ASPJ
Air & Space Power Journal

January–February 2013
Volume 27, No. 1
AFRP 10-1

Senior Leader Perspectives

Features

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
FEB 2013		**00-01-2013 to 00-02-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Air & Space Power Journal. Volume 27, Number 1. January-February 2013	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Institute (AFRI),155 N. Twining Street,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**211**	

Departments

Cyber Professionals in the Military and Industry—Partnering in Defense of the Nation

A Conversation between Maj Gen Suzanne Vautrinot, Commander, Twenty-Fourth Air Force, and Mr. Charles Beard, Chief Information Officer, Science Applications International Corporation

Transcribed and edited by Capt Jeffrey A. Martinez, USAF, and Capt Matthew R. Kayser, USAF

A strategic discussion on cyber is no longer an academic dialogue, and the associated technology is no longer the realm of industry or government development labs. The "defense" in the cyber domain is a national imperative; increasingly complex challenges force industrial and governmental seniors to expand collaborative efforts to address these challenges. Corporations across the globe are leveraging the cyber domain to deliver goods and services more quickly and cheaply while balancing the need to protect the personal information that customers entrust to them. Likewise, military commanders increasingly rely on integrated cyber capabilities to command and control and generate effects on the battlefield, both kinetic and nonkinetic. Safeguarding critical data, while allowing immediate access without interception or manipulation, is the key to mission success.

On 7 November 2012, two of our nation's senior cyber leaders, Maj Gen Suzanne Vautrinot, commander of Twenty-Fourth Air Force and Air Forces Cyber, and Mr. Charles Beard, chief information officer and senior vice president of Science Applications International Corporation (SAIC) sat down for a conversation. During this discussion, Mr. Beard recounted a journey of his efforts to reduce his company's cyber-attack surface and create a corporate environment resulting in a single enterprise information technology (IT) solution, and Major General Vautrinot not only articulated similarities in the Air Force's venture to defend the nation in cyberspace but also focused on how both the Air Force and industry can apply the lessons learned from successes like SAIC's migration as they continue to move toward a more homogeneous cybersecurity posture.

With their consent, we would like to share a private dialogue between recognized and mutually respected colleagues and partners in this dynamic domain. Additionally, interlaced into this conversation are contributions from each of Twenty-Fourth Air Force's operational cyberspace wings, which expound upon key discussion points and highlight current efforts to operationalize and normalize the cyberspace domain.

****

Vautrinot: Not surprisingly, your efforts resonate, and there is a true similarity of experience in this area. You've taken what were significantly diverse elements in a corporation and completely changed the dynamic—first organizationally and then technologically. I'm interested in which organizational changes you believe were most essential to that success; I'd like to leverage those changes toward our shared responsibility in this changing global environment.

Beard: Shared responsibility is correct. As we looked at cyber, we recognized that the governance model had to change. We grew up as 10,000 independent offices, and while that has its advantages from a market-development and a customer-responsiveness perspective, it

has its drawbacks from an enterprise IT governance and scale perspective. We needed strategic agility to engage in multiple global markets and in an increasingly hostile computer environment. The first step was to define and stabilize the environment, and that meant changing the way we thought about IT.

Vautrinot: In the military, major commands or functional organizations might be considered in the same way—all talented but very discrete . . . the description "cylinders of excellence" comes to mind. From a military operations stance, this makes sense, but it presents challenges when addressing threats and risk from a cyberspace perspective. Since information technology and communications grew up in a decentralized fashion, there's an apparent inertia toward retaining that decentralized approach. Yet, you've demonstrated the necessity in creating an enterprise solution to best operate what is now a cyber enterprise.

Beard: The first step for us was to make that connection and make sure we had a true enterprise view of the environment and begin to operate it as an enterprise asset—irrespective of how it originated. As the next action, we began to work with government to talk about the need to share threat information and improve our cyber posture. We [SAIC] operate IT environments on behalf of the government. We have client information on our networks, and we take the responsibility of stewardship very seriously. At the same time, however, we are a publicly traded company and operate on a global basis. We couldn't just take a US-centric view of how we were going to solve this problem anymore than the Air Force could take such a position. We had to change the intellectual reference for a lot of people when it came to governance and what it really meant as a multinational corporation to address this issue of cyber.

Vautrinot: In air and space domains, we had the advantage of developing unique and often superior or specialized systems: fifth-generation transitioning to sixth-generation aircraft and cutting-edge satellites . . . inherently unique. It was always about the military systems. Yet in cy-

berspace, it's a global, interconnected environment. We share the same man-made environment, and industry is at that "cutting edge." The military can't afford—technically or financially—to respond independently. We need shared responsibility—industry, government, academia, international partners—in altering the environment to our collective advantage and holding each other accountable for success. In military parlance, we can change the domain to provide freedom of movement to our allies while denying our adversaries the same. We're all working in the same space although perhaps we need to calculate risk and mission response a bit differently.

Beard: It's all about risk management and measured response. I go back to my Strategic Air Command days, where we operated in the nuclear domain. While the mission of deterrence was clear, the mission of strike was equally well understood. Preparing for both was the order of the day. Unlike the other domains within the military—ground, air, sea, and space—force projection and domination in the cyber domain are very difficult. You are running on shared infrastructure on a global basis, and the adversary often has an equal or better footing.

Vautrinot: I'm seeing a similar global dynamic in our support to remotely piloted aircraft missions. In order to provide mission assurance, we had to conduct extensive front-end research to understand the various links from the United States to the overseas flight. The system was designed with roughly 180 touch points, many of which are not military controlled, across several different networks, including foreign systems, making it critical to establish relationships with commercial organizations and allies. The security and assurance becomes a tremendous interdependency, which you are also seeing in industry.

Beard: In the commercial domain, interdependency equals continuity of operations and risk management. There is a difference in the way we view the threat, but mission assurance for a commercial company is largely driven by the markets and geographies in which it operates and the type of operation it is conducting. The fact that those operations are

conducted on globally shared infrastructure is an important context for corporate executives to understand as they consider risks.

Vautrinot: The commanders we support have indicated a similar imperative for uninterrupted access to trusted and verifiable data. Mission assurance in the cyber domain is so foundational to the mission that we can't afford to lose the capacity to communicate—it's essential to military command and control.

Beard: That's exactly right. A company can have the greatest capabilities in the world, but if it cannot operate in the digital domain and if it cannot sustain uninterrupted access to the energy and communications infrastructure, it's very difficult to have a mission profile that survives. So we see command and control very much alike in the context of the military and commercial mission because we're trying to conduct business operations around the globe. If I cannot provide access to clean communications and uninterrupted energy, then the business continuity is dramatically impaired.

Vautrinot: At a corporate level, you had to go beyond awareness. People had to get on board, understand the codependency, and see its benefit to the individual. Having the discussion on a smaller scale makes the effect tangible and makes change acceptable. A successful business can leverage this to shift a company in new directions. Was the realization something that was tailored to each individual and scaled, or did senior leadership have to drive enterprise awareness to change organizational culture?

Beard: At SAIC, we are fortunate to have people on our board who have walked the halls of government and industry, who understand that this threat is real. So what we began to do was translate that risk in the context of the business. I think what you'll find is that various commercial industries are further along in that understanding, that maturity. Certainly the financial services industry has understood it for many years. They have separate risk committees on their boards of directors, and it's one of many risks that they must consider. You've got other industries, like energy, where the awareness is ratcheting up

even further. They witness the threat vector changing from simple intelligence gathering to operational destruction, as indicated by the Saudi Aramco case.[1] In the health-care industry, a company might spend a decade and $10 billion building out a product or a new drug, only to see a carbon copy of that product launched in a foreign country a year before they get approval from the Food and Drug Administration [FDA]. All their intellectual property is gone, so the revenue stream anticipated by that company for that product for the next 10 years is significantly cut. The economic imperatives are becoming the clear and present danger to the national economy where these businesses operate, but many companies still don't understand cyber threats and their possible impacts, both physical and economic.

Vautrinot: There is similar recognition concerning cyber dependency. However, I'm not sure there's cognizance on the level of dependency, and our ability to conduct all missions—to fly, fight, and win in air, space, and cyberspace. Our challenge as we move forward is to create linkage in all mission elements . . . the operational tapestry versus the mission threads. As we expand on this focus, we must be cognizant to balance these operational efforts with the ability to maintain and defend our networks. Under the Twenty-Fourth Air Force, the 689th Combat Communications Wing specializes in maintaining this equilibrium by extending cyber capabilities to the tactical edge in support of the war fighter while continuing to provide defensible, trusted communications at that edge.[2]

Beard: The fact that e-mail is routed to servers beyond your company networks and possibly national borders—perhaps to countries that have lawful intercept laws that are different than your own—is simply not understood by the casual user. We've built entire businesses that depend on the cyber domain, but we don't really understand the security challenges associated with that domain. It is daunting when you begin to understand what the impacts really could be, and that is why leadership is so critical to navigating this challenge, and the endless extension of network reliance.

Vautrinot: In the current budget environment, there's a complicating factor: the expected resource commitment actually closes the dialogue and decision space before options can be explored. The complexity of this enterprise-level transformation becomes its own kind of inertia. If cyber is currently disordered, then we're caught somewhere between the natural "entropy" of the domain and the inertia of the decision. Did you fight that on the industry side?

Beard: I recently heard an attorney suggest that corporate directors should not be better informed on cybersecurity risks because the laws protect them on things for which they are not educated. I found that to be a shortsighted view. I think in the context of commercial industry—take a bank, for example, a public utility, a pharmaceutical life sciences company, or a defense contractor—the foundation of these businesses is reputation and trust. The boards of those companies, with robust risk-management practices, know best if they're in an informed position to adjudicate those risks. To us, the cyber risk may be the most dominant risk that we think they face. But for a defense contractor, perhaps the biggest risk they're facing is that they have people in harm's way. A financial institution may be facing a liquidity crisis. A pharmaceutical company may be concerned about achieving FDA approval to meet forecasted sales and finding the counterfeit versions of their products selling around the globe. The question is how well articulated is that risk, and this notion that we can just build a fortress around the business with static cyber defenses is simply the digital version of the Maginot Line.

Vautrinot: Agree, static defenses didn't work in World War II and won't work in the cyber environment. That's why in the Air Force, we've been focusing on a proactive defensive posture. Instead of waiting until an adversary penetrates our networks to assess our vulnerabilities, we have created specialized teams that search our networks and seek out those vulnerabilities, preferably before they are exploited. We focus on identifying and defending those interfaces that are essential to mission success—Gen Keith Alexander, commander of

US Cyber Command, would call this capability "recon/counter-recon." A key facet of this defensive effort is identifying and focusing on a commander's prioritized "defended asset list," those critical areas that must be able to operate through a contested environment or attack. This corresponds directly to something we spoke about before: linking our efforts to the operational mission. We can enter a network environment and provide the commander who is reliant on that system with timely, accurate decision information. Specifically, can he rely on the network system to successfully accomplish the mission?

This proactive posture is bolstered by the information and threat vector sharing between industry and government. A superb example was the Department of Defense's Voluntary Defense Industrial Base Cyber Security / Information Assurance Program, an agreement in which companies, including many of the larger corporations in this country, collaborated with the Department of Defense (in the Air Force, via the Air Force Computer Emergency Response Team under the 67th Network Warfare Wing) and Department of Homeland Security to share sensitive threat information and thereby improve the collective cyberspace defense.[3]

Beard: What you are beginning to see now on the commercial side is a frustration with being on static defense. The underlying economics of cyber attacks currently favor the adversary just as improvised explosive devices favor insurgents. To counter that model, we have partnered both with industry and government to develop trusted platforms that allow for dynamic defenses through our Cloudshield products. Alternatively, some in the commercial markets believe it is time to punch back. This move from the cyber operations perspective is to move from computer network defense to computer network attack. I have real concerns about commercial companies taking on a computer network attack type of mission, with unintended consequences both for law enforcement and other government agencies.

Vautrinot: Historically under international law, the concept of attack was the province of the nation-state. However, geographic boundaries

no longer demarcate actors on the offensive; for example, we've seen companies selling services purporting to respond to cyber intrusions by sending reset commands or redirecting malicious traffic. The nature of cyber is that companies may well have the capability to go much further. In doing so, they will contend with domestic law as well as statutes where they are operating or causing effects. Unfortunately, current domestic and international policies haven't kept pace with the advancement in cyber capabilities; therefore, loopholes and outright gaps in governance exist that can be leveraged by bold corporations.

