the PLA has built a dense network of electronic monitoring stations and radar early warning installations opposite Taiwan. The function of these assets is to surveil, detect, and jam Taiwanese anti-air, early warning, and control facilities. Recently, the PLA has succeeded in reverse engineering the EW equipment of several countries which has greatly improved their capabilities. They have also learned how to attach EW equipment to unmanned aerial vehicles. Hsu added that the "East China Electronic Warfare Network" has learned how to integrate all EW troops stationed in Zhejiang and Fujian and focus them on Taiwan.[52]

Taiwan scholars believe that by 2012 the PLA will have electromagnetic pulse weapons capable of paralyzing Taiwan's electronic business, aviation controls, banks, the stock market, and the Internet if war erupts. A computer network attack could also take the form of a preemptive move by the PLA to jam and paralyze US support before a war begins.

Hsu named the HD 5, HD 6, and TU-154 aircraft as EW reconnaissance and jamming platforms designed for use against Taiwan's air and sea fleets. In addition to the multitude of EW platforms available to the PLA, recent Chinese successes in space have added to Taiwan's concerns. These successes, from Hsu's perspective, indicate that China can collect a huge amount of information on Taiwan and "establish an electronic order of battle to weaken our military's EW capability … and further destroy our EW facilities for command, control, communication, and intelligence."[53] The PLA regularly practices working in an intense EW environment in their military exercises which has increased their practical experience in this area. In acupuncture war, Hsu concludes, using EW can enable "the first battle being the final battle."[54]

A Taiwanese View of China's Military Information Warfare Institutes

Taiwanese reporter Liao Wenzhong, in a set of two articles on China's military net force, listed a series of institutes and programs in China associated with the IW effort. He set the stage for his first article by citing the January 2002 PLA release of its *Seventh Generation Training and Evaluation Outlines* in which it disclosed that the PLA had formed a science and technology experimental force in order to respond to 21st century warfare challenges.[55] The force included a space, net, EW, and psychological warfare force that serves as the basic force for

IW. The PLA would be responsible for offensive network warfare and EW while other aspects (network security, psychological warfare, and intelligence warfare) would be the responsibility of other government departments.

This was far from the beginning of the Chinese effort, as the following time line for IW developments demonstrates. Much of the work began in the early 1990s. All of these references were included in Liao's two articles:

1992 Chinese authorities develop the "China Internet Plan" controlled by the mainland.[56]

1997 The Communist Party of China (CPC) creates the National Informatization Leadership Group.[57]

1997 The General Office of the State Council upgraded and renewed the project for the main computers of the general office. For the top secret portion of the project, multi-field encryption, transmission encryption, mandatory identification cards, mandatory access control, and the use of equipment with low electromagnetic leaks were instituted.[58]

1998 The State Council created the Ministry of Information Industry;[59] and the Third Research Institute of the Ministry of Public Security created the State Research Center of Anti-Computer Invasion and the Prevention of Viruses. The Third Research Institute trains information security agents to be responsible for the prevention and handling of computer viruses and basic testing. It takes on projects from the State 863 Plan and the design plan of the Gold Shield Project Security Support System.[60]

1999 The CPC started to create "information warriors."[61]

1999 The Central Military Commission of the PLA established the first psychological warfare research and teaching section at the Xi'an PLA Political College. Courses taught included military and social psychology, psychology under high-tech conditions, network warfare and psychological warfare, and psychological warfare theories and practices.[62]

2001-03 The PLA created research centers within related IW forces or research institutes in five large cities, Zhengzhou (IW simulation research center), Jinan (IW confidentiality research center), Beijing (IW operations research center), Nanjing (IW intelligence research center), and Xian (IW operations research center). The IW operation research center in Beijing has worked with the "special information research center," formerly known as the psychic function research center.[63]

2002 The IW division of the national strategic level of the CPC determined that the PLA would be responsible for EW and IW, also known as integrated network and EW; the 4th Department of the General Staff is to form a net force composed of the PLA and information militia from the National Defense Mobilization Commission and civil information technology industry, officials, and academia.[64]

2002 It is predicted that there are 46 million Internet users in China.[65]

2002 The Ministry of Defense set up scholarships and accepted more than 200 students from different universities to study and then work for the military after graduation.[66]

2002 The PLA presented the concept of a "local war under informatized conditions" to replace the term "local war under high-tech conditions."[67]

2002 The formation of an information militia for all of China was finished. Organizationally, it has four components: an EW unit, a network warfare unit, a hacker unit, and an information rescue unit. Wartime tasks include extensive reconnaissance, information defense, and information attacks.[68]

2003-04 Large information technology companies in developed in cities on the east coast of mainland China create national defense information militia units.[69]

2003 The CPC and State Council approved the Ministry of Public Security's effort to build the "Gold Shield Project," which would transform the entire information management sector of the public security system into an electronic version.[70]

2003 The State Development and Reform Commission of the State Council approved the 1203 Project of the Ministry of Public Security, the public key infrastructure, and authorization management systems.[71]

2004 The Ministry of Public Security and departments of public security in six provinces and municipalities were connected to security application systems with the PKI/PMI platform.[72]

2004 The number of Internet crime cases rose from 2,700 in 2000 to 13,600 in 2004; the number of network police and "network security guards" in China rises to 230,000. China recognizes the need for an independent Chinese Internet.[73]

2005 News networks in the US focusing on propaganda against China were modified, meaning that a guerilla war at the enemy's rear had been formed.[74]

2005 A Network Security Information Agency was organized, a social mechanism more like informants for intelligence agencies. They monitor social situations, perform social control, and conduct special case investigations of network use. Among network friends they are referred to as "net spies."[75]

2005 The Information Office of the State Council and the Ministry of Information Industry jointly issued the Provisions on the Administration of Internet News and Information Services. Anti-government speeches are not allowed under this provision.[76]

2005 There were close to 130 million Internet users in China.[77]

2006 The CPC declares that wireless local area network (WLAN) Authentication and Privacy Infrastructure Association has been created in Beijing. It is the Chinese National Standard for WLAN to which China has independent intellectual property rights.[78]

2006 The *People's Liberation Army Daily* reports that the

Second Artillery Force has created an "informatized blue army" formed by professional electronics information officers. The army's task is to simulate electronic and network attacks against the red army.[79]

2006 China cracks down on Internet crime and requires network users to go online with their actual names, identification, and registration.[80]

Other organizations and programs do exist but no dates were provided for their founding. In his article on network decapitation, Liao listed state (party) and PLA organizations. At the state level there is the Network and Information Security Team of the Informatization Work Office of the State Council. It is responsible for coordinating all institutes responsible for information security, such as the Ministries of Public Security, State Security, Information Industry, and the State Certification and Accreditation Administration, among others. The Public Information Network Security Supervision Bureau and the Net Supervision Division are in charge of the national network for information security. Some responsibility is also shared with the Division of Network and Information Security under the Information Communication Bureau for network secrets protection and security.[81]

With regard to the PLA, Liao noted that it is the 4th Department of the General Staff that is responsible for compiling IW textbooks in China. The PLA has conducted many red versus blue IW exercises. It was noted that the formation of the "blue army" by the PLA is meant to copy the combat methodology of the Red Team in the US's "IW development center." Military exercises with IW subthemes, such as "Vanguard 206B,"showed how different sub-phases, characteristics, armed services, branches, and transportation equipment could be integrated through the information power of an EW troops' "net force."[82]

The PLA believes there will be a battle for virtual territory and for the material battlefield. The true "net force" lies in the information militia of the Information Mobilization Office under the State Mobilization Commission. It will continue to try to become independent of the world of networks by developing a China Internet as well. Liao concluded the article by noting the following:

> The 'net force' is a brand new type of 'Grand War' scheme that combines high-tech knowledge with politics, economy, psychology, and information networks and that is 'all people being soldiers, the integration of peace and warfare, and dual usage for the military and civilians.' The combat types of the 'net force' include both offense and defense. It must cooperate with strictly designed psychological warfare, and must possess the capability of acquiring 24-hour accurate intelligence. Furthermore, it requires a set of rapid and dense 'network platforms' for intelligent attacks on enemies at any time, covering the whole field and from all directions.[83]

China's independent and dedicated "net force" will be able to hide while Taiwan's Microsoft system will be exposed. Taiwan will have to figure out how to deal with this as soon as possible.

In the article on network security, Liao also discussed organizations and the PLA. The CPC formed an Information Mobilization Office under the National Defense Mobilization Commission that is parallel to the Defense Ministry. The office is mainly responsible for the overall mobilization of Chinese manpower and resources during wartime. Thus the military can "incorporate the local information forces through the information mobilization offices to generate combat power, and achieve the goal of utilizing the civil forces for military purposes and integrating peacetime and wartime." Civil forces include the information industry, communications management posts, communications science and technology, information education, broadcasting and TV, and satellite communications. [84]

The CPC's Department of Information Industry has a secret office that "recruits and absorbs computer geniuses" in computer science. These individuals are termed "network warriors" and have the freedom to test computer programs. They are taught to monitor Internet surfers or become hackers, software designers, or decoders. Others are sent abroad to settle in a foreign country and become a station for China's IW efforts in that country.[85]

The Psychological Warfare Institute concluded that psychological warfare must be integrated from the beginning of a conflict. It must be combined with precision strikes and utilize the media to influence public opinion and enhance the strength of deterrence; must utilize network warfare throughout while preventing the enemy from breaking into friendly units; and must have a design aligned with national policies, strategies, and stratagem. The strategic office of the CMC plans and conducts the CPC's military strategy and psychological warfare effort. The latter is the base for strategic warfare and uses the Internet and networks as representative operational techniques.[86]

China's State Council has proposed that it will use McWILL (Multi-carrier Wireless Internet Local Loop) as its broadband wireless Internet system, to which it has independent intellectual property rights. It can cover a radius of 19 kilometers and its urban single station coverage can be one to three kilometers. It can maintain good communication while moving at 72 miles per hour.[87]

An organization that the PLA created is the Institute of Technology. It was created from the Communications Engineering College, the College of Engineering Force, the Meteorological College of the Air Force, and 63 other related research institutes with general staff affiliations. The director of the Institute of Technology was the director of the 4th Department of the General Staff (it is unknown if this affiliation has remained). The Institute founded a Research Center for Internet Technology for the entire army and allocated more than 400 experts and professors to the center. The institute plans to accept 60 students with doctorate degrees each year to enrich its faculty. Research projects are focused on the organizational structure of the military, weapons and equipment, campaign and tactics, education, training, and logistical support.[88]

Conclusion

There are areas of agreement between Taiwanese and Western analysts as to the direction of Chinese IW. One obvious area of agreement is both groups focus on the Chinese interest in gaining "control" of cyber operations. Information supremacy

is another area of common agreement. Taiwanese IW experts do, however, extract a different terminological understanding in some cases than do Western analysts and these differences lead to different degrees of emphasis.

Some of the interesting PLA IW concepts that Taiwanese military professionals highlight in the discussion above included:

- Acupuncture war, which establishes the examination of critical points in a network that, much like the pressure points in martial arts, when taken out, can shut down an entire system.
- Highly-controlled war, which is a new form of warfare that attempts to control the scale, form, means, and results of a war with information.
- Strategic information war, which is understood to be the integration of political, economic, military, diplomatic, and other areas to produce an overall or comprehensive information victory. The targets of strategic IW include national political, monetary, communications, and other crucial sectors down to single weapon systems such as aircraft carriers.
- Political work Web sites, which have established distant learning capabilities and data-bases for quick access to information not readily available in the past.
- Intangible war, which focuses on strategies, market competition, legal systems, and intellectual property rights. These are areas of importance that the West must not overlook.
- Network warriors are computer geniuses in computer science who have the freedom to test computer programs. They are taught to monitor Internet surfers or become hackers, software designers, or decoders. Others are sent abroad to settle in a foreign country and become a station for China's IW efforts in that country.