In the Air Force, we aren't just constrained by domestic laws but also by government policy. Generally, the Department of Homeland Security is responsible for defending cyber assets outside the Department of Defense's networks, but regardless of which organization is contemplating these actions, the problems of definitively attributing an intrusion to a particular attacker and deconflicting actions with other entities are particularly difficult. This again highlights the need for an information-sharing framework between government and industry that facilitates rapid action to cyber events.

Air Force senior leaders are certainly aware of the vulnerabilities of our network systems, but now there is also a keen recognition of the opportunities to enable defense as well as facilitate mission success. A great example has been our work with US Transportation Command and Air Mobility Command. Their dependencies are not limited to the .mil domain but on the .com and the ability to work with industry partners to ensure worldwide movement. As a result, they are acutely aware, and the understanding causes them to be very proactive in terms of resolution. Yet in other commands, there is resistance and belief that their networks are "private" or separate from the global Internet and therefore its inherent adversaries. In regards to your independent offices, did you experience similar variance?

Beard: We did. We had employees, partners, and even clients who operated on what they believed to be "closed" networks; therefore, they didn't feel like they had a problem. They simply did not see the

need for added layers of protection or policy enforcement on their activities. What they called bureaucracy is what we call mission assurance in the context of systems engineering.

Vautrinot: Clearly, a necessity for unity of effort and with it a clear chain of responsibility—command and control. Certainly, you were implementing an enterprise solution for all the right reasons, and the field of independent offices realized the importance. Nevertheless, there is resistance to losing what some believe is their self-actualization—their ability to control. What allowed you to bridge that natural resistance in the field and drive the implementation?

Beard: I would say three things. One was the commitment of leadership. You had to have the will of the leadership to say, "We're willing to go here." Second, we began to educate the leadership, management, and select employee groups. That was really important to us—to increase the awareness. Finally, we had to rethink the context of cybersecurity. We needed to understand what truly had to be protected and where we would establish trust. The results of that exercise materially changed our defense-in-depth strategy.

Vautrinot: What level of leadership was necessary to initiate? In our vernacular, it would be the major commands and key functionals saying, "OK, we're all in agreement. We recognize the threat, and we're all going to move together in this direction." Then it would be our responsibility to help them understand the rationale for implementing measures or taking action that may be locally restrictive.

Beard: Correct, not everybody agreed. It took a combined chief executive officer / chief operating officer / chief financial officer–level mandate, and we broke some china.[4] Although people understood the leadership decision and the need for policy enforcement and oversight, they still wanted autonomy, so we then developed tools to provide autonomy while preserving the security posture. That was done in the context of productivity and giving people what they wanted. What we didn't understand 20 years ago, when operations in the digital domain began to evolve, was this cyber-risk issue. The risk issue has

now raised its ugly head, and you can't ignore it, so you're conflicted. I want to take care of you as an end user, as a customer, but I have this other responsibility that you may or may not understand or appreciate, and I'll try to help explain it. I just can't explain it to every end user because I don't have the cycles to do that because then I'm not doing my job. So that's part of the balance.

Vautrinot: You are protecting the long-term viability of the corporate entity, the same way that we're protecting the long-term viability of the mission and our support to the nation. There has to be some freedom of action, across the enterprise, to allow that protection.

I believe that in industry you also have a requirement to report, not cybersecurity per se, but your viability as a corporate entity in the realm of cybersecurity. If I had a similar report, I anticipate we wouldn't receive a passing grade. However, we have moved toward a construct where there's both asset- and enterprise-level management, but only on the .mil and the .smil networks. Each of the mission system networks defines itself separately and is independently resourced and managed. In your model, there'd be one "general" who would be designated to control asset management of all Air Force network interfaces, soup to nuts—precisely what you had to do in industry. Certainly necessary, but I've learned that operational viability in this contested environment requires a fundamental change to the assets we would centrally manage—it requires sensoring to enable awareness and proactive response to threats within the network. The first step, having the asset management, by itself is insufficient, but being able to sensor it—to get that situational awareness and to allow your system to react in an automated fashion—is the next step. How did you approach the engineering-level changes?

Beard: That was part of the second journey in this process—to instrument and do all the enterprise vulnerability analysis and the scans against that baseline. This allows you to prepare for continuous monitoring. The reason that it's important is what makes up the third journey: I may want to morph my network based on the business mission,

actionable threat intelligence, and the intent of select adversaries that are active.

Vautrinot: This is where cyberspace operations can facilitate mission operations or provide mission alternatives. We don't need to command and control the mission, but we need to have full visibility of what's going on in the [cyber]space and be able to adjust it in real time to thwart adversary positioning. It makes the adversary's problem set much more difficult while preserving mission effectiveness.

Beard: Exactly. Because if adversaries understand your network better than you do, you've got problems, and if your computer infrastructure is so rigid that you can't dynamically allocate, they're going to take advantage of that, and once again both the economic and operational advantages go to the adversary. This is why we moved to the hybrid cloud model—because it gave us the opportunity at the application and data level to move workloads around. I can now take a workload that has historically operated on specific servers in a specific data center and dynamically assign that workload to virtual machines operating in virtual data centers that may have very different geographic characteristics. Information can stay within my data center, but I can move it to different places.

Vautrinot: In that construct, for example, employee health care doesn't own medical data, and the finance department wouldn't own financial data. Moving and providing access to desired data within the enterprise is the key, and each branch of the enterprise is using that data rather than controlling it as a segregated element. The goal shouldn't be to control but rather have trusted data accessible anytime, anywhere. Our challenge is breeding an environment that is constantly agile.

There appears to be a bit of a misnomer surrounding IT efficiency "savings." Talking to AT&T, Microsoft, and industry partners like you, the front-end investment to make that change is not only an investment of corporate culture and leadership but also a significant capital investment. Not just to save money over the long-term operation of

the IT but a financial investment in cybersecurity. How did your corporation work through the investment dynamic to determine that the company had an imperative to afford cybersecurity? What was the scope of that assessment and dialogue?

Beard: We didn't try to make it about saving money on the front end. We tried to make it about strategic agility and what that meant to us as a global corporation. We knew that we needed agility at the enterprise level. So by making this investment, it began to give us the ability to start flexing. Think of it as not just using this technology to operate companies but in the context of how to virtualize companies and recombine them. Indeed, SAIC is going through such an activity at this time, and it is exciting to see IT as an enabler rather than a roadblock.

Vautrinot: Cyber in this context that we are describing—it is a mission, and you're not viable without this mission. Despite our current national economic situation, we have to transition dialogue from cost reduction to the defense imperative and therefore worthy of the investment from a national strategy standpoint.

Beard: We pulled cyber out separately from a budget perspective and treated it as a strategic investment. If you look at IT as a cost center, you will miss the opportunity. I've advised a number of companies over the years that looked to IT cost-reduction targets as a way of meeting a corporate cost objective, but the dirty little secret is that they take on technical debt that shows up neither on the balance sheet as an unfunded liability nor on the enterprise risk register.

Vautrinot: In that vein, my "technical debt" is lack of automation and sensoring, which I'm overcoming manually—in effect a huge workforce that isn't sustainable or appropriate in a dynamic cyber environment. It drives reactionary responses to problems and precludes resourcing automated sensoring and solutions.

Our efforts to move from a dispersed, installation-managed network to a single, homogeneous, and centrally managed network will allow the follow-on of necessary sensoring and automation to free up

resources and robust network operations at the scale required for a global industry, like yours, or military operations. Until then, this drives a large back-end cost.

Beard: We all know that reactive posture is more expensive. We would never do that with a weapons system development effort—we try to design solid engineering into the front end. It's a lot cheaper in the long run to do it in that order.

Vautrinot: The assumption is that the things you see, you can at least deal with, but what about the unknown unknowns?

Beard: The unknown unknowns are unacceptable. For Sarbanes-Oxley Act purposes, for example, we are required to have preventive controls in place.[5] The unknown unknowns force you to think "left of bang."[6] But that then leads you to the realization that you can't protect everything. So let's have a business dialogue or a military dialogue about the assets—could be data assets—that we wish to protect.

Vautrinot: It's what I referred to as the defended asset list but at a discrete level instead of an enterprise level. We've worked individually with the Tanker Airlift Control Center as well as one of the many air operations centers to demonstrate this dynamic. But we cannot apply it at an enterprise level because we can't "see" or control the cyber assets in the enterprise.

Beard: In my role, I'll get a phone call that says, "I have this urgent information security problem; come help me." And the first two questions are, "When were you made aware of a requirement to protect this asset?" and "When did you know you had this problem?" If it wasn't on the defended asset list, I didn't proactively do anything to protect it, and if it's been exfiltrated or manipulated, I didn't specifically look to ensure it didn't go outbound or preserve its baseline. So if the defended asset list is incomplete, it's very difficult for me to develop and implement a cybersecurity policy to protect and defend those assets. This is a team sport, and there is shared responsibility in mission assurance that is incredibly dynamic. If you simply buy a security appliance, by

the time you deploy it, it's out of date. So you have an asymmetric threat, and you are trying to respond to it with a traditional legacy process. It's counterproductive, which is why we are looking to change the game.

Vautrinot: Absolutely, that's why we are building a platform that can be constantly adjusted. If I used a space operations comparison, I define the interface of the payload with the platform. That means I need to own the platform and the enterprise and can adjust in real time. For example, under Col Paul Welch, commander of the 688th Information Operations Wing, we developed the Information Operations Platform to provide an accredited open-architecture framework for rapid deployment of other third-party applications.[7] This ability to swap our tools allows accelerated fielding and deployment of those tools, providing dynamic and responsive operations for Air Force and Department of Defense cyberspace operations. This provides flexibility—like a fighter aircraft, which can be configured for an air-to-ground mission during one sortie and for an air-to-air mission during the next. The difference is that the fighter is reconfigured in hours/days, whereas in cyber it's got to be seconds.

Beard: Let's say my intrusion detection system has been defeated and I need something new. The software base is part of a platform and it's nonnegotiable, so the hardware platform itself doesn't change. I can deploy it right now. It's this stealth machine with out-of-band controls that only we see, but I can put different payloads on it.[8] The independent offices can do what they need to do, but the enterprise can still dominate the network on their behalf. That's the trick—command and control at the enterprise level with decentralized execution, a dynamic environment that provides enterprise agility and "trust" built into the platform that is highly configurable and allows you to look "left of bang."

Vautrinot: The intent as we continue to refine our skills in this domain is to move from the reactive to the proactive posture and present agile, sensored targets to our adversaries. All of us, whether govern-

ment or industry, are in the business of trust: we must use the available intellectual capital and emerging technologies to protect our information and systems from being linked into an expansive, malicious chain [2011 global remediation cost $388 billion].[9] The nation's cyber journey is a shared responsibility, and it's personal—only through developing partnerships can we continue to defend this nation in cyberspace.

****

The sheer scope of this domain is difficult to grasp: in the next 60 seconds, 168,000,000 e-mails will be sent; 695,000 status updates will be posted to Facebook; and 690,000 searches will be conducted on Google.[10] As the opportunities afforded by this domain continue to multiply, so do the vulnerabilities. Those of us who were present for this discussion left the room not only with a greater understanding of the challenges that lie ahead in this domain but also with a greater appreciation for the collaborative efforts occurring between government and industry to safeguard the critical information that corporations, commanders, and the country rely upon. ✪

Notes

1. In one of the most destructive acts of computer sabotage as of this writing, on 15 August 2012, a virus erased data on three-quarters of Saudi Aramco's corporate computers, posting a burning US flag in place of that information. Because of the attack, the company was forced to replace tens of thousands of hard drives.

2. The mission of the 689th Combat Communications Wing is to train, deploy, and deliver expeditionary and specialized communications, air traffic control, and landing systems for humanitarian-relief operations and dominant combat operations—anytime, anywhere. To keep up with the rapidly changing strategic environment, combat communicators rely heavily on industry to provide commercial off-the-shelf technology, which enables them to extend, operate, and defend cyberspace capabilities in the most austere locations, in the most effective manner possible.