Further, it is important to remember that China obtained Microsoft's code. We do not have the code that the Chinese will use internally and probably never will. This allows them to "interact" with our systems and code to a degree unimaginable in the past and in a way that we cannot replicate with their system.

Other Taiwanese observations of PLA capabilities were also of interest. For example, when reviewing China's military strategies after the 17th National Party Congress, several points were made by Taiwanese officials, especially in regard to the PLA's military strategy, for which Taiwan must be prepared. First, military strategy toward Taiwan revealed the requirement "to win a partial war under informatization conditions" by 2050.[89] The three step strategy to do so involves creating a solid information base by 2010, achieving a quantum leap in technology around 2020, and achieving the goal of winning an informatization war by the middle of the 21st century.

Further, Taiwan must consider not just "how" the PLA has turned from a semi-mechanized force to an informatized force but more importantly what this implies for their mode of operations and application of military strength against Taiwan. Increased reconnaissance, monitoring, and long-range capabilities will increase the PLA's overall capacity and impact on Taiwan's current assumptions about CPC invasion options. Decisive battle may be replaced by "hide-and-seek" operations under informatization conditions that use deterrence, blockades, paralysis, and other information measures. Harassing attacks may be supplemented with a "threat put forward to take massive military action to force us into political peace talks."[90]

Taiwan is rightly concerned with the aggressive direction that the Chinese have taken with their informatized force. A close eye must be kept on the scientific and technological advances that the PLA is making and how it will integrate them with their military forces' operations and strategy.

Notes:

[1] This article is taken from a chapter in the author's forthcoming book *The Dragon's Quantum Leap*, slated for publication in the summer of 2009.

[2] Wang Baocun, "China and the Revolution in Military Affairs," *China Military Science*, no. 5 (2001): 149, 154.

[3] O. Hundley, *Past Revolutions, Future Transformations*, RAND, 1999, 9.

[4] Dai Qingmin, "Discourse on Armed Forces Informationization Building and Information Warfare Building," *On the Chinese Revolution in Military Affairs,* ed. Shen Weiguang (New China Press, 2004), 39-47.

[5] Li An-yao, "PLA Thinking on War, 'Revolution in Military Affairs with Chinese Characteristics," Taipei *K'ung-chun Hsueh-shu Yueh-k'an*, Internet version, 25 April 2008 as downloaded and translated by the Open Source Center (OSC) Web site, doc. no. CPP20080421312006.

[6] Ibid.

[7] Ibid.

[8] Hsu Hsieh-jung, "An Investigation of the Impact of the Second Gulf War on the PRC's New Revolution in Military Affairs," Hsien-ping Hsueh-shu Pan-nien-k'an, online 1 December 2007 as translated and downloaded from the OSC Web site, doc. no. CPP20080701312002.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Chen Wei-k'uan, "A Study of Our Due Perception of the PLA's Asymmetric Warfare," Taipei *K'ung-chun Hsueh-shu Yueh-k'an*, 25 July 2007 as translated and downloaded from the OSC Web site, doc. no. CPP20080507312001.

[14] Chung Chien, "High-Tech War Preparation of the PLA, Taking Taiwan Without Bloodshed," *Taiwan Defense Affairs*, 1 September 2000, as translated and downloaded from the OSC Web site, doc. no. CPP20050411000204.

[15] Pan Chin-chang, "On the Role of Psychological Warfare as a Part of the PLA's Informatized Warfare Operations," *Lu-chun Hsueh-shu Shuang-yueh-k'an*, 4 June 2007 as translated and downloaded from the OSC Web site, doc. no. CPP20071119312002.

[16] Ibid.

[17] Ibid.

[18] Ibid.

[19] Maubo Chang, Taiwan Central news Agency, 1350 GMT 21 May 1999, as translated and downloaded from the OSC Web site, doc. no. FTS19990521000902.

[20] Ibid.

[21] Lin Jui-yang, "The ROC Armed Forces Strengthen Security over Information," *Chung-Yang Jih-Pao*, 17 August 1999, 3, as translated and downloaded from the OSC Web site, doc. no. FTS19990818000447.

[22] Seiji Yajima, Interview in Japanese Journal with Lin Chin-ching, *Sankei Shimbun*, 5 November 1999, as translated and downloaded from the OSC Web site, doc. no. FTS1999110500047.

[23] Lin Chin-ching, "Comparison of PRC-ROC Information Warfare Capabilities, *Ch'uan-Ch'iu Fang-Wei Tsa-Chih*, 1 March 2000, 68-73, as translated and downloaded from the OSC Web site, doc. no. CPP20000725000181.

[24] Maubo Chang, Central News Agency, 1456 GMT, 22 November

2000, as translated and downloaded from the OSC Web site, doc. no. CPP20001122000162.

[25] Brian Hsu, (no title provided) *Taipei Times*, 23 November 2000, as translated and downloaded from the OSC Web site, doc. no. CPP20001124000107.

[26] Lin Tsung-ta, *All Out War on the PRC's Information Warfare* (Crystal Books, May 2005) as translated and downloaded from the OSC Web site, doc. no. CPP20071102320002.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Tschai Hui-chen, "A Discussion of Information Warfare from a Taiwanese Perspective," *IO Sphere*, special edition 2008, 15-21.

[32] See http://www.strategypage.com/htmw/htnavai/articles/20080109/aspx.

[33] P'an Chin-chang, "A Study of the PLA's Informatized Operations for Political Work," *Kung-chun Hsueh-shu Yueh-kan*, online, 25 July 2007 as translated and downloaded from the OSC Web site, doc. no. CPP20080616312009.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] P'an Chin-chang, "On the Role of Psychological Warfare as a Part of the PLA's Informatized Warfare Operations," *Lu-chun Hsueh-shu Shuang-yueh-k'an*, 4 June 2007 as translated and downloaded from the OSC Web site, doc. no. CPP20071119312002.

[39] Ibid.

[40] Ibid.

[41] Ibid.

[42] P'an Chin-chang, "A Study of the PLA's Informatized Operations for Political Work."

[43] Ibid.

[44] Ibid.

[45] Liu Wan-lin, "An Investigation into the Impact of the PRC's Military Media Warfare on the ROC Military," Taipei *Hai-chun Hsueh-shu Yueh-k'an*, 22 April 2008, as downloaded and translated by the OSC Web site, doc. no. CPP20080602312005.

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] Ibid.

[50] Ibid.

[51] Hsu Keng-wei, "How to Effectively Counter the PRC Military's Electronic Warfare Attacks," Taipei *Hai-chun Hsueh-shu Yueh-k'an*, 22 April 2008, as downloaded and translated by the OSC Web site, document number CPP20080602312007. For a more detailed examination of the PLA's EW capabilities (too extensive for this brief survey), see Liu Yi-Chung, "How to Enhance the EW Capabilities of the ROC Military to Satisfy War Requirements across the Taiwan Strait," Taipei *Hai-chun Hsueh-shu Yueh-k'an*, 1 June 2006, as downloaded and translated by the OSC Web site, doc. no. CPP20061004312001.

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] Liao Wenzhong, "China Military Net Force: National Security, Public Security, and the People's Liberation Army," Taipei *Ch'uan-Ch'iu Fang-Wei Tsa-Chih*, 1-31 March 2007, 58-65 as downloaded and translated by the OSC Web site, doc. no. CPP20071023318001.

[56] Ibid.

[57] Liao Wenzhong, "China Military Net Force: National Security…"

[58] Liao Wen-chung, "China Military Net Force: Network Decapitation Strike and Public Security Net Force," Taipei *Ch'uan-Ch'iu Fang-Wei Tsa-Chih*, 1 April 2007-30 April 2007, 58-65, as downloaded and translated from the OSC Web site, doc. no. CPP20071016318001.

[59] Liao Wenzhong, "China Military Net Force: National Security…"

[60] Liao Wen-chung, "China Military Net Force: Network Decapitation…"

[61] Liao Wenzhong, "China Military Net Force: National Security…"

[62] Ibid.

[63] Ibid.

[64] Ibid.

[65] Liao Wen-chung, "China Military Net Force: Network Decapitation…"

[66] Liao Wenzhong, "China Military Net Force: National Security…"

[67] Ibid.

[68] Ibid.

[69] Ibid.

[70] Liao Wen-chung, "China Military Net Force: Network Decapitation…"

[71] Ibid.

[72] Ibid.

[73] Ibid.

[74] Liao Wenzhong, "China Military Net Force: National Security…"

[75] Liao Wen-chung, "China Military Net Force: Network Decapitation…"

[76] Ibid.

[77] Ibid.

[78] Liao Wenzhong, "China Military Net Force: National Security…"

[79] Liao Wen-chung, "China Military Net Force: Network Decapitation…"

[80] Ibid.

[81] Ibid.

[82] Liao Wen-chung, "China Military Net Force: Network Decapitation…"

[83] Ibid.

[84] Liao Wenzhong, "China Military Net Force: National Security…"

[85] Ibid.

[86] Ibid.

[87] Ibid.

[88] Ibid.

[89] Liu Wen-hsiang and Wu Chien-te, "Investigation into the PRC's Taiwan Military Strategy after the 17th National Congress of the Communist Party of China (CPC)," Taipei *K'ung-chun Chun-kuan Shuang-yueh-k'an*, as downloaded and translated by the OSC Web site, doc. no. CPP20080819312002.

[90] Ibid.

Mr. Timothy L. Thomas (BS, Engineering Science, USMA; MA, International Relations, University of Southern California) is a senior analyst at the Foreign Military Studies Office at Fort Leavenworth, Kansas. Mr. Thomas conducts extensive research and publishing in the areas of peacekeeping, information war, psychological operations, low intensity conflict, and political-military affairs. Mr. Thomas was a US Army foreign area officer who specialized in Soviet/Russian studies. His military assignments included serving as the director of Soviet Studies at the United States Army Russian Institute in Garmisch, Germany; as an inspector of Soviet tactical operations under the Commission on Security and Cooperation in Europe; and as a brigade S-2 and company commander in the 82nd Airborne Division. He has written three books on information warfare topics, focusing on recent developments in China and Russia. Mr. Thomas is an adjunct professor at the US Army's Eurasian Institute; an adjunct lecturer at the USAF Special Operations School; and a member of two Russian organizations, the Academy of International Information, and the Academy of Natural Sciences.

Global Effects: Pilot Explores Integrated Command and Control

Mr. John F. Vona
Technical Director and Chief
Concepts and Technology Directorate
Air Force Global Cyberspace Integration Center
Langley AFB,Virginia

"We are under [cyber] attack, we are behind, we are reactive, not proactive, and we—all of us—are making it too easy for those who would exploit and attack our networks."[1]
~ General Kevin Chilton, commander, US Strategic Command

Improving warfighter concepts and capabilities can no longer be pursued based strictly on traditional regional perspectives or single domains. In responding to the challenges of the 21st century, resources and capabilities must support the global effects senior leaders seek to achieve. Commanding and controlling these global capabilities must work seamlessly across geographical and organizational boundaries. In addition, the command and control (C2) of domains such as air, space, and cyberspace must be well integrated. The breadth and depth required for such innovation necessitates collaboration and cooperation including government, industry, and academia.

"The Department has determined it is appropriate for each Service to develop capabilities to conduct cyberspace operations. Improvements are needed in … C2 for cyberspace operations."[2]
~ Quadrennial Roles and Missions Review Report, January 2009

The Global Cyberspace Integration Center (GCIC) teams with major commands, joint and coalition partners, national agencies, industry and academia to develop, integrate and standardize air, space, and cyberspace components. The GCIC manages C2 innovation, experimentation and transition efforts including the Joint Expeditionary Force Experiment. The GCIC plans, programs, and guides enterprise-level capability-based planning, requirements, architectures, and integration of Air Force warfighting networks, combat support, and C2 systems. It also serves as lead command for tactical datalinks to include joint interoperability of tactical C2 systems, joint and coalition C2 interoperability data standards, air component information management, and satellite communication terminal management.