3. Ensuring the defense of military information and systems—both through computer network defense and computer network attack—is a daily challenge. The 67th Network Warfare Wing executes Air Force network operations, defense, attack, and exploitation to create integrated cyberspace effects on behalf of Twenty-Fourth Air Force and the combatant commands. The wing operates within current Department of Defense authorities to protect Air

Force and Department of Defense information and systems and to ensure freedom of maneuver in the cyber domain. The 67th includes the on-net operators responsible for the day-to-day operation of Air Force networks. Extensive collaboration between the wing's personnel and other government and civilian organizations ensures the continuous sharing of cyber threat information across public and private entities.

4. Just as "a bull in a china shop" breaks china. In this case, the introduction of cybersecurity processes broke normal business processes.

5. A congressional bill enacted in 2002, the Sarbanes-Oxley Act is also known in the Senate as the Public Company Accounting Reform and Investor Protection Act, and in the House of Representatives as the Corporate and Auditing Accountability and Responsibility Act. The bill was enacted due to a number of major corporate and accounting scandals, including those involving Enron and WorldCom.

6. The term *left of bang* refers to a timeline in which each marked incident is a "bang." Activities "right of bang" are reactive responses to the incident; those "left of bang" are proactive actions in preparation for such incidents.

7. The 688th Information Operations Wing delivers these proven information operations and engineering infrastructure capabilities integrated across the air, space, and cyberspace domains. The wing has developed an innovative, rapid tool-development process accompanied by a rapid-acquisition program that reflects immediate, medium, and long-term systems approaches. The innovation framework involves Air Force Materiel Command (AFMC) working with Air Force Space Command to establish a center of cyber innovation to provide cost-effective cyberspace capabilities, such as the Information Operations Platform, in the appropriate time frame to support the joint war fighter.

The 688th expands the innovations achieved by the research topic of interest, hosted by Colonel Welch, by locally partnering with science and technology expertise from the Air Force Research Laboratory and simultaneously joining with their acquisition counterparts such as Col Chris Kinne, from AFMC in San Antonio, to expand local acquisition authority delegated from the Office of the Secretary of the Air Force for Acquisition. A diverse, colocated knowledge set is required to complement the resident cyber-development expertise. Lt Col Jim Smith leads the Air Force Operational Test and Evaluation Center's presence in this new organization to test and verify the effectiveness of proposed capabilities in an operational environment.

8. Out-of-band control passes control data on a separate connection from main data.

9. *Norton Cybercrime Report 2011*, Symantec Corporation, 7 September 2011, http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/.

10. "60 Seconds—Things That Happen On Internet Every Sixty Seconds," GO-Gulf.com, 1 June 2011, http://www.go-gulf.com/blog/60-seconds/.

Maj Gen Suzanne M. Vautrinot, USAF

Major General Vautrinot (USAFA; MS, University of Southern California) is the commander of Twenty-Fourth Air Force, Air Forces Cyber, and Air Force Network Operations, Lackland AFB, Texas. She is responsible for the Air Force's component numbered air force providing combatant commanders with trained and ready cyber forces that plan and conduct cyberspace operations. The general directs the activities of three operational cyber wings—two headquartered at Lackland and one at Robins AFB, Georgia—as well as the 624th Operations Center at Lackland. General Vautrinot has served in various assignments, including cyber operations, plans and policy, strategic security, space operations, and staff work. She has commanded at the squadron, group, and wing levels, as well as the Air Force Recruiting Service. The general has served on the Joint Staff, the staffs at major command headquarters, and Air Force headquarters. Prior to assuming her current position, she was the director of plans and policy, US Cyber Command, Fort George G. Meade, Maryland, and the special assistant to the vice-chief of staff of the US Air Force, Washington, DC. A National Security Fellow at the John F. Kennedy School of Government, Harvard University, General Vautrinot is a distinguished graduate of Squadron Officer School, Air Command and Staff College (with honors), Joint and Combined Staff Officer School, and Air War College (correspondence).

Charles E. Beard Jr.

Mr. Beard (BS, Texas A&M University; MBA, University of Montana) is the senior vice president and chief information officer for Science Applications International Corporation (SAIC) and general manager of the SAIC Cybersecurity Business Unit. In this dual role, he has led SAIC to become the first in its industry to transition the enterprise to a cloud computing infrastructure and address the security and control challenges inherent in that journey. He is secretary of the Inova Health Care Services Board of Trustees and chairman of the Quality Board at Inova Mount Vernon Hospital. Prior to joining SAIC, Mr. Beard was a director in the Oliver Wyman division of Marsh & McLennan. In this role, he provided strategic advisory services associated with corporate transactions and restructurings and developing information technology strategies to achieve business design objectives. He also served as the senior vice president for Global Transportation and Industrial Markets at KPMG Consulting (later BearingPoint), leading the company's strategy and operations services for global commercial clients, including GE, Honeywell, United Technologies, and Southwest Airlines. He has completed continuing education at the Harvard Business School and MIT Sloan. Mr. Beard is a featured speaker at the university level and a frequent contributor to major media publications.

Let us know what you think! Leave a comment!

Some Reflections on the Intersection of Law and Ethics in Cyber War

Maj Gen Charles J. Dunlap Jr., USAF, Retired

Few security issues have captured the attention of the public as has the specter of cyber war. In a recent op-ed, President Obama warns that "the cyber threat to our nation is one of the most serious economic and national security challenges we face."[1] This, in turn, has raised many questions about the legal parameters of cyber operations, including the rules applicable to actual cyber war.[2]

Parallel to the growing interest in the legal aspects of cyber war are an increasing number of questions focused on the ethical dimension. That is an important consideration for any military endeavor but one just emerging with respect to cyber operations.[3] Mounting concern about the ethical aspects of cyber activities led the US Naval Academy to sponsor an entire conference on the subject in the spring of 2012.[4] Even

more recently, the *Atlantic* published an article entitled "Is It Possible to Wage a Just Cyberwar?," which discussed several intriguing issues.[5]

This article reflects upon a few issues that illustrate how legal and ethical concerns intersect in the cyber realm. Such an intersection should not be especially surprising. As historian Geoffrey Best insists, "it must never be forgotten that the law of war, wherever it began at all, began mainly as a matter of religion and ethics. . . . It began in ethics and it has kept one foot in ethics ever since."[6] Understanding that relationship is vital to appreciating the full scope of the responsibilities of a cyber warrior in the twenty-first century.

Law and Ethics

How do law and ethics relate? Certainly, adherence to the law is a baseline ethical responsibility, but it is only that—a baseline. In the March 2012 edition of *Armed Forces Journal*, Lt Gabriel Bradley, USN, points out that "the law of armed conflict sets minimum standards." He goes on to argue persuasively that inculcating individual and institutional moral and ethical values—a sense of honor, if you will—is essential to ensuring *actual* compliance with the law. And he is certainly right when he quotes Christopher Coker's observation that "laws can reaffirm the warrior ethos; they cannot replace it."[7]

Of course, even determining the baseline—that is, the law—is not always easy in twenty-first-century operations generally but especially with regard to cyber activities. Among the many reasons for this difficulty is the fact that most of the law of armed conflict was designed to address conflicts waged mainly with kinetic weaponry. Nevertheless, in this writer's view, existing law has ready applicability to cyber operations, a notion that perhaps brings us to the first issue regarding the intersection of law, ethics, and cyber operations.[8] Specifically, we sometimes hear that cyberspace is such a new domain that no existing law could—or even *should*—apply to military operations in it.

Such an idea is simply untrue. Most of the law of armed conflict is not domain specific. Along this line, consider a recent project by the Harvard Program on Humanitarian Policy and Conflict Research to write a manual specifically on the international law applicable to air and missile warfare.[9] The program did produce a useful volume, but it is a relatively thin one since the project discovered a comparatively modest amount of law that seemed wholly unique to the air and space domains. One can say much the same about the cyber domain, including ethical considerations.[10]

Furthermore, what sometimes masquerades as a legal problem in cyber operations is often more of a technical issue or a policy conundrum—*not* an authentic legal problem. The much ballyhooed issue of what constitutes the proverbial "act of war" in the cyber domain offers a good example. Although the phrase "act of war" is a political term, not a legal axiom, such phrases as "use of force" and "armed attack" *do* have legal meaning and could relate to a casus belli in terms of a forceful response.[11]

In fact, the interpretation of such expressions in the cyber realm is resolvable under the law if—*and, really, only "if"*—technology can provide adequate data regarding, for example, the actual harm caused by the supposed "attack," as well as sufficient information about who actually did it. Of course, the absence of attribution data (technically challenging to obtain in the cyber realm) can be a definitive legal and ethical bar to a forceful response. This may prove frustrating when people want to "do something" in answer to a cyber incident, but it is hardly unreasonable for the law—*and ethics*—to require reliable information concerning who might be responsible before launching a counter of some kind.

Technologically speaking, the daunting task of determining attribution is *not* a problem for lawyers or, for that matter, ethicists; rather, it is something for technologists to solve.[12] It is interesting, therefore, that the authors of the above-mentioned *Atlantic* article argue—in relation to the alleged use of a cyber weapon (Stuxnet) against Iran's nu-

clear development facilities—that "the lack of attribution of Stuxnet raises ethical concerns because it denied Iran the ability to counterattack, encouraging it towards ever more extreme behavior."[13]

Aside from the question of whether Iran would necessarily have a legal or moral basis to counterattack as a result of the alleged Stuxnet operation, it is of further interest that the authors of the *Atlantic* piece say that "to make attribution work, we need international agreements." These would include, they contend, agreements that "cyberattacks should carry a digital signature of the attacking organization" and that certain networking protocols could be used to "make attribution easier."[14]

Most experts would probably say that current law does not require such facilitation of cyber attribution.[15] Nevertheless, the authors of the *Atlantic* article argue for "better [cooperation] on international network monitoring to trace sources of attacks" and seem to believe that "economic incentives, such as the threat of trade sanctions, can make such agreements desirable."[16] Again, one might disagree with much about these proposals, but the authors should be commended for at least beginning the dialogue on possible ways of addressing one of the most perplexing legal and moral questions of cyber war.

As with attribution, technological issues—not the law per se—are also the most challenging aspect of the targeting of cyber weaponry. The cardinal legal and ethical principles of distinction and proportionality require technical data that will inform decision makers as to who might be affected by a particular technique, and to what extent.[17] Again, that this may prove technically difficult is neither a legal nor an ethical problem but a scientific one. Indeed, one can say that the ability to model effects with dependable accuracy represents one of the most needed capabilities in the world of cyber operations. Such an ability would give decision makers—not to mention lawyers and ethicists—the kind of information that is patently essential for making reasoned judgments about employing a cyber methodology.

Do Legal and Ethical Values Unduly Encumber Cyber Warriors?

Over and above questions about the application of legal regimes and ethical mores to a particular cyber scenario is the broader question of whether any restraints should apply at all. More specifically, some people believe that attempts to apply the law will encumber the United States' cyber efforts and put its security at risk. This rather surprising question lies at the heart of a serious debate in which Stewart Baker and this writer engaged under the auspices of the American Bar Association.[18]

By way of context, Mr. Baker, a highly respected lawyer with the prestigious Washington law firm of Steptoe and Johnson, had previously served in government as general counsel for the National Security Agency as well as assistant secretary for policy in the US Department of Homeland Security. He begins his polemic this way: "Lawyers don't win wars. But can they lose a war? We're likely to find out, and soon. Lawyers across the government have raised so many showstopping legal questions about cyberwar that they've left our military unable to fight, or even plan for, a war in cyberspace."[19]

Mr. Baker further claims that any attempts to "impose limits on cyberwar [are] . . . doomed."[20] Among the most troubling aspects of his argument is really an ethical one of the first order. He points to the devastation caused by air warfare during World War II and refers to the claim made by former British prime minister Stanley Baldwin in 1932 that in air warfare "the only defense is in offense, which means that you have got to kill more women and children more quickly than the enemy if you want to save yourselves."[21]

Mr. Baker then goes on to cite Mr. Baldwin's "kill more women and children more quickly" concept by asserting that "if we want to defend against the horrors of cyberwar, we need first to face them *with the candor of a Stanley Baldwin*" (emphasis added).[22] Only after construct-

ing a cyber war strategy so framed would Mr. Baker consider it appropriate to "ask the lawyers for their thoughts."[23]

Fully reprising my response lies beyond the scope of this article (although the title—"Lawless Cyberwar? Not If You Want to Win"—may suggest its content).[24] Suffice it to say that it is vitally important in cyber war (as in any military operation) to ground the "limits" whenever possible, not only in the law or ethics per se but also in pragmatic, war-fighting rationale. In the case of cyber, this is not particularly difficult to do, especially if the actual war fighters do not perceive an asymmetry between what law and ethics might require and what they believe they need to accomplish their mission.