"The Defense Department intends to learn from the new, innovative capabilities and experiences of our counterparts across the US government, in the private sector, and internationally."[3]
~ Quadrennial Roles and Missions Review Report, January 2009

Building upon the success of Strategic Worldwide Integration Capability (SWIC), a previous GCIC-led C2 prototyping effort to improve global air operations collaboration and information sharing in support of 8th Air Force, the Air Force GCIC has undertaken an innovative Global Effects C2 effort. Leveraging partnerships and trust established with warfighters, industry, research labs, and acquisition centers through previous C2 efforts, the Air Force GCIC employs a proven collaborative concept development framework for refining concepts, requirements, and capabilities in helping reduce risks to full-scale acquisition programs.

"Greater integration of cyber … within the US government and with industry is necessary to better understand the requirements and effects of military operations in this domain. "[4]
~ Quadrennial Roles and Missions Review Report, January 2009

Initial phases of the Global Effects C2 (GEC2) Pilot have been working to demonstrate a more integrated air and cyberspace C2 environment. The foundation of the Global Effects C2 Pilot includes tools currently in use by theater warfighters. The tools, and associated processes, are being adapted to better support global information sharing, collaboration, and synchronization—independent of geographic boundaries and integrated across the air, space, and cyberspace domains.

"The Department seeks strategic, operational, and tactical cyberspace capabilities that provide … the ability to provide warfighting effects within and through the cyberspace domain that are synergistic with effects within other domains."[5]
~ Quadrennial Roles and Missions Review Report, January 2009

GEC2 activities are in full-swing. The GCIC has facilitated numerous warfighter analysis workshops (WAW) to facilitate GEC2 discussions aimed at defining requirements, developing concepts, and maturing tactics, techniques, and procedures. Requirements and concepts are aimed at integrating air, space, and cyberspace capabilities to plan, coordinate, and execute both kinetic and non-kinetic means to deliver integrated global effects at the strategic, operational, and tactical levels. While warfighters provide the primary input during WAWs, stakeholders from the research and acquisition communities also participate to provide a deeper understanding of the processes and requirements. In addition, the participation of technology providers such as industry and government laboratories allows immediate discussion regarding the "art of the possible" consistent with constraints such as time, funding, and manpower. The warfighter needs and pilot objectives are then allocated to specific technical solutions. GCIC negotiates with system program office and other technology providers to supply the prototype capability for each increment of the pilot. Additionally, GCIC formulates and manages the appropriate experimentation or risk reduction event to provide the appropriate environment for capability integration and assessment.

"Dominance of air, space, and cyberspace are of little use unless we achieve integrated domain control, … that is why scalable C2 capabilities across the spectrum of conflict is so important. ... All of us … have a duty to promote innovation."[6]
~ General Norton Schwartz, chief of staff, USAF

In the July 2008 initial risk reduction event, the GEC2 Pilot demonstrated the ability to merge strategic and theater strategies. In addition, web services for targeting and planning were demonstrated. Kinetic and non-kinetic targeting and planning were also integrated.

Two programs of record, The Joint Targeting Toolkit (JTT), developed by Air Force Research Laboratory's (AFRL) Information Directorate, and Project Suter System (PSS), developed by the Aeronautical System Center's Big Safari office, were employed for targeting tasks. These systems are employed today in operations centers to support targeting operations, but were initially designed before the widespread use of technology permitting net-centric global collaboration and information sharing. To achieve the GEC2 objective of integrating kinetic and non-kinetic effects, a Computer Network Operations Database (CNODB), a National Air and Space Intelligence Center (NASIC)-led initiative, was included for cyberspace targeting and planning. The CNODB provides a repository of potential cyber targets based on validated analysis. JTT and PSS are being adapted to interoperate as well as to access the CNODB through web services.

The Syzygy Interactive Network Visualization capability, provided as part of NASIC's CNODB, was used to provide analysts the ability to display associations and links between computer, social, military and political networks. The visualization of these relationships significantly enhanced target analysis and prioritization.

The SWIC was used by the Air Forces Strategic Command Air Operations Center to produce an integrated tasking order and attack plan matching prioritized targets with units responsible for execution. This cross-domain integration (e.g., air, space, and cyberspace) is one of the key GEC2 goals.

Later in 2008, the GEC2 Pilot team participated in the US Joint Forces Command (USJFCOM)-led Pirates Dagger cyber limited objective experiment (LOE). During this LOE, the demonstration was expanded to include initial execution and standalone assessment capabilities.

Operational assessment was conducted via AFRL Information Directorate's Advanced Capability for Understanding and Managing Effects Networks (ACUMEN) advanced technology demonstration (ATD). The ACUMEN capability is being enhanced to address cyber C2 requirements as a result of the first Cyber Applied Technology Council in July 2008. Measures of effectiveness are being developed to address integrated kinetic and non-kinetic operations. The information from this assessment will be fed back into the process to aid in the development of additional course of actions (COA) and re-planning.

"Cyberspace attacks involve significant potential for producing unexpected second- and third-order effects that might result in unintended and possibly undesired consequences."[7]
~ General Kevin Chilton, commander, US Strategic Command

Through collaboration with US Strategic Command and USJFCOM, the GEC2 results to date are helping to mature joint warfighting concept development. The GCIC is also collaborating with the science and technology community regarding further capability gaps discovered via the GEC2 Pilot. The refined requirements and concepts will help reduce risk to full-scale acquisition efforts aimed at delivering integrated C2 capabilities capable of addressing 21st century warfighter challenges.

"… the biggest thing is trying to keep up with the pace of change and the capabilities of our adversaries as well."[8]
~ Lt Gen William Shelton, chief of warfighting integration and chief information officer, Office of the Secretary of the Air Force

The GCIC plans to continue GEC2 into 2010. Activities are scheduled to include integration with combatant command/joint task force activities and additional analysis regarding global functional support to theater warfare. Specific efforts to be included in upcoming phases are improved COA generation, collateral damage estimation, battle damage assessment, and improved cyberspace visualization. Industry is encouraged to provide relevant technologies in these areas via the GCIC web site at http://www.gcic.af.mil/gcicinnovationsubmissionsite/index.asp.

Notes:

[1] General Kevin Chilton, commander, US Strategic Command, Air Force Association Conference, Orlando, Florida, 26 February 2009.

[2] Mr. Dennis C. Blair, director, National Intelligence, Hearing of the House permanent Select Committee on Intelligence, 25 February 2009.

[3] *Quadrennial Roles and Missions Review Report*, January 2009.

[4] Ibid.

[5] Ibid.

[6] General Norton Schwartz, chief of staff, Air Force Association Conference, Orlando Florida, 26 February 2009.

[7] General Kevin Chilton, commander, US Strategic Command, "Waging Deterrence in the Twenty-First Century," *Strategic Studies Quarterly* 3, no. 1 (Spring 2009).

[8] Lt Gen William Shelton, chief of warfighting integration and chief information officer, Office of the Secretary of the Air Force, Warfighting Integration Interview with Defense Systems, 3 March 2009.

Mr. John F. Vona (BS and MS, Electrical Engineering, Syracuse University, New York) is technical director and chief, Concepts and Technology Directorate, Air Force Global Cyberspace Integration Center (GCIC), Langley AFB, Virginia. As a Headquarter Air Force Field Operating Agency reporting to the Secretary of the Air Force, chief of warfighting integration and chief information officer, the center defines requirements, sets standards, identifies priorities, budgets and advocates for enterprise wide command and control (C2) capabilities. Mr. Vona oversees advanced concepts and technology initiatives, operational and technical analyses and assessments, technology transition planning, and defines future Department of Defense and Air Force experimentation strategies through leadership of the $28 million C2 constellation program. In addition, he works to guide and advocate for Department of Defense science and technology investment through collaboration with the Air Force Research Laboratory, other government laboratories, acquisition product centers, industry and academia. Mr. Vona serves as GCIC senior acquisition advisor.

Prior to assuming his current position, Mr. Vona served as the deputy technical director for the Air Force Command and Control, Intelligence, Surveillance and Reconnaissance Center, Langley AFB, Virginia. Mr. Vona spent sixteen years in various positions at the Air Force Research Laboratory, Information Directorate, Rome, New York.

Mr. Vona is a graduate of the Syracuse University Maxwell School of Government National Security Studies Program and Air University's Air War College

Clausewitz and Network Centric Warfare: A Beautiful Marriage

Lt Col Patrick Clowney, USAF
Action Officer
Pentagon, Washington DC

Since the dawn of the information age with its emphasis on the plaudits, principles, and propositions of technology, a great deal of speculation has surrounded the role of Carl von Clausewitz's genius in network centric warfare (NCW). NCW is an emerging theory of warfare in the information age that describes the combination of organizations, strategies, and emerging tactics, techniques, and procedures that a networked force can employ to create a decisive warfighting advantage.[1] Military genius refers to the "quick recognition of a truth that the mind would ordinarily miss or would perceive only after long study and reflection."[2] It also refers to what Clausewitz termed *coup d'oeil*, or the inward eye, intuition.[3] Cyber advocates and pundits speculate that the proliferation of open systems, spread of information sharing technologies, and growth of virtual-communal societies will abrogate the necessity for a military genius. On the other hand, more traditional military experts and analysts posit the essentially human nature of war; and the friction introduced by technology itself has not changed the nature of war, with the implication that Clausewitzian genius remains an important factor in military success. For these traditionalists, cyberspace, like air, space, land, and water, is just another medium that affects the changing character of war. Cyber advocates usually espouse the opposite point of view. Although theoretical arguments exist supporting and opposing the relevance of a military genius in NCW, this essay opines that since Clausewitz's rationale—complexity, uncertainty, and chance—for a military genius and the nature of warfare remain relevant and prevalent in NCW, the role of the military genius still deserves a prominent place in the annals of warfare.

Figure 1. Aggressors prowl for Air Force information. SrA Kyle Stackman (front) and Tech Sgt James Thoni with the Information Protection Operations office at Nellis Air Force Base, Nevada, monitor the base's computer network to keep it secure.

Clausewitz, Complexity, and Network Centric Warfare

The first reason espoused by Clausewitz for why a military genius is required that remains relevant to NCW is the complexity of war. He wrote, "any complex activity, if it is to be carried on with any degree of virtuosity, calls for appropriate gifts of intellect and temperament."[4] Complexity in this sense meant the infinite perturbations caused by the interactions of the variables affecting a war environment. Some of the variables included the very nature of war: the passions of the people, the play of chance and probability, and the instruments of policy.[5] As complexity remains relevant in NCW, a military genius is required to traverse a complex and perplexing environment.

In one sense, the capabilities offered by NCW may appear to assuage complexity and NCW does provide tools that help manage the informational complexity of modern war. However, cyber technologies and informational derivatives of those technologies introduce additional complexity, rather than a decline. An abridged consideration of the development of weaponry and types of war help illustrate this concept. In terms of weaponry, types of weapons have evolved from rocks to nuclear weapons. As the weaponry changed, so did the complexity of war. Commanders, be they cavemen or joint force commanders, had to deal with not only the traditional forms of warfare, but the implications of new weaponry. Their wars in effect became more complex. With respect to the types of warfare, as humanity and weaponry have evolved, so has the type of warfare. During Clausewitz's time, attritional warfare was the predominate type of war, and Clausewitz was surely referring to this type in his pronouncements on complexity. However, as man and machine evolved, the character of warfare became more complex. For example, the Department of Defense has a spectrum of warfare that spans from low intensity conflict to conventional warfare. These multiple forms add to the complexity of war and commanders must be versed in all. NCW, like all evolutions or revolutions in warfare, adds to this complexity.

Paul T. Mitchell presents further insights into the growth of complexities surrounding NCW. Mitchell writes that "NCW is changing how militaries operate in both battle and in operations other than war, and that the sharing of information can only grow in importance as armed forces continue their never-ending quest for a competitive advantage."[6] These changes add to the complexity of war. Mitchell also highlights the complexities associated with coalition operations in NCW. He argues that states will continue to share information amongst them, but perfect transparency will be impossible.[7] Information is simply too central to the competitive advantages offered by NCW to be jeopardized by automatic disclosure.[8] Dr. Martin C. Libicki also

Figure 2. SrA Ricardo Reveles and A1C Sven Bickham install an antenna and align a satellite dish for the best signal.

adds, "the increasingly complex demands being made on and largely accommodated by information systems," make the information systems more complex. The robustness of information often produces more noise into the decision making process.[9] As a result, the mechanisms to filter become more complex and important. The dictates of sovereignty, noise, and comparative advantage ensures that seamless command interoperability will remain an issue, ensuring further complexity in war.[10] As such, a military genius is required to navigate the complex environment.

Clausewitz propounded that the complexities of war merit the attributes of a military genius. The history of technology and the derivatives of NCW suggest that complexity remains prevalent in NCW. Because of this complexity, the military genius is still required to employ NCW within the arena of warfare.

Clausewitz, Uncertainty, and Network Centric Warfare

Closely related to complexity, Clausewitz also offered the idea of uncertainty in war as another reason for needing a military genius. He stated that war operates in the realm of uncertainty. He estimated that "three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty."[11] Because of uncertainty, "a sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth."[12] Clausewitz identified two factors that contribute to a constant uncertainty in war—the impossibility of calculating moral forces and the interaction of humans at all levels.[13] Advocates of NCW often assert that NCW technologies and the free flow of information decreases uncertainty in war. However, like complexity, tangible and intangible uncertainties may actually increase in NCW. Therefore, a military genius is still required to mitigate uncertainties in war.

Michael I. Handel in *Masters of War* addresses the relationship between uncertainty and military genius and adds support to the necessity of a military genius in NCW. Handel writes that many military experts writing on NCW often imply that war has transformed into a rationale activity based on perfect or near perfect information.[14] These experts also claim vast amounts of information make war highly predictable.[15] However, Handel also identifies the fallacy of this logic, based on a desire to identify laws or principles of war when in fact the conduct of war is a situational dependent art.[16] On this concept and the critique of those attempting to apply hard science to war, Clausewitz said, "Efforts were … made to equip the conduct of war with principles, rules, or even systems. They did present a positive goal, but people failed to take adequate account of the endless complexities involved … the conduct of war branches out in almost all directions and has no definite limits: while any scientific system, any model has the finite nature of a synthesis."[17] Uncovering the manifestations of Clausewitz's uncertainties in NCW illuminates the necessity for a military genius.

The unpredictability of human nature that leads to uncertainty will remain present in NCW. Inherent in the cyber medium are humans; they are involved in every level of NCW. From controlling unmanned flying intelligence, surveillance, reconnaissance platforms to filtering the mounds of information from various nodes, humans control NCW. Although computers have the capacity to help humans interpret data and make complex decisions, a human remains the deciding factor. Furthermore, as artificial intelligence becomes more reliable, Seth Lloyd hypothesizes that computer-based decision will exhibit or approach the unpredictability of humans.[18]

Moreover, the unpredictability introduced by humans can be a source of good decisions. For example, many businesses seek inputs via wiki-sites. The goal is to encourage collaboration to produce better products.[19] In many cases, the businesses have gleaned ideas that have produced better products. The belief,

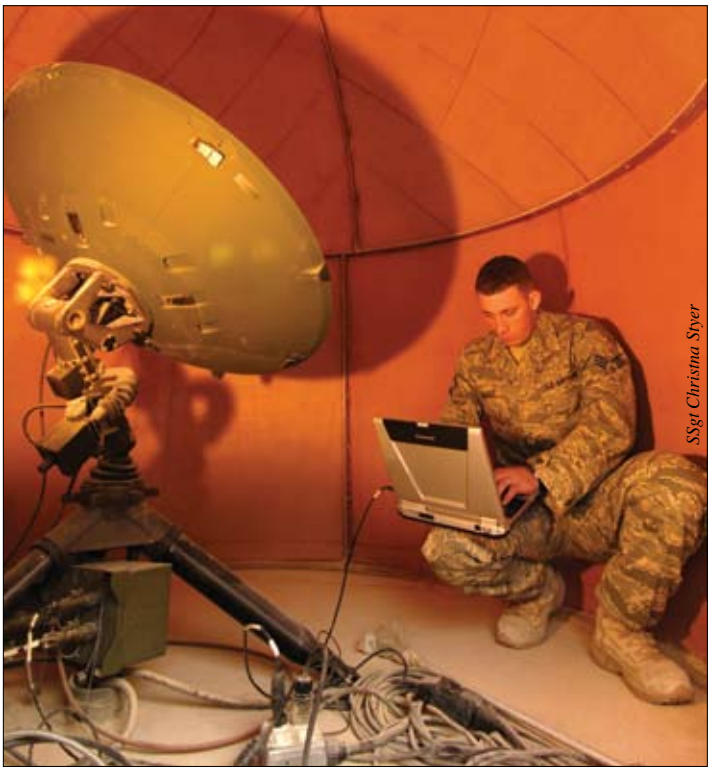


Figure 3. Keeping the information flowing. SrA Sean Reuter, a network systems technician, reacquires the Global Broadcast System, which is part of keeping uninterrupted flow of information streaming to decision makers in the Combined Air Operations Center.

following the logic of genetic diversity, is that this free flow of information creates a diversity of ideas from which companies can derive a better product. However, despite this free flow of information, a human still makes the decision on which information is applicable to the ultimate product. Although many solutions may exist, a human decides the best course of action.

In NCW, this same logic still applies. Technologies afford commanders and decision-makers unprecedented situational awareness of the battlefield and a plethora of information. With exposure to so much information that is rooted in morale and unpredictable human forces, the commander's ability to decipher, feel, and predict outcomes becomes more imperative. As John Ferris and Michael I. Handel declare, this uncertainty attributed to human nature is the condition when military genius reveals itself.[20] Therefore, whether computers or humans are making decisions, unpredictability will remain present. A military genius is required to deal with this uncertainty.

In NCW, uncertainty can manifest in humans and technology. The technologies and information sharing associated with NCW may well produce benefits that will speed the decision cycle of the commander. However, it is unrealistic to assume that perfect information will always be available and negate the need for a military genius. On the contrary, history suggests the proliferation of technology will likely require a commander, a military genius, who has the acumen to amalgamate the strengths of NCW along with other tools and facets of warfare to develop a cogent strategy.

Clausewitz, Chance, and Network Centric Warfare

Along with complexity and uncertainty, chance also played a huge role in Clausewitz's rationale for a military genius. He wrote, "war is the realm of chance."[21] He further amplified his thoughts on chance: "No other human activity gives it greater scope; no other has such incessant and varied dealings with the intruder."[22] "Chance makes everything more uncertain and interferes with the whole course of events."[23] Therefore, since all information and assumptions are open to doubt and with chance everywhere, a commander continually finds things not as expected.[24] NCW will not change this.

Before delving into the relationship between chance and NCW, it is imperative to define what Clausewitz meant by chance. Clausewitz never explicitly defines chance in *On War*, but he addresses three forms of chance. Alan D. Beyerchen, professor of military history at Ohio State, offers that chance is a stochastic phenomenon, since Clausewitz repeatedly stresses the nexus between politics and war.[25] The second form of chance is the amplifications of unknown causes that tie chance and friction together in the inevitable confusion of war.[26] The third is the tendency of humans to configure a chaotic war into manageable pieces and then perceive as chance the interactions of those configurations.[27] All three aspects of chance can be expected in NCW.

Like in all forms of war, the elements of chance remain relevant in NCW. With regard to the nexus between politics and war, the commander will have to contend with the capricious nature of policy. For example, a commander developing a war strategy based on policy may prefer to attack the infrastructure

Figure 4. Tower-climbing certification. SrA Lakendrick Fisher climbs up a Radio-over-Internet Protocol Routed network tower.

of an adversary through cyberspace in order to cajole an adversary without kinetic means. However, policymakers may prefer a kinetic strike as well as a cyber attack. In this instance, the chasm between policy and strategy has introduced chance. In these instances, a military genius is required to possess the flexibility to account for chance, adapt a military strategy in accordance with policy, and fuse the policy-strategy fissure. With respect to undetectable causes producing chance, NCW has many. Seth Lloyd's theories on computer science and entropy help illustrate this concept. Lloyd, borrowing from Second Law of Thermodynamics, postulates that the information takes on the properties of entropy—a continuous proliferation of unknown information interacting with itself.[28] Although the interactions may produce plausible solutions to real problems, they may also introduce more chaos into a system.[29] As chaos, or undetectable causes increase, so can chance. In such an environment rife with chance, the intuition of military genius is required to deal with chance. The last aspect of chance, the tendency to put the pieces of war into preconceived boxes, bears consideration. Lonsdale and others argue that NCW is based on the preconception of a static rather than a reactive enemy, or they fail to consider the enemy's reactions to NCW. As Dr. Everett C. Dolman notes, true strategy is about derivative moves in response to the first move and subsequent moves.[30] Every concept of how to fight wars carries its own preconceptions. Each interaction in war

between adversaries is unique unto itself and that uniqueness fosters a dynamic strategic environment. As Libicki remarks, "information operators must first understand the enemy's command and control system that would give them some feel for what the dysfunctional coping strategies might be."[31] NCW, like all forms of warfare, fits this pattern. The complexity and uncertainty discussions earlier illuminate these points. However, the predilection of some NCW theorists may well introduce chance in NCW. Consequently, a military genius is required for such an environment.

Given Clausewitz's assertions on chance, a military genius still appears a requisite for warfare. No matter how chance manifests, a commander with intuition appears necessary. The NCW environment promises to pose many of the same concerns and risks as traditional warfare. A military genius is required to lessen the negative impacts of chance.

Conclusion

Clausewitz's concept of a military genius is applicable to NCW. Clausewitz's rationale—complexity, uncertainty, and chance—are present in NCW as it is to all forms of war. Sir Michael Howard provided credence to these assertions. He stated the technological dimension of strategy is but one amongst four; operational, social, and logistical are the others.[32] Howard argues the relative dominance of each dimension is dependant upon circumstance.[33] In other words, the degree to which the technological capabilities of NCW will be a deciding factor in a given conflict depends on the chance and uncertainty of emerging situations as well as the complex interaction of technology with other aspects of warfighting. A military genius is thus required to navigate, adapt, and think in a mercurial environment of which NCW is but a small part.

Notes:

[1] Department of Defense, *The Implementation of Network Centric Warfare* (Washington, DC: Office of Director, Force Transformation, March 2005), 3.

[2] Carl von Clausewitz, Michael Eliot Howard, and Peter Paret, *On War*, ed. rev. (Princeton, NJ: Princeton University Press, 1984), 102.

[3] Ibid.

[4] Clausewitz, 100.

[5] Clausewitz, 89.

[6] Paul T. Mitchell and International Institute for Strategic Studies, *Network Centric Warfare: Coalition Operations in the Age of Us Military Primacy* (London: International Institute for Strategic Studies, 2006); Clausewitz et al., *On War*.

[7] Ibid., 52.

[8] Ibid.

[9] Martin C. Libicki and Rand Corporation, *Conquest in Cyberspace : National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007).