Notwithstanding Mr. Baker's assertion that legal machinations have left the armed forces "unable to fight, or even plan for, a war in cyberspace," Gen Robert Kehler, USAF, commander of US Strategic Command, whose subordinate organization US Cyber Command is the leading proponent of military cyber planning and operations, seems to disagree. In November 2011, he declared that he did "not believe that we need new explicit authorities to conduct offensive operations of any kind." Furthermore, Kehler said that that he did "not think there is any issue about authority to conduct [cyber] operations."[25] In short, the *war fighters* apparently do not see an incompatibility with legal and ethical restraints and their ability to effectively "plan for a war in cyberspace."

Adherence to the rule of law is especially important in the cyber realm because nearly all experts agree that confronting the threat requires the cooperation of foreign countries in order to track and neutralize cyber threats—in peace or war.[26] Nations vital to this effort, including especially the world's major democracies, doubtlessly would not be inclined to cooperate with any country that rejected limits on military operations, cyber or otherwise. Professors Michael Reisman and Chris T. Antoniou point out in their book *The Laws of War* that "in modern popular democracies, even a limited armed conflict requires a substantial base of public support. That support can erode or even reverse itself rapidly, no matter how worthy the political objective, *if*

people believe that the war is being conducted in an unfair, inhumane, or iniquitous way" (emphasis added).[27]

A dismissal of Mr. Baker's construct for cyber war does not suggest, however, that ethical and legal concerns about cyber war are therefore obviated. For example, one of the most serious concerns involves the role of civilians in cyber operations.

Civilian Cyber Warriors

It almost goes without saying that enormous cyber expertise lies in the civilian community and that the armed forces must have access to it. That said, the extent of that access and precisely what that access does—or *should*—mean are properly the subject of legal and ethical scrutiny.

The basics are not hard. To enjoy the combatant privilege—that is, a "license," so to speak, to engage in lawful destructive acts against the enemy's person or property without fear of prosecution—one must ordinarily be a member of the duly constituted armed forces of a belligerent in an armed conflict.[28] People have often mistakenly taken this to mean that a civilian cannot directly participate in hostilities. Actually, civilians can do so without necessarily committing a war crime, but there are consequences.

Chief among them is the fact that if civilians fall into the hands of enemies, they might properly subject them to domestic criminal law for acts that, if done by a member of the opposing military, would be privileged from prosecution. Moreover, under the law of war, civilians are targetable—by either kinetic or cyber means—when they directly participate in hostilities. In the cyber context, one should understand that even the International Committee of the Red Cross explicitly uses as examples of direct participation acts that one would expect of a cyber warrior—that is, "interfering electronically with military computer networks (computer network attacks) and transmitting tactical targeting intelligence for a specific attack."[29]

What does all of this mean from an ethical perspective? For one thing, it is essential that civilians understand the potential consequences, especially when they are away from the work site, such as at home with their families. Despite the debate in the international community about circumstances that would allow an adversary to target a civilian on the same basis as a member of the armed forces, the International Committee of the Red Cross agrees that such targeting applies to civilians who "assume a 'continuous combat function' " (as opposed to merely "participating in hostilities in a spontaneous, sporadic or unorganized way").[30]

Members of the armed forces—along with civilians regularly engaged in a "a continuous combat function" such as computer network attack—can be attacked with any legal weapon wherever and whenever found, regardless of whether at that particular moment they present an imminent threat or are otherwise performing a military function. This means, for example, that a civilian cyber warrior regularly engaged in computer network attack operations could legitimately come under attack by a lawful belligerent (not a terrorist) in his or her home in a Washington suburb. Further, the adversary could use any lawful weapon—not just a cyber weapon—if it otherwise complies with the law of war. Accordingly, if the civilian is sufficiently critical to military cyber operations, he or she could be assaulted with great violence wherever found. However, the incidental death and injury to innocent civilians (e.g., the cyber warrior's own family) that might occur in the attack should not be "excessive in relation to the concrete and direct military advantage anticipated" ("military advantage," of course, refers to the elimination or neutralization of the cyber expert).[31]

Thus, the ethical issue for cyber warriors may be the extent to which one may appropriately ask civilians to take these kinds of risks. It is one thing for members of the armed forces who voluntarily undertake the proverbial "unlimited liability contract" of military service to put themselves at risk. It is quite another to ask civilians to do so—and something further to expect the families of civilians to accept that they

may become collateral damage in a conflict that has violent expressions along with nonkinetic cyber effects. In cyber war, the "front lines" may be far from what anyone might recognize as the traditional battlefield.

No one knows how real this kind of threat might be. However, in an era of "sleeper cells" and the proliferation of other clandestine special operations forces among many countries, this type of counter to America's cyber capabilities may not be as outlandish as some might think. In any event, this discussion of personal risk that cyber operations might occasion makes it somewhat ironic that cyber warriors need to steel themselves for a cruel assault on their ethics and professionalism by some critics.

Challenges to the Martial Ethic of Cyber Warriors?

Perhaps one of the most perplexing critiques that has accompanied the growing use of advanced technologies in war is the penchant among some contemporary commentators to assume that it is somehow "unmanly" or "unworthy" to employ them. Consider the experience of drone operators who, like cyber combatants, wage war from computer consoles. One pundit's very recent article entitled "With Its Deadly Drones, the US Is Fighting a Coward's War" offers an example of the kind of nasty rhetoric used.[32] Though such aspersions have not yet made their way to cyber warriors, it is perhaps only a matter of time before they find themselves subject to the same kind of insult to their professional ethic.

How did all of this start? We might trace it to remarks a few years ago by Dr. David Kilcullen, a lieutenant colonel retired from the Australian army who has become one the foremost advocates of the ground-centric, manpower-intensive form of counterinsurgency that found expression in Field Manual 3-24 / Marine Corps Warfighting Publication 3-33.5, *Counterinsurgency*, published in 2006.[33] It is important to understand that the manual is rather hostile to air operations in

general, devoting just five pages to them in the 300-page document, so Dr. Kilcullen's critique of drones does not seem inconsistent with his broader views about airpower.

In any event, Dr. Kilcullen argued before Congress in 2009 that drone attacks against terrorists were "backfiring": "In the Pashtun tribal culture of honor and revenge, face-to-face combat is seen as brave; shooting people with missiles from 20,000 feet is not." According to Kilcullen, "using robots from the air . . . looks both cowardly and weak."[34] Quite obviously, one might rather easily apply his thesis to cyber operations and those who conduct them.

What makes these statements stunning in their irony is that the adversary to which Kilcullen refers not only uses remotely detonated improvised explosive devices to kill US forces from the safety of distance, but also employs children to plant them.[35] Would that not make such an enemy, by his own "culture of honor" standards, "cowardly and weak"? Regardless, this entire discussion, however demoralizing and inaccurate, is—in terms of actual war fighting—rather immaterial. The "object of war," as Gen George Patton rather graphically put it, "is not to die for your country but to make the other guy die for his."

Physical courage, however admirable, is not the only quality one needs for victory in twenty-first-century warfare—and perhaps ever. Native Americans, for example, waged war with extraordinary courage. Yet, in the April 2012 issue of the *Journal of Military History*, historian Anthony R. McGinnis points out that Native Americans' individualistic and stylized form of warfare was no match for "a modern technologically advanced nation" with "ultimate victory as its goal."[36] Of course, there is nothing wrong with being "a modern technologically advanced nation" with "ultimate victory as its goal" as long as one uses those technological advances in a legally and ethically appropriate way.

In reality, there is nothing unethical about waging war from afar, and there is nothing especially unusual about it. Since practically the beginning of time, warriors have sought to engage their adversaries in

ways that denied them the opportunity to bring their weapons to bear. For example, as this writer has said elsewhere,

> David slew Goliath with a missile weapon before the giant could bring his weapons to bear; the sixteen-foot pikes of Alexander the Great's phalanxes reached their targets well ahead of the twelve foot pikes wielded by their opponents; English longbowmen destroyed the flower of French knighthood at Agincourt from afar when they rained arrows down upon the horsemen; and, more recently, U.S. and British tanks destroyed the heart of Saddam's armor forces during 1991's Battle of 73 Easting much because their guns outranged those of Iraq's T-72 tanks. There is nothing new about killing from a distance.[37]

Still, something about computerized warfare draws special scorn from certain individuals, however wrongly and unfairly. For example, the United Nations commissioned Philip Alston, a New York University law professor, as a "special rapporteur" to write a report on targeted killings. The document he produced included his opinions about drone operators. In it he charged that because drone operations can be conducted "entirely through computer screens and remote audiofeed, there is a risk of developing a 'Playstation' mentality to killing."[38]

A "Playstation" mentality to killing? That even the suggestion of such an insulting lack of professionalism would find itself into an official United Nations report is, itself, disquieting. The principal evidence for Professor Alston's finding appears to be his own speculations about the mind-set of those doing a task he himself has never performed. The actual evidence, however, points in a very different direction than the one Alston suggests—one that reinforces the idea that these officers hardly consider their duties a game. Indeed, Dr. Peter Singer of the Brookings Institution said in 2010 that in his studies he found "higher levels of combat stress among [some drone] units than among some units in Afghanistan." He concluded that operators suffered "significantly increased fatigue, emotional exhaustion and burnout."[39] These maladies are hardly indicative of "game" players.

More recently, the *Air Force Times* quoted an Air Force official who countered the "video game" accusation directly by pointing out that

the responsibilities of drone operators were extremely stressful and that the operations were "a deeply, deeply emotional event. It's not detached. It's not a video game."[40] While debate still roils, it demonstrates how quickly some critics deride the professionalism of principled people doing what their nation asks them to do.[41] Quite obviously, the comparison with cyber operations is not quite the same. Regardless, cyber operators are in the very serious business of defending their country and, in doing so, may be called upon to wreak havoc via cyber methodologies upon an adversary. Though the means of doing so may be different, the professionalism demanded by the operations is very high, and the psychological burdens on those who conduct them are likely very great.

Another aspect of the drone campaigns has emerged that might find analogy in the ethics and professionalism that cyber operators must display. In an April 2012 article in *Rolling Stone*, controversial writer Michael Hastings claims that

> the remote-control nature of unmanned missions enables . . . the Pentagon and the CIA [to] now launch military strikes or order assassinations without putting a single boot on the ground—and without worrying about a public backlash over U.S. soldiers coming home in body bags. The immediacy and secrecy of drones make it easier than ever for leaders to unleash America's military might—and harder than ever to evaluate the consequences of such clandestine attacks.[42]

For all his bluster, Hastings has something of a point when he says that "the immediacy and secrecy of drones make it easier than ever for leaders to unleash America's military might." In this writer's experience, senior decision makers are keenly aware that any military operation can have unintended consequences—no matter how "cost free" it might seem in planning. Still, what he says with respect to drones might find a parallel with cyber operations and could call upon cyber warriors to robustly exhibit ethical virtues, including especially candor and courage.

The Need for Frank, Holistic Advice

The newness of cyber operations, the uncertainty of their precise effect, and the sheer difficulty of their execution may not always be fully understood by all participants in the chain of decision. These conditions may give rise to another ethical responsibility: to render frank, holistic advice. It is possible that in a given situation, those involved in the process may have to step out of their lane, so to speak, to ask the hard questions or point out inconvenient facts. If America's cyber power is to be "unleashed," as Hastings might put it, the nation must do so with the same care as it would with a more traditional military operation. To underline this point, we may call upon someone to go beyond the norm, just to make sure that all the right concerns are taken into account—including ethical and legal ones—so that the best decisions are made.

Fortunately (for lawyers, anyway) the American Bar Association's Model Code of Professional Conduct—the ethical "bible" for lawyers—specifically allows such holistic advice. Rule 2.1 of the code calls upon lawyers to "exercise independent professional judgment and render candid advice." Furthermore, lawyers are not limited to providing legal advice, as the rule goes on to say that "in rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client's situation."[43] In truth, this is the right guidance not just for lawyers but, really, for *all* military and civilian cyber professionals because the success of such operations depends upon a wide range of factors, and it is incumbent upon all involved to work together to ensure that they come to light and receive appropriate consideration.