[10] Ibid.

[11] Clausewitz, 102.

[12] Clausewitz, 101.

[13] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, Cass Series—Strategy and History, 9 (London ; New York: Frank Cass, 2004).

[14] Michael I. Handel, *Masters of War: Classical Strategic Thought*, 3rd rev. and expanded ed. (London; Portland, OR: F. Cass, 2001).

[15] Ibid.

[16] Ibid.

[17] Clausewitz, 134.

[18] Seth Lloyd, *Programming the Universe : A Quantum Computer Scientist Takes on the Cosmos*, 1st ed. (New York: Knopf, 2006), 37.

[19] Don Tapscott and Anthony D. Williams, *Wikinomics: How Mass Collaboration Changes Everything* (New York: Portfolio, 2006).

[20] John Ferris and Michael I. Handel, "Clausewitz, Intelligence, Uncertainty and the Art of Command in Military Operations," *Intelligence and National Security* 10, no. 1 (1995): 1-4.

[21] Clausewitz, 101.

[22] Ibid.

[23] Ibid.

[24] Ibid., 102.

[25] Alan Beyerchen, "Clausewitz, Nonlinearity and the Unpredictability of War," *International Security* 17, no. 3 (Winter, 1992): 59-90. Copyright 1993 by the president and fellows of Harvard College and the Massachusetts Institute of Technology. Reprinted as ppendix 1 in Tom Czerwinski, *Coping With the Bounds: Speculations on Nonlinearity in Military Affairs* (Washington, DC: National Defense University, 1998) http://www.ndu.edu/inss/books/books%20201998/Complexity,%20Global%20Politics%20and%20Nat'l%20Sec%20-%20Sept%2098/ch07.html.

[26] Ibid.

[27] Ibid.

[28] Lloyd, *Programming the Universe,* 76.

[29] Ibid.

[30] This assertion was taken from class notes from lectures performed by Dr. Everett C. Dolman in a Coercion class in October 2007 at the School of Advanced Air and Space Studies, Maxwell AFB, AL.

[31] Libicki, 54.

[32] Lonsdale, 5.

[33] Ibid.

Lt Col Patrick Clowney (BS, Engineering Science, USAFA; MPA, University of Oklahoma; MA, Organizational Behavior, The George Washington University) is an action officer assigned to the Pentagon. He entered the Air Force in 1994 after graduating from the United States Air Force Academy. He earned his Navigator wings from Joint Specialized Undergraduate Navigator Training at Randolph AFB, Texas. Following navigator training, he was assigned to fly the RC-135S and WC-135 at Offutt AFB, Nebraska.

Colonel Clowney transitioned to the AC-130H in June 2001. He served as a mission commander for AC-130 operations during Operation Enduring Freedom and as chief of Future Operations, Combined Joint Special Operations Air Component Command during Operation Iraqi Freedom. Colonel Clowney has also commanded at the flight level.

Colonel Clowney is a former Air Force intern where he served in the Office of the Deputy Secretary of Defense and in the Office of the Secretary of the Air Force International Affairs Weapons Division. He is a senior navigator with more than 1,700 flying hours, including over 200 combat hours during Operation Enduring Freedom.

Among his many awards, Colonel Clowney has been awarded the Meritorious Service Medal with one Oak Leaf Cluster, Air Medal with three Oak Leaf Clusters, and the Air Achievement Medal. He is a resident graduate of the Squadron Officer School, Naval Command and Staff College, and the School of Advanced Air and Space Studies.

Protecting Our Most-Powerful Weapon System: Information

Ms. Linda R. Gooden
Executive Vice President
Lockheed Martin
Information Systems and Global Services
Gaithersburg, Maryland

When military leaders and defense experts began several years ago at the dawn of the information age to assert that information is America's most powerful weapon system, many people scratched their heads. How can a long series of 0's and 1's be more powerful than an intercontinental ballistic missile or a squadron of fighter jets?

Today, of course, there are few who would question the value of timely, accurate, and reliable information that can be packaged, transmitted, and manipulated with lightning-fast agility. It's the lifeblood of virtually every enterprise, from large corporations managing multinational operations to individuals managing a household budget. For the military, digital information is the ultimate force multiplier. It delivers real-time situational awareness from the command level down to individual weapons platforms, and it enables the translation of that awareness into effective action. The ability of a commander to see in real time the position and status of his assets—as well as his enemy's—and the ability of a warfighter to know with assurance what's around the next corner or behind the next mountain is simply invaluable.

If digital information has become the lifeblood of our national defense, the body through which it flows is cyberspace—the Global Information Grid (GIG). Increasingly the architecture of cyberspace exists in real space: the satellites and supporting ground stations through which much of global data transmission must at some point pass. That's why the Air Force Space Command (AFSPC) is uniquely positioned to carry out the Air Force's cyberspace mission and present cyber forces to the joint warfighting commander at US Strategic Command (USSTRATCOM). It's also why AFSPC will play a vital role as a component of STRATCOM's Joint Task Force–Global Network Operations (JTF-GNO), bringing unique perspective into the management of the network, information flow across the network, and information assurance and network protection.

At Lockheed Martin, we also appreciate the critical link between space and cyberspace. We design, build, and operate spacecraft and the technology they carry. In addition, we are the largest provider of information technology to the federal government, and we assist the Department of Defense in developing netcentricity concepts and designing network solutions.

From these many vantage points, we have observed not only the tremendous capabilities brought by the growth of the GIG, but also the serious challenges involved in protecting it. A report from the Commission on Cyber Security for the 44th Presidency in December 2008 reveals: "Cyber security is now one of the major national security problems facing the United States."

Cyber threats come from many sources. Some are state-sponsored attempts to steal classified information and intellectual property. Some are initiated by military enemies to thwart operations and gain a tactical advantage. Some are criminal attempts to gain personal information for identity theft. And still others are simply attacks perpetrated by malcontents bent on causing damage and disruption.

The US military faces every one of these threats and at a greater level of intensity than any other target. That's nothing new, of course. Cyber defense was the original reason behind the formation of JTF-GNO's heritage organization in 1999. What's new is the sophistication of today's cyber threats and the stealth nature of the attacks.

Recognizing the escalation of the threat to our military, civil, and commercial customers, Lockheed Martin recently established a Center for Cyber Security Innovation led by Lee Hol-

Figure 1. Cyber Security – ensuring mission resilience.

Cyber security must consist of holistic, end-to-end solutions capable of detecting an attack anywhere around the globe and immediately responding to drive out the intruder.

comb, former chief technology officer for the US Department of Homeland Security, with strategic support from retired US Air Force Lt Gen Charles Croom. The purpose of our initiative is to return the advantage in the cyber security race to the defenders rather than the attackers. In recent years, attackers have become much more effective at breaking into networks and carrying out their work undetected. No longer is it sufficient to patch vulnerabilities to known threats and monitor network traffic in search of unusual data flows. Too often, a network operator does not realize an attack has occurred and data has been compromised until the event is over.

The answer is to design cyber security solutions that not only detect rapidly and respond aggressively but also to look across cyberspace for threat activity and predict how nascent attacks will behave. We need to prevent rather than react, and the tool we will use to do that is technology itself. We are currently pursuing solutions that enable cyber assets to respond automatically to block vulnerabilities and cascade defenses from machine to machine, locking down the network to a trusted state until security is assured and full systems capability is restored.

These types of solutions are not easy to design or to implement, especially across a network of the size, complexity, and importance of the GIG. But they can and must be developed. We can no longer rely on traditional "point" solutions that aim to protect an end user's computer or a particular network device. Cyber security must consist of holistic, end-to-end solutions capable of detecting an attack anywhere around the globe and immediately responding to drive out the intruder. These solutions must be designed into our systems as an integral part of the network itself, rather than as a system add-on. At Lockheed Martin, we are implementing this approach in all of our business units. We are requiring every product development effort to incorporate cyber security from the earliest stages of design. We are sharing best practices across the corporation. And we are conducting netcentric exercises in cyber defense using our innovation centers, such as the Center for Innovation in Suffolk, Virginia, and a newly constructed technology center complete with cyber range opening in Maryland later this year. The imperative nature of effective cyber defense goes beyond protecting resources and preserving a tactical advantage. It goes to the heart of the value of information itself.

Ultimately, information is useful only when the user has absolute faith in its integrity. Soldiers about to turn the corner of a building do not know or care that the information they are receiving has passed through multiple networks and was relayed by the world's most sophisticated satellites. They only care that it's accurate. Their lives depend on it. Providing these warfighters with that assurance is a responsibility that AFSPC can be proud to own.

Ms. Linda Gooden (BS, Computer Technology, Youngstown State University; BS, Business Administration, University of Maryland University College) is executive vice president of Lockheed Martin's Information Systems and Global Services (IS&GS) business area and an officer of Lockheed Martin Corporation. Under her leadership, IS&GS includes 54,000 experienced professionals who provide integrated information technology solutions, systems and services to support worldwide missions of civil, defense, intelligence, and other government customers. Established in February 2007 as one of four principal business areas within Lockheed Martin, IS&GS generated $11.6 billion in sales in 2008. Headquartered in Gaithersburg, Maryland IS&GS operates in all 50 US states and about 60 countries around the world.

Ms. Gooden actively supports professional, academic, and civic organizations, serving on numerous executive boards including Eisenhower Fellowships Board of Trustees; Armed Forces Communications and Electronics Association International; Information Technology Association of America; University of Maryland's A. James Clark School of Engineering; University of Maryland, Baltimore; and Prince George's Community College Foundation. She also serves on the Board of Directors for ADP, Inc.

In 2008, Ms. Gooden was inducted into the Maryland Business Hall of Fame and named to Corporate Board Member magazine's Top 50 Women in Technology. She was selected in 2007 as Executive of the Year by the Greater Washington Government Contractor Awards and in 2006 as Black Engineer of the Year by US Black Engineer and *Information Technology* magazine. Ms. Gooden was featured as one of *Black Enterprise* magazine's 100 Most Powerful Executives in Corporate America for 2009. She won *Federal Computer Week's* 2002 Federal 100 "Eagle" Award and received Women in Technology's 2002 Corporate Leadership Award.

Prior to assuming her current role, Ms. Gooden was executive vice president of Lockheed Martin's Information Technology and Global Services business area, and before that she was president of Lockheed Martin Information Technology, a business unit she grew over 10 years to become a multibillion dollar business. She was vice president of Lockheed Martin's Software Support Services unit from 1994 and earlier held other positions of increasing responsibility.

In 2005, she was awarded an honorary Doctor of Public Service degree from the University of Maryland University College in recognition of her service to the community and to higher education. She successfully completed the Executive Program Manager course at the Defense Systems Management College in 1998.

Year of Leadership

CMSgt Richard T. Small, USAF
Command Chief, Air Force Space Command
Peterson AFB, Colorado

Leadership is the foundation on which the Air Force and Air Force Space Command (AFSPC) achieve success in every mission area. Experience teaches us that the quality of tomorrow's leaders depends on the effectiveness of the training we provide today. In our profession—the profession of arms—training and education are force multipliers that benefit individual Airmen, their organizations, and the Air Force.

From September 2008 through August 2009, AFSPC is focusing on the critical role our leaders play in executing the command's missions. Under the banner, "Year of Leadership," we are conducting activities that emphasize important leadership attributes and traits, improve leadership focus, enhance leadership skills, and increase leadership interaction with those we lead.

Why a Year of Leadership?

We live in a complex world with complex security risks. Our nation, our allies, and our friends rely on us to guarantee a safe, secure and combat ready force with an unwavering commitment to excellence and the highest possible standards. The Air Force is an excellent organization, globally renowned for having the most deliberate and effective programs and leaders to create mission success. Along with our joint partners, America's Airmen protect the nation's security. AFSPC is and must remain committed to leading the way by leveraging its greatest asset–its leaders–to guarantee mission success.