The American Bar Association's rule mentions candor. Again, this is not something simply for attorneys but a fundamental ethical virtue for all defense professionals.[44] Among other things, one should keep this trait in mind when assessing the potential threat that cyber represents. Misstating or, worse, deliberately misrepresenting the threat can lead to poor allocations of resources and other errors in judgment. Opinions

about the scope and nature of the threat differ widely; in a *PBS Newshour* interview in the spring of 2012, Terry Benzel of the Information Research Institute insists that "all of us in [the cyber] community, we talk about cyber-Pearl Harbor. And it's not if. It's when."[45] Similarly, a "leading European cybersecurity expert says international action is needed to prevent a catastrophic cyberwar and cyberterrorism."[46]

Not everyone agrees, however. In April 2012, Rear Adm Samuel Cox, director of intelligence at US Cyber Command, reportedly "downplayed the prospect that an enemy of the United States could completely disable the nation's electric power grid or shut down the Internet because those systems are designed to withstand severe cyberattacks."[47] More stinging is an article of February 2012 in *Wired*, in which researchers Jerry Brito and Tate Watkins debunk much of the histrionic talk about the threat of cyber war: "Evidence to sustain such dire warnings [about cyberwar] is conspicuously absent."[48] Consistent with their conclusions is a 2011 report by the Organization for Economic Cooperation and Development. Asserting that governments "need to make detailed preparations to withstand and recover from a wide range of unwanted cyber events, both accidental and deliberate," the authors of the study nevertheless conclude "that very few single cyber-related events have the capacity to cause a global shock."[49] Writing in *Foreign Policy*, analyst Thomas Rid contends that cyber war is "still more hype than hazard."[50]

All of this raises concerns because Brito and Watkins say that "in many respects, rhetoric about cyber catastrophe resembles threat inflation we saw in the run-up to the Iraq War." They also point out that "cybersecurity is a big and booming industry" and that "Washington teems with people who have a vested interest in conflating and inflating threats to our digital security." Although they stop short of actually accusing anyone of pushing fears of cyber war for personal gain, they do call for a "stop [in the] apocalyptic rhetoric" and insist that "alarmist scenarios dominating policy discourse may be good for the cybersecurity-industrial complex, but they aren't doing real security any favors."[51]

The scope and immediacy of the threat are rightly debated, yet all might agree that, in any case, deliberately overstating (or understating) the threat—*even for the well-intentioned reasons of advocacy*—can raise questions of ethics and professionalism. As Brito and Watkins suggest, the run-up to the war with Iraq in 2003 makes clear what can happen when a threat is misconstrued (perhaps the reason that they entitle their polemic "Cyberwar Is the New Yellowcake"). In short, candor—and tempered rhetoric *if appropriate*—are critical qualities for cyber warriors. President Obama's measured language, which urges people to take the cyber threat "seriously" and to make planning for it a "priority," represents a responsible approach that highlights the dangers without falling victim to counterproductive and misleading hyping.[52]

The Virtue of Competence

Finally, one of the key ethical responsibilities of cyber warriors is competence. Again, the American Bar Association's Model Rules of Professional Conduct provide guidance that all cyber professionals may want to consider analogizing to their responsibilities. Rule 1.1 of that code says that "competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[53] For those concerned about the legal and ethical aspects of cyber war, the mandate for competence goes well beyond knowledge and understanding of law and/or ethics per se.

Undoubtedly, many aspects of cyber operations are extraordinarily complex. Thus, legal—and other—advisers must become as familiar as possible with the cyber client's "business," including its technical aspects. A working knowledge of the technology not only will help advisers understand the facts sufficiently to apply legal and ethical principles to them, but also will give such advisers all-important *credibility* with those who seek their counsel in the first place. Decision makers in the cyber realm, like those seeking counsel in other activities, naturally will gravitate towards those who show a genuine understanding of the many intricacies of their discipline.

This is not an easy task. Staying current with the technology in this phenomenally complicated field is a time-consuming and never-ending job. But it is one that must be undertaken well in advance of need because failing to do so may lead to a lifetime of regret. Winston Churchill once observed that "to every man, there comes in his lifetime that special moment when he is figuratively tapped on the shoulder and offered that chance to do a very special thing, unique to him and fitted to his talents. What a tragedy if that moment finds him unprepared or unqualified for that which would be his finest hour."[54]

Concluding Observations

This article has sought to illustrate just a few of the examples of how law and ethics might intersect. It may invite the question, Which of these imperatives will best operate to impose the limits on cyber war that honorable, yet pragmatic, people demand? Kenneth Anderson, a professor of law at American University, recently had occasion to consider one of his earlier writings about the efficacy of law and honor as "engines" for right behavior in conflict:

> Faith in legality as the engine driving such adherence as exists to the laws of war seems to me, however, entirely misplaced; it is a fantasy tailor-made for lawyers, and especially for American lawyers. Lawyers believe the problem is one of enforcement, whereas in fact it is one of allegiance. Codifications of international law are a useful template for organizing the categories of a soldier's duties. But, in the end, the culture relevant to respect for international humanitarian law is not the culture of legality and the cult of lawyers, but instead it is the culture of the professional honour of soldiers, and what they are willing or not willing to do on the battlefield.[55]

The question of whether "honor" is conterminous with ethics or a subset of the same may be appropriate for a lively university debate. What is more important to note, however, as Anderson does, is that John Keegan, perhaps the most eminent military historian of the modern era, had no reservations in saying that "there is no substitute for

honour as a medium for enforcing decency on the battlefield, never has been, and never will be."[56]

The cyber "battlefields" may not much resemble the ones to which Keegan refers, but his view certainly has equal applicability. In the end, honor and the ethical mind-set it implies are indispensable. Yet the discussion cannot end there because merely having developed the character to come to know the right answer is not enough since it may take courage to insist upon it.

The courage that cyber warriors need is not necessarily the *physical* courage that traditional battlefield combatants are called upon to display. Rather, it is vastly more likely that cyber combatants will need to exhibit *moral* courage.[57] This is especially so as norms develop for the conduct of cyber operations. Doing the right thing, particularly in circumstances of extreme urgency for which we have no explicit guidance—save for reference to classic tenets of law and ethics—may be quite a challenge.

Cyber combatants may wish to consider that in his classic study of military heroism, another British historian, Max Hastings, concludes that "physical bravery is found [in the military] more often than the spiritual variety." "Moral courage," he insists "is rare."[58] Yet, cyber warriors most need to exhibit exactly this kind of "rare." The law can provide an architecture, but only when honor and moral courage intersect can we truly rest assured that ethical principles worth defending are actually preserved. ✪

Notes

1. Barack Obama, "Taking the Cyberattack Threat Seriously," *Wall Street Journal*, 19 July 2012, http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html.

2. For example, the International Law Division of the US Naval War College held a conference devoted to the legal aspects of cyber war in June 2012. See "2012 ILD Conference," US Naval War College, accessed 25 September 2012, http://www.usnwc.edu/ILDJune2012.

3. See, for example, Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (December 2010): 384, 385. "There are no informed, open, public or political discussions of what an ethical and wise policy for the use of such [cyber] weapons would be" (ibid., 385).

4. "McCain Conference: Warfare in a New Domain; The Ethics of Military Cyber Operations," United States Naval Academy, Stockdale Center for Ethical Leadership, 26–27 April 2012, http://www.usna.edu/ethics/publications/mccain2012.php. Much of this article comes from a presentation the author made at this conference.

5. Patrick Lin, Fritz Allhoff, and Neil Rowe, "Is It Possible to Wage a Just Cyberwar?," *Atlantic*, 5 June 2012, http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/.

6. Geoffrey Best, *War and Law since 1945* (Oxford, UK: Oxford University Press, 1994), 289.

7. Lt Gabriel Bradley, "Honor, Not Law," *Armed Forces Journal* 149, no. 7 (March 2012), http://www.armedforcesjournal.com/2012/03/9563756.

8. Harold Hongju Koh, legal advisor, Department of State, "International Law in Cyberspace" (remarks, USCYBERCOM Interagency Legal Conference, Fort Meade, MD, 18 September 2012), http://www.state.gov/s/l/releases/remarks/197924.htm.

9. Program on Humanitarian Policy and Conflict Research, *Manual on International Law Applicable to Air and Missile Warfare* (Cambridge, MA: Program on Humanitarian Policy and Conflict Research, Harvard University, 2009), http://ihlresearch.org/amw/HPCR%20Manual.pdf.

10. See, for example, Roger Crisp, "Cyberwarfare: No New Ethics Needed," *Practical Ethics* (blog), 19 June 2012, http://blog.practicalethics.ox.ac.uk/2012/06/cyberwarfare-no-new-ethics-needed/.

11. These terms are used, for example, in Article 2 and Article 52, respectively, of the Charter of the United Nations. United Nations, *Charter of the United Nations and Statute of the International Court of Justice* (Washington, DC: Government Printing Office, 1946), http://treaties.un.org/doc/Publication/CTC/uncharter.pdf.

12. "Over the last two years, DoD has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America." Secretary of Defense Leon E. Panetta (remarks on cybersecurity to the Business Executives for National Security, New York City, 11 October 2012), http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

13. Lin, Allhoff, and Rowe, "Is It Possible?"

14. Ibid. If, for example, one can make a factual case for the proper application of the doctrine of anticipatory self-defense by a nation-state, then Iran would have neither a legal nor a moral basis to respond. For a discussion of anticipatory self-defense, see, generally, Kinga Tibori Szabó, *Anticipatory Action in Self-Defence: Essence and Limits under International Law* (Hague, Netherlands: T. M. C. Asser Press, 2011).

15. See, for example, Crisp, "Cyberwarfare," 9.

16. Lin, Allhoff, and Rowe, "Is It Possible?"

17. Harold Koh, legal adviser for the US State Department, explains the terms: "First, the principle of *distinction*, which requires that attacks be limited to military objectives and that civilians or civilian objects shall not be the object of the attack; and second, the principle of

proportionality, which prohibits attacks that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, that would be excessive in relation to the concrete and direct military advantage anticipated" (emphasis in original). Harold Hongju Koh, "The Obama Administration and International Law" (speech, Annual Meeting of the American Society of International Law, Washington, DC, 25 March 2010), http://www.state.gov/s/l/releases/remarks/139119.htm.

18. Stewart A. Baker and Charles J. Dunlap Jr., "What Is the Role of Lawyers in Cyberwarfare?," *ABA Journal*, 1 May 2012, http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/.

19. Ibid.

20. Ibid.

21. Ibid.

22. Ibid.

23. Ibid.

24. Charles J. Dunlap Jr., "Lawless Cyberwar? Not If You Want to Win," American Bar Association, accessed 21 September 2012, http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch9/ch9_ess2.html.

25. Quoted in Jim Wolf, "U.S. Military Better Prepared for Cyber Warfare: General," Reuters, 16 November 2011, http://www.reuters.com/article/2011/11/17/us-usa-cyber-military-idUSTRE7AG03U20111117?feedType=RSS&feedName=everything&virtualBrandChannel=11563.

26. See, for example, Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 9, http://www.defense.gov/news/d20110714cyber.pdf. "Cyberspace is a network of networks that includes thousands of [Internet service providers] across the globe; no single state or organization can maintain effective cyber defenses on its own" (ibid.).

27. W. Michael Reisman and Chris T. Antoniou, eds., *The Laws of War: A Comprehensive Collection of Primary Documents on International Laws Governing Armed Conflict* (New York: Vintage Books, 1994), xxiv.

28. See, generally, Gary D. Solis, *The Law of War* (New York: Cambridge University Press, 2010), 41–42.

29. "Direct Participation in Hostilities: Questions and Answers," International Committee of the Red Cross, 6 February 2009, http://www.icrc.org/eng/resources/documents/faq/direct-participation-ihl-faq-020609.htm.

30. Ibid.

31. Koh, speech.

32. George Monbiot, "With Its Deadly Drones, the US Is Fighting a Coward's War," *Guardian* (United Kingdom), 30 January 2012, http://www.guardian.co.uk/commentisfree/2012/jan/30/deadly-drones-us-cowards-war.

33. Field Manual 3-24 / Marine Corps Warfighting Publication 3-33.5, *Counterinsurgency*, December 2006, http://armypubs.army.mil/doctrine/DR_pubs/DR_a/pdf/fm3_24.pdf.

34. Quoted in Doyle McManus, "U.S. Drone Attacks in Pakistan 'Backfiring,' Congress Told," *Los Angeles Times*, 3 May 2009, http://articles.latimes.com/2009/may/03/opinion/oe-mcmanus3.