In every organization—military or civilian, public or private—success rises or falls on one fundamental element … and that element is leadership. From the intercontinental ballistic missile force—the ultimate backstop to our national security—to the global positioning system, our Airmen operate space capabilities vital to national security, economic growth, and public safety. These capabilities serve joint forces, the nation, and the world at large … shaping America's approach to warfare. To that end, leaders at every level must accept responsibility, take ownership, enforce standards, and demand accountability. They must also be hands-on leaders. Our Airmen deserve resources and the best leadership we can provide them to meet our standards. We must set them up for success.

Figure 1. Air Force Space Command, Year of Leadership.

For us, perfection remains our standard. We clearly understand the awesome responsibility that comes with the global impact of our missions. We also must understand that, as leaders, the manner in which we perform our duties not only impacts the daily operations of the unit, but the mission readiness of the command and the Air Force. In fact, the influence of a single leader will cascade across generations of Airmen impacting those who serve today and influencing the way in which they will lead our Air Force in the future.

Whether reinvigorating the nuclear enterprise or activating the Air Force's first numbered air force focused on the cyberspace warfighting domain, we are facing a number of challenges that require positive leadership at all levels. "Hands on" leaders who set the appropriate tone and establish the proper way forward can best address these challenges. While net-centric tools can help us guide and direct actions or manage processes, information technology will never supplant nor suffice for face-to-face leadership. Leadership remains a "contact sport."

What is the Year of Leadership?

AFSPC's "Year of Leadership" blends a variety of initiatives and events together to enhance awareness and understanding of the roles and responsibilities of leaders. We have dedicated 12 full months to focus on leadership across the command to:

- Reinvigorate leaders' commitment to the Air Force as a profession and way of life, not as a job … living our core values—Integrity First, Service Before Self, and Excellence In All We Do—regardless of rank, location, or echelon of assignment
- Emphasize the importance of standards … setting them, leading by them, living them, holding ourselves, and our fellow Airmen accountable to them … being the example all Airmen—enlisted, officer, and civilian—strive to emulate
- Foster leadership with a warrior mindset—knowing the criticality of our global mission and the impact we have both on the fight we are in and the fight we deter
- Insist on excellence—at all times—and demand a positive self-assessment culture that identifies problems and gets to root causes
- Encourage speaking up … not walking past failures or letting growing problems worsen … fixing them or getting the attention of those who can

- Emphasize developing and maintaining a professional attitude—supporting downward-directed policies
- Facilitate hands-on leadership … getting leaders out from behind the desk and into the work centers and the field
- Put leaders out front during physical training, thus leading our people to increased levels of fitness and enhanced esprit de corps … fitness is a force multiplier for mission readiness and individual well-being
- Cultivate increased awareness of importance of taking action on personal and professional needs and issues for Airmen and their families
- Promote leading beyond the work center ... getting involved in unit, base, and local community activities
- Highlight the need to invest quality time developing and furthering careers of deserving subordinates … from performance evaluations to award submissions to performance feedback
- Expand professional development and inspire continuous self-improvement through educational and developmental opportunities … technical, functional, academic, and professional
- Encourage confidence when making tough calls evaluating subordinates, delivering bad news or when facing a hard issue
- Enhance AFSPC's leadership role through engagement beyond the fence line with professional civic and military associations and organizations
- Articulate the history, heritage and mission of AFSPC and the Air Force … educate Airmen to do the same and ensure understanding of the priorities of unit leaders and the command
- Accentuate "An American Airman First" … reminding the command's Airmen that they are the *Guardians of the High Frontier*

Figure 2. Year of Leadership. The sustainment, growth, and health of all organizations - civilian or military - rise and fall on one fundamental factor: Leadership.

Figure 3. Change in curriculum. A1C Michael Fuerte, left, and David Reynolds, technical school students at the 532nd Training Squadron, Vandenberg AFB, conduct hands-on training for the environmental control system of a missile launch facility.

As a road map to achieving these goals, each of the 12 months is focused on an important topic, trait, or aspect of leadership: back to basics, discipline, core values, compassion, followership, and so forth. Commanders develop a schedule of events, activities, and leadership encounter opportunities tailored to each month's focus area. Further, commanders were provided a list of actions around which they could structure their local efforts, such as:

- Designating one day per week to facilitate, encourage, and accommodate work center level leadership encounters by de-emphasizing e-mail, computer-based activities, and scheduled meetings.
- Leading and encouraging work center, unit and/or field visits with a focus on personal and first-person interaction, including 24-hour work centers or outlying/remote locations
- Establishing periodic and recurring leadership encounters with professional military organizations/associations, such as company grade officers (CGO) council, chiefs group, first sergeants council, top three association, mid-tier noncommissioned officer (NCO) association, Airman's councils, civilian workforce forums, and so forth.
- Implementing warrior fitness/formation runs to demonstrate support for physical fitness, enhance unit esprit de corps, and engage with Airmen outside work centers; monthly competitive warrior run to encourage increased fitness; biannual (or annual) non-competitive numbered air force/center/wing run by echelon with unit flags/guidons to bolster esprit de corps
- Encouraging guest speakers at Airman Leadership School graduations, First Term Airmen Center (FTAC) completion ceremonies, quarterly/annual awards banquets, and so forth, to tailor speeches/messages to "Year of Leadership" focus areas
- Ensuring supervisors attend/participate in completion ceremonies for Airmen completing FTAC
- Integrating CGOs into portions of senior noncom-

missioned officer (SNCO) professional development courses

- Offering representatives from professional military organizations or associations (CGO council, chiefs group, first sergeants council, top three association, mid-tier NCO association, Airman's council) the opportunity to attend wing/installation staff meetings
- Establishing leadership encounter opportunities, particularly for Airmen (E-4 and below), such as an "Airman's Night" focused on junior enlisted Airmen, organized by mid-tier NCO association
- Developing a "shadow" program where junior personnel can spend time with senior leaders to observe them in leadership roles
- Establishing a force development council comprised of leaders from professional military organizations or associations to identify, facilitate, and encourage professional and leadership development

The command headquarters staff engaged to support field commanders in executing the "Year of Leadership." Headquarters (HQ) AFSPC Public Affairs helped kickstart the effort with an initial commander's video underscoring the importance of the initiative and produces each month a "Leadership in Focus" video consistent with the monthly focus area. Headquarters AFSPC Manpower, Personnel, and Services (A1) is reviving and revising the command's "Vigilant Look" program. The revised course will target CGOs, mid-grade NCOs and civilian equivalents with a week-long professional development opportunity focused on improving and enhancing the understanding of the command's missions and challenges. The first session is currently scheduled for August 2009.

Along with each installation's career assistance advisor, HQ AFSPC/A1 completed a top-to-bottom review of the command's professional development programs at the NCO and SNCO levels. The focus of this review was to ensure these programs are properly focused and provide the scope of instruction appropriate for each level of leadership development. As a result, we are implementing standardized lessons plans for NCO and SNCO professional development courses. In recognition of the synergy to be gained from integrating CGOs into SNCO professional development, each SNCO program will have a "Leadership Team Day." This portion of the course will team CGOs and SNCOs during presentations/discussion on topics such as standards, promotions, counseling and mentoring.

Figure 4. General C. Robert Kehler, commander of Air Force Space Command, talks to Airmen during a field training exercise.

Some installations have recruited senior mentors in support of their programs. General Ron Fogelman, USAF, retired former Air Force chief of staff (CSAF), discussed core values in a packed auditorium at Peterson AFB, Colorado. General Fogelman shared his unique perspective on the topic, as he was the CSAF when the Air Force codified its core values. Schriever AFB, Colorado Airmen benefitted from the experience of Chief Master Sergeant of the Air Force Sam E. Parish, retired as he led them in a discussion on the importance of followership. From leadership discussions in our squadron commander's course to being the theme for the command's annual Airmen of the year awards program, we have leveraged the "Year of Leadership" at every turn to inform our leaders of the critical role they play in mission success and inspire them to higher levels of achievement.

These are just a few examples from countless others which illustrate the importance and impact of the "Year of Leadership." By embracing this effort and applying it to the entire team, the activities and actions are proving to be a key to unlock our best leadership skills and techniques. In the words of one of our youngest Airmen, this effort has "raised the leadership bar in AFSPC."

CMSgt Richard T. Small (AAS, Administrative Management and Personnel Administration, Community College of the Air Force, Alabama; AA, Management Studies, University of Maryland; BA, Human Resource Administration, Saint Leo College, Florida; MPA, Personnel Management, Troy State University, Alabama) is the command chief master sergeant, Air Force Space Command, Peterson AFB, Colorado. Air Force Space Command is responsible for the development, acquisition, and operation of the Air Force's space and missile systems. The command oversees a global network of satellite command and control, communications, missile warning and launch facilities, and ensures the combat readiness of America's intercontinental ballistic missile force. Chief Small is responsible to the commander for the professional development, military readiness, and mission effectiveness of the command's enlisted Airmen assigned to 160 units in more than 48 locations across the globe.

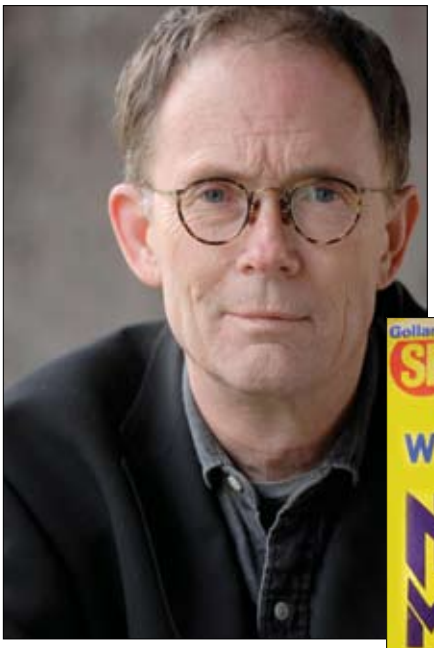
Chief Small entered the Air Force in October 1983, and is a native of Kershaw, South Carolina. He has served in a variety of progressively responsible positions at every echelon from squadron to Headquarters Air Force, as well as the diplomatic staff of the American Embassy in Sarajevo, Bosnia-Herzegovina. He has significant multinational, coalition, Joint service and interagency experience in support of Operations Southern Watch, Joint Forge, Allied Force, Enduring Freedom, and Iraqi Freedom. He served as the first permanent party command chief for the 379th Air Expeditionary Wing and deployed with special operations forces as command chief for the Combined/Joint Special Operations Air Component.

Cyberspace: An Etymological and Historical Odyssey

Dr. Rick W. Sturdevant
Deputy Command Historian
HQ AFSPC History Office
Peterson AFB, Colorado

In the beginning was the word, and the word was "cyberspace." Or, was it? Just days after Air Force Space Command (AFSPC) became the service's focal point for the cyberspace mission in October 2008, General C. Robert Kehler, AFSPC commander, talked about the importance of defining the domain and its pedigree as a first step toward understanding precisely what the Air Force was asking AFSPC to do in cyberspace. His remarks prompted AFSPC historians to wonder about the origin of the word "cyberspace" and its journey into the vocabulary of the United States Air Force (USAF).

Science-fiction writer William Gibson conceived "cyberspace" as a completely new word and shared it in print for the first time in "Burning Chrome," his short story in the July 1982 issue of *OMNI* magazine. He referred to a matrix-simulator console as the "Cyberspace Seven" (p. 72). Although he used "cyberspace" only once in that composition, he liked the word enough to use it more than twenty times in his prize-winning 1984 novel *Neuromancer*. A synonym for "the matrix" or "grid," which Gibson characterized as rooted "in early graphics programs and military experimentation with cranial jacks," cyberspace was "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts … A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data" (p. 69). Popularization of "cyberspace" began with record sales of *Neuromancer* and Gibson's publication of two additional novels—*Count Zero* (1986) and *Mona Lisa Overdrive* (1988)—to complete what became known as the "Sprawl trilogy."



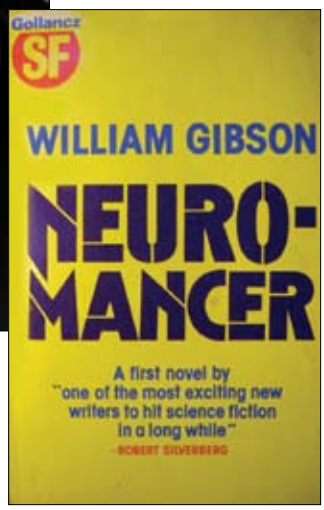


Figure 1 and 2. William Gibson coined the word "cyberspace" in 1982; The first hardback version of Neuromancer was published later in 1984 in the United Kingdom.

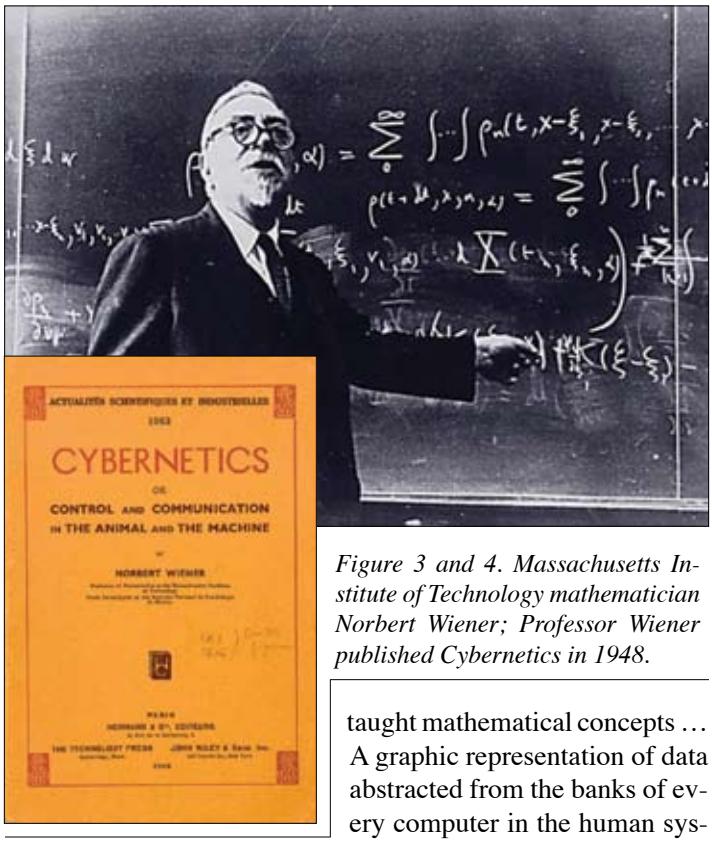


Figure 3 and 4. Massachusetts Institute of Technology mathematician Norbert Wiener; Professor Wiener published Cybernetics in 1948.

In the 2000 documentary film *No Maps for These Territories*, Gibson said he coined "cyberspace" because "it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page." He did not foresee that a word he intended as nothing more than a metaphor would become a ubiquitous descriptor for the ever-changing domain created, and constantly recreated, by people all over the world communicating via the Internet and other electronic means.

Although Gibson discounted semantics when it came to "cyberspace," it almost certainly is a condensation of two separate words that also appear in *Neuromancer*: "cybernetics" and "space." Stemming from the Greek Κυβερνήτης (kybernētēs, steersman, governor, pilot, or rudder), which Plato first used in the context of governing people, "cybernetics" emerged in the 1940s as an interdisciplinary field of study involving the struc-

… people of the Western World have conceptualized space in different ways—sometimes in physical terms, sometimes nonphysical, and often in a combination of physical and nonphysical dimensions.

ture of so-called "information feedback" or regulatory systems. The first person to use the term in this latter sense was Massachusetts Institute of Technology mathematician Norbert Wiener, who worked during World War II on guided missile technology and studied how the feedback principle allowed sophisticated electronics to control a missile's flight path. He subsequently observed how plants and animals employ the feedback principle to change their actions in response to their environment, which led him to introduce the neologism "cybernetics" into his emerging scientific theory. On 22 October 1948, Wiener popularized the term with publication of his book *Cybernetics, or Control and Communication in the Animal and the Machine*. Wiener's work would significantly influence how technologists later perceived human-computer interfaces.

As for the second half of "cyberspace," etymologists trace derivation of the English word "space" back through the Old French "espace" to the Latin word "spatium" (interval, extent, area, or expanse). Historically, from medieval times to the present, from Dante Alighieri's *The Divine Comedy* to William Gibson's *Neuromancer*, people of the Western World have conceptualized space in different ways—sometimes in physical terms, sometimes nonphysical, and often in a combination of physical and nonphysical dimensions. For example, science writer Margaret Wertheim, in her book *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet*, categorized cyberspace as a communally shared network of physical and logical relationships (p. 303). She perceived both outer space and cyberspace as "mediated" spaces, because both are realms "we know only through 'virtual eyes'"—domains we cannot experience except "through a technological filter" (p. 143).

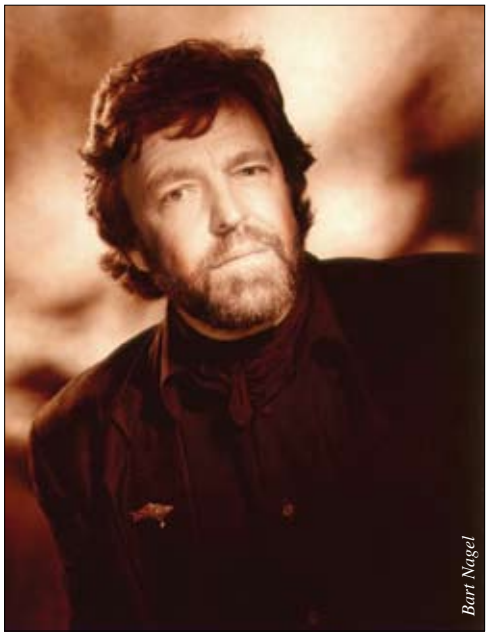


Figure 5. John Perry Barlow applied "cyberspace" to the space created by Internet users.

Credit for application of "cyberspace" to the global, electronic place mapped, and remapped daily, by Internet users goes to John Perry Barlow. A Wyoming native, who attended the Fountain Valley School in Colorado Springs, Colorado, in the early 1960s and wrote lyrics for the Grateful Dead rock band during the 1970s and 1980s, Barlow published an article in the 22 January 1990 issue of *Microtimes Magazine* titled "Being in Nothingness." He predicted people would "develop cyberspace because … it's there. Sort of." Furthermore, the "settlement of cyberspace," he explained, would occur as "the next logical step in the quest to eliminate the interface … the mind-machine information barrier."

In early June 1990, Barlow elaborated on this concept in a *Whole Earth Review* article titled "Crime and Puzzlement," where he wrote that cyberspace "extends across that immense region of electron states, microwaves, magnetic fields, light pulses and thought" first named by "sci-fi writer William Gibson." He added, "Cyberspace, in its present condition, has a lot in common with the 19th Century West…. It is, of course, a perfect breeding ground for both outlaws and new ideas about liberty…. Like open range, the property boundaries of cyberspace are hard to stake and harder still to defend."

Ultimately, on 8 February 1996, Barlow's staunch libertarianism and his thorough rejection of the recently promulgated Telecommunications Reform Act drove him to compose "A Declaration of the Independence of Cyberspace." He asserted, "Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live…. Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter. There is no matter here…. We will create a civilization of the mind in cyberspace." Barlow's manifesto appeared on dozens of web sites within days, and cyber surfers soon dubbed him "the Thomas Jefferson of Cyberspace."

By 1997, the year lexicographers added "cyberspace" to the *Oxford English Dictionary*, the term already had begun to creep into the jargon of USAF members—both active duty and civilian. An article by 1Lt Gary Vincent in the Summer 1993 issue of *Airpower Journal* proposed a "cybernetic" design for command and control. In the Spring 1995 issue of that same journal, Air War College professor George Stein's article titled "Information Warfare" found "new and dangerous players in 'cyberspace'–the battlefield for information warfare." Later that year, USAF Chief of Staff General Ronald Fogleman signed a memorandum to accompany distribution of *Cyber Strike*, an Air University film that quoted computer expert Wynn Schwartau's definition of cyberspace as "that intangible place between computers where information momentarily exists on its route from one end of the global network to the other." A chapter in *Battlefield of the Future*, published by Air University Press in September 1995, referred to "the realms of land, sea, space, and cyberspace." Eventually, none other than

"The mission of the USAF is to deliver sovereign options for the defense of the United States of America and its global interests—to fly and fight in air, space, and cyberspace."
Secretary of the Air Force Michael Wynne and USAF Chief of Staff General T. Michael Moseley

USAF Chief of Staff General Michael Ryan, stated in the Winter 1999 issue of *Aerospace Power Journal* that "Our aviation forefathers certainly did not limit their visions but established the Air Force on a journey we have extended into space and cyberspace."

The early years of the twenty-first century only solidified the USAF's acceptance of "cyberspace" as a word and a domain. In the Spring 2001 issue of *Aerospace Power Journal*, General Simon Peter Worden pointed to "the issue of protecting the global commons of outer and cyberspace" and perceived "effective space and cyberspace control" as constituting "a critical new national security dimension." Intentionally, on Pearl Harbor Day in 2005, Secretary of the Air Force Michael Wynne and USAF Chief of Staff General T. Michael Moseley released a "joint letter to airmen" with a new mission statement: "The mission of the USAF is to deliver sovereign options for the defense of the United States of America and its global interests—to fly and fight in air, space, and cyberspace." The same two individuals signed a 6 September 2006 memorandum calling for "Establishment of an Operational Command for Cyberspace."

From that point onward, USAF senior leaders and underlings alike have produced an unceasing plethora of articles, studies, discussions, briefings, and speeches on "cyberspace," covering everything from its definition and doctrinal implications to organizing, training, and equipping forces to "fly and fight" there. Should anyone question how seriously the service takes its mission in this domain, they need look no further than Air University's cyberspace web site (http://www.au.af.mil/info-ops/cyberspace.htm).

Suggestions for Further Reading

1. Michael Benedikt, ed., *Cyberspace: First Steps* (Cambridge, Massachusetts: MIT Press, 1991).

2. Rebecca Bryant, "What Kind of Space is Cyberspace?" *Minerva–An Internet Journal of Philosophy* 5 (2001):138-155.

3. Anna Cicognani, "On the Linguistic Nature of Cyberspace and Virtual Communities," 1996, http://fragment.nl/mirror/various/Cicognani_1996.html.

4. Flo Conway and Jim Siegelman, *Dark Hero of the Information Age: In Search of Norbert Wiener, the Father of Cybernetics* (New York: Basic Books, 2005).

5. William Gibson, *Neuromancer, 20th Anniversary Edition* (New York: Ace Books, 2004).

6. Ananda Mitra, "Cybernetic Space: Bringing the Virtual and Real Together," *Journal of Interactive Advertising* 3, no. 2 (Spring 2003), http://www.jiad.org/article31. Ananda Mitra and Rae Lynn Schwartz, "From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces," *Journal of Computer-Mediated Communication* 7, no. 1 (October 2001), http://jcmc.indiana.edu/vol7/issue1/mitra.html.