35. Christopher Leake, "Taliban Make Children Plant IEDs to Thwart Army Snipers," *Daily Mail*, 6 February 2010, http://www.dailymail.co.uk/news/article-1249044/Taliban-makes-children-plant-IEDs-thwart-Army-snipers.html.

36. Anthony R. McGinnis, "When Courage Was Not Enough: Plains Indians at War with the United States Army," *Journal of Military History* 76, no. 2 (April 2012): 473.

37. Charles J. Dunlap Jr., "Does Lawfare Need an Apologia?," *Case Western Reserve Journal of International Law* 43, no. 1/2 (2011): 132.

38. United Nations, General Assembly, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston: Addendum, Study on Targeted Killings*, A/HRC/14/24/Add.6 (New York: United Nations, General Assembly, 28 May 2010), 25, http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf.

39. Marc Pitzke, "Interview with Defense Expert P. W. Singer: 'The Soldiers Call It War Porn,' " *Spiegel Online International*, 12 March 2010, http://www.spiegel.de/international/world/0,1518,682852,00.html.

40. Jeff Schogol and Markeshia Ricks, "Demand Grows for UAV Pilots, Sensor Operators," *Air Force Times*, 21 April 2012.

41. See, for example, Kenneth Anderson, "Laurie Blank on Mark Mazzetti's 'The Drone Zone'—Last in Series from Lewis, Dunlap, Rona, Corn, and Anderson," *Lawfare* (blog), 21 July 2012, http://www.lawfareblog.com/2012/07/laurie-blank-on-the-mazzetti-the-drone-zone-last-in-series-from-lewis-dunlap-rona-corn-and-anderson/.

42. Michael Hastings, "The Rise of the Killer Drones: How America Goes to War in Secret," *Rolling Stone*, 16 April 2012, http://www.rollingstone.com/politics/news/the-rise-of-the-killer-drones-how-america-goes-to-war-in-secret-20120416#ixzz22VDkfR00.

43. "Rule 2.1: Advisor," American Bar Association, Center for Professional Responsibility, accessed 25 September 2012, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_2_1_advisor.html.

44. Compare the following from the listing of "Primary Ethical Values" found in the Department of Defense's *Joint Ethics Regulation*:

a. Honesty. Being truthful, straightforward and *candid* [emphasis added] are aspects of honesty.

> (1) Truthfulness is required. Deceptions are easily uncovered and usually are. Lies erode credibility and undermine public confidence. Untruths told for seemingly altruistic reasons (to prevent hurt feelings, to promote good will, etc.) are nonetheless resented by the recipients.
>
> (2) Straightforwardness adds frankness to truthfulness and is usually necessary to promote public confidence and to ensure effective, efficient conduct of Federal Government operations. Truths that are presented in such a way as to lead recipients to confusion, misinterpretation or inaccurate conclusions are not productive. Such indirect deceptions can promote ill-will and erode openness, especially when there is an expectation of frankness.
>
> (3) *Candor is the forthright offering of unrequested information. It is necessary in accordance with the gravity of the situation and the nature of the relationships. Candor is required when a reasonable person would feel betrayed if the information were withheld. In some circumstances, silence is dishonest, yet in other circumstances, disclosing information would be wrong and perhaps unlawful*. (emphasis added)

Department of Defense Regulation 5500.07-R, *Joint Ethics Regulation*, 17 November 2011, 118, http://www.dtic.mil/whs/directives/corres/pdf/550007r.pdf.

45. "Preventing a 'Cyber-Pearl Harbor,' " *PBS Newshour*, 16 April 2012, http://www.pbs.org/newshour/bb/science/jan-june12/deterlab_04-16.html.

46. "Expert Warns on Cyberwar Threat," UPI.com, 16 March 2012, http://www.upi.com/Science_News/2012/03/16/Expert-warns-on-cyberwar-threat/UPI-33781331937216/#ixzz1sRYZauJc. The article cities Eugene Kaspersky, chief executive officer and cofounder of Kaspersky Lab, the self-described largest antivirus company in Europe.

47. Quoted in Richard Lardner, "US Needs Top-Level Approval to Launch Cyberattacks," *Salon*, 24 April 2012, http://www.salon.com/2012/04/24/us_needs_top_level_approval_to_launch_cyberattacks/.

48. Jerry Brito and Tate Watkins, "Wired Opinion: Cyberwar Is the New Yellowcake," *Wired*, 14 February 2012, http://www.wired.com/threatlevel/2012/02/yellowcake-and-cyberwar/.

49. Peter Sommer and Ian Brown, *Reducing Systemic Cybersecurity Risk* ([Paris, France:] Organization for Economic Cooperation and Development, 14 January 2011), 5, http://www.oecd.org/dataoecd/57/44/46889922.pdf.

50. Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, no. 192 (March/April 2012): 80, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full.

51. Brito and Watkins, "Wired Opinion."

52. Obama, "Taking the Cyberattack Threat Seriously."

53. "Rule 1.1: Competence," American Bar Association, Center for Professional Responsibility, accessed 25 September 2012, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html.

54. Quoted in Maj Gen Stephen R. Lorenz, "Lorenz on Leadership," *Air and Space Power Journal* 19, no. 2 (Summer 2005): 7–8.

55. Kenneth Anderson, "Sir John Keegan, Ave Atque Vale," *The Volokh Conspiracy* (blog), 3 August 2012, http://www.volokh.com/2012/08/03/sir-john-keegan-ave-atque-vale/.

56. Quoted in ibid.

57. The author has discussed the need for moral courage elsewhere. See, for example, Charles J. Dunlap Jr. "The Ethical Issues of the Practice of National Security Law," *Ohio Northern University Law Review* 38 (2012): 1093–95.

58. Max Hastings, *Warriors: Portraits from the Battlefield* (New York: Vintage Books, 2005), xvii.

Maj Gen Charles J. Dunlap Jr., USAF, Retired

General Dunlap (BA, St. Joseph's University; JD, Villanova University School of Law) is the executive director of the Center on Law, Ethics and National Security at Duke University Law School. His 34-year career as judge advocate included tours in both the United Kingdom and Korea, and he deployed for military operations in Africa and the Middle East. A distinguished graduate of the National War College, General Dunlap has recently published such cyber-related pieces as "Perspectives for Cyber Strategists on Law for Cyberwar" (*Strategic Studies Quarterly*, Spring 2011) and "Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors" (*Nebraska Law Review*, 2008). He and Stuart Baker debate cyber law issues in *Patriots Debate: Contemporary Issues in National Security Law*, published in 2012 by the American Bar Association.

Let us know what you think! Leave a comment!

Refocusing Cyber Warfare Thought

Maj Sean C. Butler, USAF

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

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

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

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

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

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

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

Cyberspace as a Physical Domain

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The Unique Character of Cyberspace

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

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

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

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

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

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

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

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

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

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

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

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

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

Conclusion

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

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

Notes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15. Ibid., 5.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Maj Sean C. Butler, USAF

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

The Interim Years of Cyberspace

1st Lt Robert M. Lee, USAF

> *There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success than to take the lead in the introduction of a new order of things.*
>
> —Machiavelli

Cyber power will be as revolutionary to warfare as airpower, but the current vectoring of the domain will determine which nation will hold cyber dominance and to what effect. In the early years of the cyberspace domain, the United States primarily considered cyber power a means of establishing broad command and control across the war-fighting domains. Cyberspace focused on communication; indeed, operational success depended upon maintaining the lines of communication. As the domain grew, it assumed additional roles to provide a support force to traditional military operations while experts explored other roles—a process that occurred at the highest levels of secrecy. Many of the first cyberspace leaders realized that cyber assets offered a number of options for attack, defense, and exploitation never

before afforded to military commanders. In a highly connected world where substantial advancements in technology were common, the capabilities and weapons in cyberspace became even more impressive.

The current stage of cyberspace development resembles the interim years between World War I and World War II, when airpower responded to challenges by emerging as a powerful military tool. No comparison does better justice to contemporary cyberspace than airpower during those foundational years. At that time, theorists and military officers, including Gen Giulio Douhet, Marshal of the Royal Air Force Hugh Trenchard, and Brig Gen William "Billy" Mitchell, helped guide the direction of airpower. As cyberspace reaches its full potential as a domain of warfare equal to the traditional domains, we—like those leaders—must vector it properly.

Toward that end, this article discusses airpower during the interwar period as well as key lessons learned that we can apply to the cyberspace domain. It then offers three suggestions that address the vectoring of the cyberspace domain: empowering commanders with actionable cyber intelligence, defending the nation with a combined civilian-military approach, and developing a long-term strategy for the domain by embracing the cyber culture and educating our young leaders in cyber. Understanding the past, applying lessons learned, and planning the way forward will allow us to secure true cyberspace dominance.

The Interim Years of Airpower

Prior to World War I, the use of aircraft was extremely limited, and many people did not consider them a viable military option. For example, in *Aeronautics* (1908) William H. Pickering, a notable American astronomer, observed that "another popular fallacy is to suppose that flying machines could be used to drop dynamite on an enemy in a time of war."[1] Only six years later, on 14 August 1914, a French Voisin aircraft bombed German zeppelin hangars at Metz-Frascaty.[2] The idea of conducting aerial warfare quickly gained prominence. The next few

years saw the development of strategic-bombing aircraft and their use in air actions such as the raids by German Gothas on England.[3] However, the employment of aircraft and balloons in warfare was not new. In China during the third century, Gen Zhuge Liang signaled military forces and scared away enemies with balloons known as Kongming lanterns.[4] Yet, only advancements in technology and powerful demonstrations of force in World War I could expedite the domain's importance and use.

The success of airpower in that war, including Lt Frank Luke Jr.'s destruction of 14 heavily guarded German balloons, convinced several military leaders that aircraft could support the traditional domains of land and sea warfare.[5] The debate at the time did not concern whether or not to use airpower but the means of developing it and determining which branch of service would take the lead. In the years between the world wars, aviation concentrated on defending the nation from adversaries.[6] However, some of those defensive capabilities also offered offensive possibilities. The flexibility of airpower created intense debates between the Army and Navy because Army Air Corps aircraft could fill traditional Navy roles.

In 1921 General Mitchell used MB-2 bombers from Langley Field, Virginia, to sink three naval vessels, including the *Ostfriesland*, a modern battleship captured from the Germans.[7] This test demonstrated that aircraft could independently attack offshore targets. It also showed that if the Army continued to empower the Air Corps, the Navy might lose its primary mission of coastal defense.

Partially in rebuttal to General Mitchell's test, in 1925 the Navy revealed a plan to increase the number of its shore-based aircraft from 334 to 583.[8] Maj Gen Mason Patrick, chief of the Air Service, saw this as a move by the Navy Department to take control of the entire coastal defense mission.[9] This dispute between the Army and Navy continued to escalate, and leaders of both services worried that if they could not find a solution, Congress might create an independent air corps.[10] Attempts by the War Department and Congress to satisfy both services

proved fruitless.[11] Amidst the services' disagreement, General Mitchell strongly advocated the establishment of a separate branch of service and attempted to win the support of the public in an effort to pressure Congress to act.[12] After his court-martial, he resigned from the Army Air Service in 1926 but continued to campaign publicly for an independent Air Force.[13]

In 1934 Gen Henry "Hap" Arnold received a tasking to fly from Dayton, Ohio, to Alaska with 10 Martin B-10 bombers. On the return trip, he detoured from his route by flying over the ocean instead of across Canada, not only demonstrating the bombers' coastal range but also enraging Gen Douglas MacArthur, the Army chief of staff.[14] Nevertheless, members of Congress and the War Department ultimately embraced the claims of such individuals as Arnold and Mitchell that the nation needed an independent Air Force.

Lessons Learned from Airpower

The cyberspace domain need not be a separate branch of service. However, the true potency of cyber power remains unrealized, as was the case with airpower in the early years of the aerial domain. If we understand this, we can extract key lessons learned from the nascent aerial domain and apply them to the development of the cyberspace domain.

Lesson One: A Unified Military Approach Is More Beneficial to Securing a Domain of Warfare

One of the issues with realizing the potential of the aerial domain concerned early competition between the Army and Navy over its control—competition that led to creation of the Air Force. That service acted as a combined and vectored national approach to creating better aerial technologies and strategies. Had its establishment occurred sooner, the Air Force may have generated even more gains. In this way, cyber power has an advantage. The cyberspace domain does not encroach upon the traditional roles of the Army, Air Force, or Navy.

The cyber mission can work both independently from, and synergistically with, the traditional war-fighting domains across each branch. This combined approach from the services benefits the entire domain, and although we should encourage competition among the services, each one should play a significant role.

Lesson Two: Airpower Had the Ability to Make Influential Political Statements That Transcended Its Own Destructive Capability

Cyber power, very much like airpower, can be a destructive force if wielded alone and to full measure. Early Airmen took pride in believing that aerial attacks by themselves could lead to victory; however, they understood neither its destructiveness if left unchecked nor the importance of limiting conflict.[15] During the Vietnam War, President Lyndon Johnson and Secretary of Defense Robert McNamara met weekly to discuss the targets that pilots would bomb. Once considered political micromanagement, this handpicking of targets controlled the political implications of aerial attacks.[16] The new—and in many cases frightening—power brought by bombing raids made a strong statement not only to North Vietnam but also to other nations watching closely. Similarly, cyber power can make influential statements, and we should not wield it indiscriminately. A cyber attack that collapses the global stock market, disables a fleet of naval warships, or crashes the latest development in aircraft will have enormous political consequences.

Lesson Three: Like Airpower, Cyber Power's Technologically Advanced Nature Allows It to Blur the Lines of War; Thus, We Must Wield It Responsibly

Douhet believed that the range of aircraft would permit the targeting of civilians and combatants alike in future wars. Airpower, he reasoned, did not know the limits of traditional battlefields and could act without inhibition. Without boundaries on the battlefield, no areas would feel safe to civilians.[17] Cyber power, too, can quickly and specifi-

cally target networks and information systems throughout the world, blurring the lines of battlefields. This characteristic, in conjunction with its destructive force, generates fear of its capabilities among the population—one just as strong as that from terrorist attacks. Consequently, we cannot underestimate its power to influence popular opinion and politics or its ability to guide the development of cyber capability. When a nation uses cyber power, it must first carefully evaluate its own citizens' sense of security and the effects that cyber assets will have on that feeling after their employment.

Lesson Four: The Nature of War Is Not Limited by Technological Advancements

Nevertheless, the idea that technology will eliminate the ugliness of war has influenced military planners throughout history.[18] Douhet believed that the inherently offensive nature of airpower, later famously reinforced by Sir Stanley Baldwin's statement that "the bomber will always get through," would curtail bloodshed during war.[19] To him, bombing cities and attacking civilians would result in fewer deaths than would the clash of armies.[20] The Italian general thought that strategic bombing would break the morale of civilians, prompting them to demand that their leaders end wars early. Instead, aerial bombing raids usually bolstered civilian morale against the known enemy.[21] Without proper attribution, though, in cyberspace the enemy may remain unknown, creating unspecified effects on the civilian population, perhaps including broken morale. Regardless of the effects of an unknown cyber attacker, technology cannot end bloodshed. Therefore, we must employ cyber's capabilities with the understanding that proper use can limit casualties but that overuse can equally encourage them. War will always be an ugly thing.[22]

Lesson Five: Airpower Used a Varied Approach to Secure the Domain, and So Must Cyber Power

General Mitchell did not consider bombers the quintessential form of airpower, believing instead in the necessity of multiple types of aircraft, including those with offensive and reconnaissance missions.[23] His concept of airpower is more akin to the current diverse nature of cyber power and varied cyber assets, which can support national defense, intelligence gathering, and offensive actions—and do so just as well as or better than other military assets. Multiple types of aircraft enabled the development of persistent intelligence, surveillance, and reconnaissance (ISR) aerial platforms and offensive air capabilities, which help ensure air dominance and support to other war-fighting domains.[24] The addition of a variety of cyberspace capabilities directly enhances already-established ISR and offensive operations while enabling the development of new ones.

Commanders and Actionable Cyber Intelligence

Vectoring the cyberspace domain should involve empowering commanders with more actionable intelligence through cyber capabilities. Cyber power offers critical advantages to campaign planning; consequently, intelligence-based cyber operations should become part of the preparation of the operational environment phase, which includes compromising enemy networks and readying cyber weapons for use in the event of conflict. During the posturing for offensive cyber operations, information exploited from compromised systems can aid in the joint intelligence preparation of the operational environment, improving commanders' situational awareness of the battlefield.[25]

Commanders use campaign planning to "synchronize efforts" and issue complementary guidance.[26] The two major phases of the planning process—contingency planning and crisis action planning—benefit from the timely information and attack options that cyber power pres-

ents, including an understanding of enemy capabilities and strategies. Having the assumptions and plans made in the contingency phase more closely match the crisis action phase expedites the joint operation planning process.[27] This quick-selection process empowers commanders with the ability to strike first, target precisely, and more readily defend counterattacks. Information gathered from the preparation of the operational environment phase also decreases the effectiveness of the enemy's attempts at deception.

With access to military doctrine, enemy forces may choose to avoid efficient courses of action or even fake them. The combination of cyber and ISR capabilities can detect these deceptions. Multiple ISR platforms such as manned aircraft, remotely piloted aircraft, and satellites, as well as human-gathered intelligence, contribute to creation of the intelligence preparation of the battlespace.[28] Individually, cyber and ISR severely weaken the enemy's ability to hide troops, sensitive information, operational plans, and centers of gravity. The combination of the two through imagery intelligence, signals intelligence, human intelligence, and computer network operations provides an unprecedented level of battlefield situational awareness to commanders. This awareness can also enable cyberspace operations, whose capabilities include weapon systems platforms that degrade, disrupt, and destroy an adversary's communication, control, and physical assets. The enhanced situational awareness that cyber and ISR give to commanders aids in creation of holistic and realistic statements of the commander's intent, as discussed in the joint operation planning process model. Better statements make the planning guidance more accurate and assist in the selection of effective courses of action.[29]

With adversaries relying heavily on cyberspace for communication, the number of capabilities offered to commanders to collect, exploit, and disrupt this information has never been greater. These options, which exist throughout all military operations, could help minimize what military theorist Carl von Clausewitz referred to as the fog of war.[30] However, many commanders cannot access them. If shared properly, cyber

operations would increase the chances for operational success in other domains and restrict the human and financial costs of war.

These cyber capabilities have not gone unnoticed, though, and the stand-up of US Cyber Command indicates that the cyberspace domain is moving in the right direction.[31] However, we need to do more to supply commanders with actionable intelligence and capabilities through cyber operations. Regarding the direction of cyberspace, Maj Gen Brett T. Williams, director of operations (J3) for US Cyber Command, called for empowering joint force commanders and combatant commands (COCOM) with cyber capabilities and command and control of cyber operations. A lack of visibility of cyber components critical to a mission's success puts commanders at a disadvantage. Major General Williams suggested creation of the Theater Cyber Operations Command, similar to a Theater Special Operations Command, to provide geographic combatant commanders with cyber capabilities under the control of COCOMs.[32] Establishing a method similar to this one would give commanders more actionable intelligence, and they could then request cyber capabilities relevant to their mission. Having the cyber situational awareness to accurately request capabilities is one of the most critical components of leveraging cyber power. This aspect has gained attention since Major General Williams made his observations. In the summer of 2011, Gen Keith Alexander, head of US Cyber Command, discussed progress in supporting operations in Iraq and Afghanistan through the deployment of expeditionary teams, especially in terms of combatant commanders' ability to request cyber support.[33]

Much work in the cyberspace domain remains with regard to delivering cyber intelligence and capabilities to commanders. After the establishment of more direct approaches for doing so, classification of the information becomes the limiting factor in making it actionable. To protect cyber capabilities, we must not reveal certain details and technologies that would allow adversaries to counter or safeguard against them. Currently, however, the intelligence and information gathered from cyber capabilities are overclassified. Commanders cannot request

capabilities they don't know about. Instead of providing processes to request cyber, we must make an effort to declassify cyber intelligence and information that does not weaken cyber capabilities. Doing so will not only support commanders but also enable tactical-level leaders to make reasonable requests to their leadership in support of daily operations. Moreover, the declassification of some cyber intelligence and information would allow more sharing among government agencies and civilian leaders who operate in law enforcement agencies. Perhaps even more important, the sharing of actionable cyber intelligence that could assist network defenses would enable civilian leadership to better protect sectors such as critical infrastructure. This sharing of information would directly correlate with improvements in national security.

Cyber Weapons and the Home Front

During these interim years of cyberspace, increased civilian-military partnership for the defense of the nation would also prove advantageous. Recent cyber events have shown that the level of versatility and expertise in select cyber weapons can overpower even carefully crafted defenses. The combined experience and knowledge of military and civilian professionals can better protect against these advanced threats. No better example of advanced cyber threats currently exists than the dangers associated with Stuxnet.

In June 2010, the Stuxnet worm came to light and quickly gained notoriety as one of the most advanced pieces of malware ever discovered. The worm, which self-replicates and spreads among information systems, takes advantage of an unprecedented four unpatched vulnerabilities—known as zero-day vulnerabilities—while employing a root kit (a piece of code that enables persistent access), two command and control servers, and legitimate signed certificates.[34] The code consists of two sections: the weapon system and the payload, the former quite impressive and containing the aforementioned features but paling in comparison with the advanced nature of the payload.

Stuxnet was specifically designed to target supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS). More accurately, the payload specifically targeted programmable logic controllers (PLC) that governed the centrifuges at the Iranian nuclear facility in Natanz. The worm's payload physically damaged the centrifuges by spinning them up and slowing them down to precisely the appropriate speeds for maximum degradation.[35] Although the full outcomes of the worm remain unknown, satellite imagery indicates that over 1,000 of the centrifuges were destroyed.[36] This feat required not only some of the best programmers and ICS/PLC engineers in the world but also a better understanding of the secretive Natanz facility's layout than most of the engineers that worked there would have had.[37]

Largely seen as a cyber weapon created and employed by at least one nation-state, Stuxnet launched intense discussions and multiple academic papers on the use of cyberspace as a domain of warfare. The Russian ambassador to the North Atlantic Treaty Organization even went so far as to state that the Stuxnet worm could have caused "a new Chernobyl" if the program had released the uranium gas in the centrifuges instead of causing degradation.[38] Though operations had previously taken place in cyberspace, the media portrayal of the power of the Stuxnet cyber weapon made the discussion of cyber warfare a very public one. Stuxnet did for cyberspace what the early bombings in World War I did for airpower; that is, it brought the discussion to the public and undoubtedly forced many corporations and nation-states to research cyber capabilities more heavily. In a way, this event—coupled with past cyber operations over the last few decades, including the attacks against government and financial sectors in Estonia in 2007 and those that coincided with the Russian invasion of Georgia in 2008—represents the start of the interim years of cyberspace.[39]

Although Stuxnet infected and spread to thousands of computer systems, its only recognized targets were the centrifuges at Natanz. The event did not greatly affect systems in the United States or reach the level of a cyber attack that would push a nation into war. However, ac-

cording to Secretary of Defense Leon Panetta, "The potential for the next Pearl Harbor could very well be a cyber attack."[40] This observation, coupled with General Alexander's statements that segments of the nation's critical infrastructure are not prepared to handle cyber attacks and that this situation worries him the most, makes obvious the paramount importance of protecting these assets from cyber attacks.[41] Furthermore, Stuxnet has shown that these cyber capabilities exist and have been utilized by at least one nation-state.

The Stuxnet story is not over, though. The laboratory that discovered the piece of malware now known as Duqu on 14 October 2011 quickly recognized its relationship to the Stuxnet malware. Duqu differs from Stuxnet in that it is a targeted remote-access Trojan that steals information instead of a worm that damages centrifuges.[42] It infected a number of different sites, including universities, manufacturers, and certificate authorities in a style of attack that gathers data to use in making another Stuxnet-styled cyber weapon.[43] Although different in style and targets, Duqu uses much of Stuxnet's source code, and the same coding team, utilizing a common coding platform named Tilded, seems to have produced both pieces of malware.[44]

Similar to a "Lego set," the Tilded platform lends itself to putting together different pieces or modules of code to create entirely different malware.[45] This platform-based approach allows a team to create a quickly adaptable cyber weapon that can use different modules and payloads for employment against very different targets and produce different outcomes. Additionally, the malware created from the platform can be updated with different stealth measures, including the changing of encryption algorithms used to hide its code—as occurred with an updated version of Duqu found in February 2012.[46]

Aerial warfare has taken a platform-based approach to weaponry for years. Instead of creating aircraft with single functions, the Department of Defense (DOD) has purchased aircraft such as the F-16, F-22, and MQ-1, which can fulfill completely different mission sets based on their type of payload. Evidently this approach is now catching on in

the cyberspace domain, posing a number of risks to various aspects of national security. A single cyber weapon platform could steal information from universities and manufacturers to create multiple cyber weapons that would then attack aircraft, Internet nodes essential to command and control, air defense systems, and critical infrastructure.