7. Margaret Wertheim, *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet* (New York: W.W. Norton & Company, 1999).

Dr. Rick W. Sturdevant (BA, History, University of Northern Iowa; MA, History, University of Northern Iowa; PhD, University of California, Santa Barbara) is deputy command historian, Headquarters Air Force Space Command (HQ AFSPC), Peterson AFB, Colorado. He joined the Air Force History and Museums Program in April 1984 as chief historian, Airlift Information Systems Division, Scott AFB, Illinois, and moved one year later to the Chidlaw Building near downtown Colorado Springs as chief historian, Space Communications Division (SPCD). When SPCD was inactivated in 1991, he moved to the HQ AFSPC history office and became deputy command historian in 1999.

An acknowledged expert in the field of military space history, Dr. Sturdevant appears frequently as a guest lecturer on space history topics and is author or co-author of chapters or essays in *Beyond the Ionosphere: Fifty Years of Satellite Communication* (1997); *Organizing for the Use of Space: Historical Perspectives on a Persistent Issue* (1995); *Golden Legacy, Boundless Future: Essays on the United States Air Force and the Rise of Aerospace Power* (2000); *Air Warfare: An International Encyclopedia* (2002); *To Reach the High Frontier: A History of US Launch Vehicles* (2002); *The Limitless Sky: Air Force Science and Technology Contributions to the Nation* (2004); *Encyclopedia of 20th-Century Technology* (2005); *Societal Impact of Space Flight* (2007); and *Harnessing the Heavens: National Defense through Space* (2008). His articles or book reviews have appeared in such journals as *Space Times*, *Journal of the British Interplanetary Society*, *Air & Space/Smithsonian*, *Quest: The History of Spaceflight Quarterly*, *Air Power History*, *High Frontier: The Journal for Space & Missile Professionals*, and *Journal of the West*. He sits on the editorial board of *Quest* and on the staff of *High Frontier*.

Dr. Sturdevant is an active member of the American Institute of Aeronautics and Astronautics (AIAA), American Astronautical Society (AAS), British Interplanetary Society (BIS), and Society for the History of Technology (SHOT). His professional honors include the Air Force Exemplary Civilian Service Award (1995-1999), the AAS President's Recognition Award (2005), and election as an AAS Fellow (2007).

Book Review

Conquest in Cyberspace: National Security and Information Warfare

Conquest in Cyberspace: National Security and Information Warfare. By Martin C. Libicki. New York: Cambridge University Press, 2007. Pp. 336 $85.00 ISBN: 0521871603 .

Martin C. Libicki is an expert of information warfare at the RAND Corporation. In his latest book *Conquest in Cyberspace*, Libicki advocates the "friendly conquest of cyberspace." This idea draws upon political scientist Joseph Nye's conception of "soft power." The idea introduced in 1990 and further developed in the eponymous 2004 book emphasizes the value of non-coercive tools of grand strategy, such as media, diplomacy, and economic aid. Libicki argues that offensive information warfare operations will have only limited utility, and that soft power strategies have untapped potential. The friendly conquest of cyberspace he envisions could be achieved in much the same way Facebook conquered Internet social networking: bearing the costs of developing a useful product, distributing it cheaply, and reaping the rewards once the consumers are "stuck"—unwilling or unable to switch to a competitor. In this manner, a team of software designers with ulterior motives could hope to gain "the willing, perhaps enthusiastic, assent of its victims."

Although the "friendly conquest" of cyberspace is the main idea, there is no "central" idea. The contents of one chapter do not necessarily support or relate to the contents of the next: topics converge and diverge like the tributaries of a river. This is not a weakness, though. Libicki intends to give the non-expert an introduction (e.g., an understanding of how private information is collected on the Internet), his own predictions (e.g., the effects of decreasing storage costs), and his recommendations, all in a little over 300 pages.

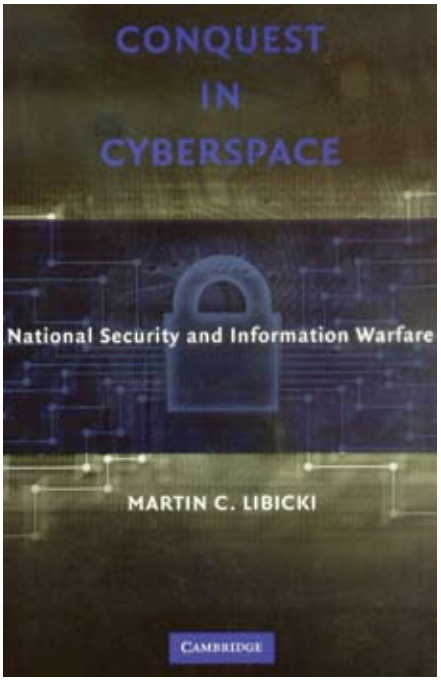
Libicki discusses both cyber defense and cyber attack. For Libicki cyber warfare is not simply a matter of attacking opponents' information: it is ultimately about affecting the decisions that are made. One way to do this is by creating noise, "wreak[ing] confusion rather than destruction." Information overload fuels confusion. Essentially, information can be acquired by search engines, web crawlers, and so forth, much faster than human analysts can process it.

Libicki also notes that getting information in cyberspace does not require hacking into a network—low tech tactics can be just as troublesome. Information can be acquired via phishing scams, scams in which con artists masquerade as someone they are not—a Nigerian prince in need of money or Bank of America asking you to confirm your account information—in hopes of obtaining your personal data. Often times, deceit is not even necessary: anyone who blogs or joins a social networking site gives up their private information willingly. Although Libicki does not discuss it in detail, abundance of easily accessible personal information could be used in personalized psychological operations.

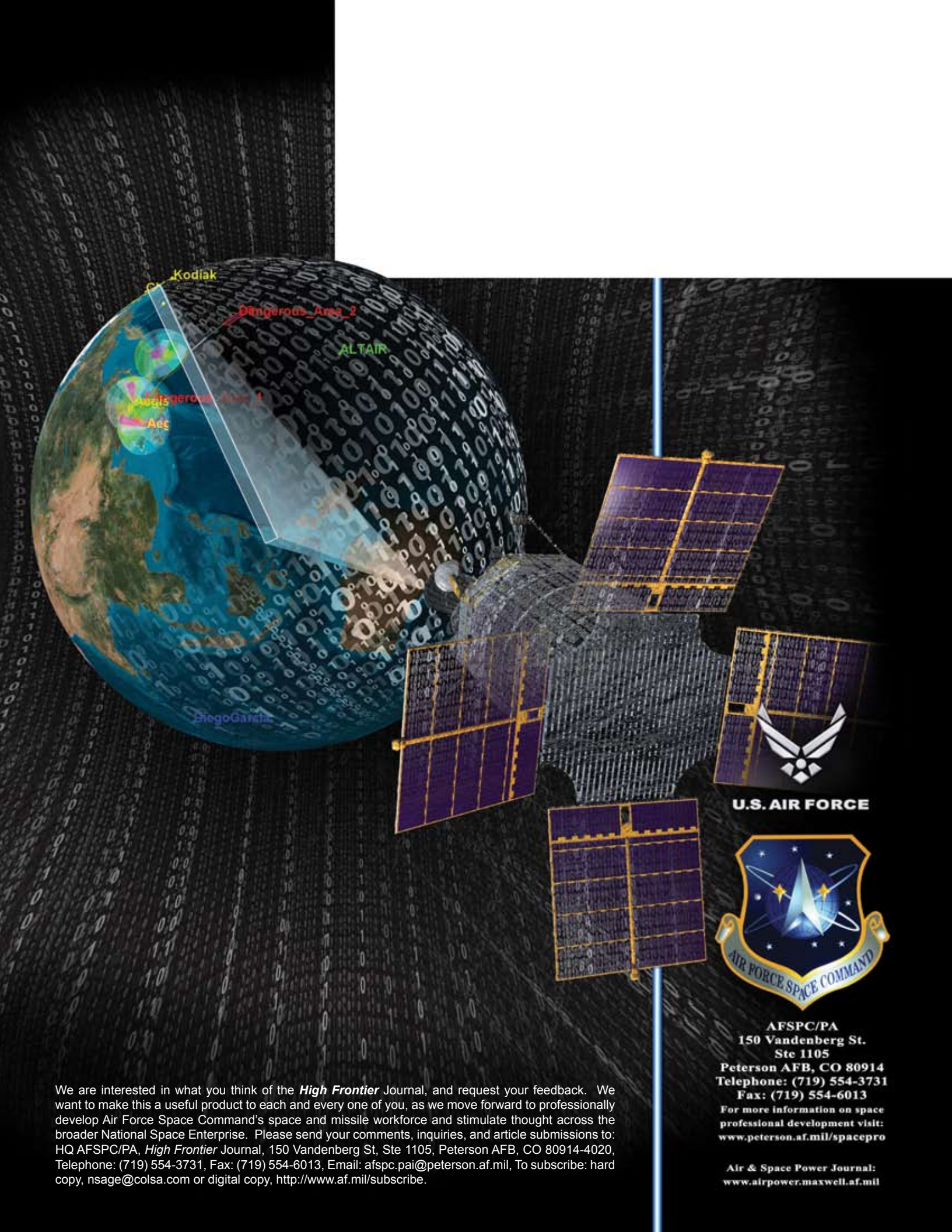
Propaganda could become targeted and efficient. Consider a simple example: instead of e-mailing every American a laundry list of US government shortcomings and failures, enemies could send tailored messages. An undergraduate computer science major could design a program that searches the "Education and Work" details of millions of Facebook users. Every time it recognizes the word "bank," "finance," "equity," "capital," or "markets," it would send the user an e-mail about the terrible inflation, financial mismanagement by the government, overbearing regulations, and so forth.

Any summary of the *Conquest in Cyberspace* will not do it justice. Libicki has a command of fields as disparate as computer networking, military strategy, organizational psychology, and cyber punk literature. The novice will not be overwhelmed and the expert will have come away learning something new.

After reading this book, I have concluded that a weakness in American computer science education, specifically—and science and math education in general—is a serious strategic threat. Talented computer scientists are supply inelastic. It may be difficult to ramp-up tank production at the onset of war, but additional computer scientists simply cannot be cranked out when demand rises. If things do not change, it is likely we will be caught on the horns of (what I like to call) the Groves Dilemma. During the Manhattan Project, General Leslie Groves had to decide whether to let scientists with suspicious affiliations work on a project of the highest sensitivity or to struggle with insufficient manpower. The very people who "won" World War II, embroiled us in the Cold War. A larger supply of manpower is the best way to overcome this dilemma. As it is said: "a man of knowledge increaseth might."



Reviewed by Muhammad "Mac" Elatab. Mr. Elatab will be graduating from Dartmouth College in June 2009 with a bachelor's degree in Government (International Relations). He founded the first undergraduate affiliate of the Intelligence and National Security Alliance and is writing a book on the conquerors Tamerlane and Babur.



We are interested in what you think of the ***High Frontier*** Journal, and request your feedback. We want to make this a useful product to each and every one of you, as we move forward to professionally develop Air Force Space Command's space and missile workforce and stimulate thought across the broader National Space Enterprise. Please send your comments, inquiries, and article submissions to: HQ AFSPC/PA, *High Frontier* Journal, 150 Vandenberg St, Ste 1105, Peterson AFB, CO 80914-4020, Telephone: (719) 554-3731, Fax: (719) 554-6013, Email: afspc.pai@peterson.af.mil, To subscribe: hard copy, nsage@colsa.com or digital copy, http://www.af.mil/subscribe.

AFSPC/PA
150 Vandenberg St.
Ste 1105
Peterson AFB, CO 80914
Telephone: (719) 554-3731
Fax: (719) 554-6013

For more information on space professional development visit: www.peterson.af.mil/spacepro

Air & Space Power Journal: www.airpower.maxwell.af.mil