Gen Norton Schwartz, former Air Force chief of staff, stated that the Air Force is pursuing "cyber methodologies to defeat airborne threats," but other sources have indicated that the technology is already available.[47] During testimony to the Senate Armed Services Committee, Lt Gen Herbert Carlisle stated that "the Russians and the Chinese have designed specific electronic warfare platforms to go after our high-value assets. Electronic attack can be the method of penetrating a system to implant viruses."[48] As traditional platform-based weapon systems become more diverse and utilize more capabilities, such as advanced radar systems, they become more vulnerable to cyber attacks. These cyber vulnerabilities make the benefits of cyber weapon platforms more alluring to adversaries. Such weaknesses, combined with the capabilities demonstrated by the Tilded platform, suggest that the threat of a future platform-based cyber weapon system attacking multiple DOD and civilian sectors is not merely possible but probable. We cannot defend against the power of such weapons without a combined military-civilian approach.

In these interim years of cyberspace, the government must ensure national security by encouraging cooperation with civilian leadership in sectors such as critical infrastructure. Operators, engineers, and developers of that infrastructure possess keen insight into the systems that demand active protection, yet they can supply full details about their systems and their understanding of them only when they receive actionable intelligence from the government. Armed with declassified intelligence, civilian counterparts can give better advice about defending systems they have operated for years. Just as it makes sense to classify some cyber offensive capabilities, so should we leave some cyber defense capabilities classified as well. Some cyber defenses,

though, should be largely transparent so that we can identify and remediate weaknesses.[49]

Even non-cyber-related ICS and SCADA system incidents can produce significant, drastic effects on civilian populations. On 17 August 2009, the 245-meter-high Shushenskaya dam—the largest in Russia—experienced an ICS failure that shook south central Siberia. A break in communications produced by a fire at a power station more than 500 miles away caused a sudden surge of water pressure that ripped apart a 940-ton turbine. The incident resulted in the death of 75 people and $1.3 billion in rebuilding costs.[50] Neither a cyber attack nor the action of any nation-state, the incident could have occurred as a result of a deliberate cyber strike and could have generated more civilian deaths and financial costs.

The Natanz nuclear enrichment facility and the Shushenskaya dam are only two examples of the uses of ICS and SCADA systems, which affect every aspect of daily life, including the stock market, oil industry, electrical power grid, water filtration, and Internet and satellite communication networks. Thus, these systems have become one of the most sought-after and viable targets of cyber weapons based in nation-states and must be treated accordingly. We can properly protect them only with a unified civilian-military approach.

Winning the Next Generation

Lastly, embracing a long-term strategy for developing the cyber culture and educating the next generation of cyberspace operators, including the nation's youth, would help establish dominance in the cyberspace domain. Severe shortages exist in the availability of skilled cybersecurity professionals to fill such jobs as investigative forensics and programming at the FBI Cyber Division.[51] Further, the DOD finds itself in a difficult position in terms of educating the next generation. Dr. Michael Wertheimer, the National Security Agency's director of research and development, briefed members of the Senate Armed Ser-

vices Subcommittee on problems in recruiting and retaining professionals in computer science, pointing out that 77 percent of the agency's information technology staff resigns rather than retires.[52] We may need to address the issue of paying salaries competitive with those in private industry, but our long-term strategy must look to lessons learned from the aerial domain.

Excitement and a sense of magic surrounded airplanes and their pilots during the early days of airpower. Those flyers braved dangerous situations in an unchartered domain to break records and mesmerize crowds. France's Reims Air Meet of 22 August 1909, the world's first major air show, opened the door for many more around the globe.[53] Such shows and air races both inspired future pilots and educated the public on the capabilities of airpower.[54] The National Air Races, held in 1929 during the interwar years, attracted even more attention, drawing more than half a million people.[55]

The golden age of the 1920s embodied the allure of flying. Pilots wanted to fly higher, faster, and farther than anyone else. Three times between 1919 and 1921, Army pilots broke the world record for altitude.[56] Cyber operators, however, do not have to brave dangerous speeds and acrobatics, but cyber capabilities can certainly captivate audiences and inspire the next generation of cyber operators.

Hacking and security conferences demonstrate the latest in security advancements, vulnerabilities, and exploits. These conferences also offer a way for those in attendance to network with people from a variety of backgrounds who all have in common a certain passion for cyberspace. Unlike the early air shows, these conferences are neither inexpensive to attend nor embraced by the public. Although admission to some well-known conferences such as DEF CON is as little as $150, others require thousands of dollars, and optional training costs even more.[57] Granted, these prices reflect both the type of audience the event wishes to reach and operating costs, but persuading the mainstream public to attend cyberspace-related conferences presents a problem.

Other orchestrated conferences and advances in cyber-related education benefit the domain. The DOD's Cyber Crime Center hosts an annual cyber forensics challenge and convention that provide a wonderful opportunity to network, learn about the latest advances in technology, and sign up for training courses. The forensics challenge is free, but the well-intended and beneficial conference costs $500.[58] The government and DOD must host low-cost conferences akin to air shows where they can display capabilities and allow cyberspace to create its own sense of magic and allure.

With regard to making cyber deterrence more effective, Gen James Cartwright, USMC, retired, former vice-chairman of the Joint Chiefs of Staff, urged open discussion of and training in some cyber offensive capabilities.[59] Cyber conferences would be a perfect venue for members of the DOD to showcase some of the nation's cyber capabilities, attract audiences, and encourage the next generation while deterring adversaries. Moreover, cyber operators could offer these individuals low-cost or possibly free interactive, appealing classes on the fundamentals of cybersecurity and hacking, thus stimulating interest in the domain they will inherit.

Educating young people and stirring their interest in cyber are incredibly important. Although the DOD is deficient in this area, it is taking steps in the right direction in terms of educating and training young officers and enlisted members who have signed up to take part in the cyberspace domain. For example, the Air Force's Undergraduate Cyber Training technical school at Keesler AFB, Mississippi, which opened on 21 June 2010, offers cyber officers a six-month training course that concludes with students earning their cyberspace wings.[60] The schoolhouse fails students who do not pass the blocks of instruction, either retraining them into new Air Force specialty codes or separating them from the service.

The high-quality education offered at Undergraduate Cyber Training reflects the efforts of the faculty, made up of Air Force enlisted and officer personnel who have firsthand experience with and knowledge of

cyberspace operations. These instructors work to inspire and train the next generation of cyberspace officers as they put into practice General Schwartz's belief that a successful career should include a tour of duty as an instructor.[61] Doing so allows the faculty not only to sharpen their skills and academic pursuits but also to network and train with future squadron leaders. This networking creates buy-in from both the instructors and students, contributing to the overall cyber culture. The domain is infused with a sense of passion when instructors relate their experiences and students become excited about creating their own stories. Instructor pilots, war veterans, and participants in various cyber missions can inspire members of the next generation.

The early airpower culture even supported acts of defiance toward superiors and nonflyers to gain their peers' favor and reverence. Army Air Corps members would elevate their status by eliciting trouble and reprimand from Army leaders. They embraced the role of outcasts and found it empowering to create a diverse group and culture associated with flying.[62] Of course, military cyberspace professionals need not take such bold steps or challenge authority. The current military environment favors growth of the cyberspace domain, and, as mentioned previously, we do not need an independent cyber service. Nevertheless, members of the military cyberspace culture can feel very much like outcasts because of the domain's newness and its unexplored, misunderstood capabilities.

We must embrace, not shun, the infant cyber culture. Education and the fostering of a competitive, rewarding instructor-duty option for military members will permit the cyber culture to grow and develop. The best cyberspace operators should compete for duty as instructors and be rewarded with personal and career-enhancing opportunities. This will have the effect of continually updating the educational process and invigorating the cyberspace operators who participate. Consequently, a strong and unique cyber culture will develop, attracting and retaining passionate individuals dedicated to establishing cyber dominance.

Conclusion

The cyberspace domain will forge its own place in history as a domain of warfare. However, similarities with the traditional war-fighting domains, especially the aerial domain, provide many lessons that leaders can use to guide the direction of cyberspace. By understanding these lessons and engaging in open dialogues about the direction of the domain from both a military and civilian perspective, we can apply the proper focus to cyberspace. Specifically, we must encourage actionable intelligence through cyber capabilities, the partnership of civilian and military professionals for national defense, and the cultivation of a cyber culture by means of educating the next generation.

Commanders must know what they can request in terms of support from cyber operators that will directly benefit their missions. Refraining from overclassifying information that pertains to cyber intelligence and cyber capabilities would empower leaders at the tactical, operational, and strategic levels and facilitate the sharing of information with civilian sectors to increase cyber awareness and create meaningful defense strategies. This would bolster national security by allowing civilian leaders to help defend their sectors instead of relying on the DOD and Department of Homeland Security. Lastly, by showcasing cyber capabilities and cyber intelligence at learning events and conferences, we could not only fortify cyber deterrence but inspire members of the next generation to take part in the cyberspace domain. Those individuals must remain the center of our long-term strategy for protecting the domain and establishing cyber dominance.

As General Alexander observed, "If people who seek to harm us in cyberspace learn that doing so is costly and difficult, we believe we will see their patterns of behavior change. The technology is ready."[63] Interested parties throughout the cyberspace domain, including the DOD, civilian sectors, and the next generation, are also ready for the challenges ahead. Cyber power is a powerful political and military tool that we must guide. We must also cement its place in history. The in-

terim years of cyberspace are taking place now, and leaders at all levels must act accordingly to ensure its future success. ✪

Notes

1. William H. Pickering, "The Future of Artificial Flight," *Aeronautics* 6, no. 2 (1908): 17.
2. Alan Axelrod, *Little-Known Wars of Great and Lasting Impact: The Turning Points in Our History We Should Know More About* (Beverly, MA: Fair Winds Press, 2009), 222.
3. David Stevenson, *With Our Backs to the Wall: Victory and Defeat in 1918* (Cambridge, MA: Belknap Press of Harvard University Press, 2011), 186.
4. Andreas Wittmer, Thomas Bieger, and Roland Müller, eds. *Aviation Systems Elektronische Daten: Management of the Integrated Aviation Value Chain* (Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2011), 7.
5. "2nd Lt. Frank Luke Jr.," Official Web Site of the US Air Force, 2 November 2010, http://www.af.mil/news/story.asp?storyID=123006460.
6. Dr. James P. Tate, Lt Col, USAF, Retired, *The Army and Its Air Corps: Army Policy toward Aviation, 1919–1941* (Maxwell AFB, AL: Air University Press, 1998), 33, http://permanent.access.gpo.gov/websites/dodandmilitaryejournals/www.maxwell.af.mil/au/aul/aupress/books/tate/tate.pdf.
7. Capt B. Chance Saltzman and Thomas R. Searle, *Introduction to the United States Air Force* (Maxwell AFB, AL: Airpower Research Institute, College of Aerospace Doctrine, Research and Education, and Air University Press, 2001), 6, http://permanent.access.gpo.gov/websites/dodandmilitaryejournals/www.maxwell.af.mil/au/aul/aupress/books/searle/searle.pdf.
8. Tate, *Army and Its Air Corps*, 62.
9. Pamela Feltus, "Mason Patrick and the Creation of the U.S. Air Corps," US Centennial of Flight Commission, accessed 20 September 2012, http://www.centennialofflight.gov/essay/Air_Power/Patrick/AP15.htm.
10. Tate, *Army and Its Air Corps*, 67.
11. Ibid., 68.
12. Ibid., 190.
13. "Brig. Gen. William 'Billy' Mitchell," National Museum of the US Air Force, 11 February 2010, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=739.
14. Saltzman and Searle, *Introduction*, 12.
15. Col David A. Moore, USAF, *The Art of Aerial Warfare* (Maxwell AFB, AL: Air University Press, 2005), 17, http://dtlweb.au.af.mil///exlibris/dtl/d3_1/apache_media/L2V4bGlcmlzL2R0bC9kM18xL2FwYWNoZV9tZWRpYS81MDUxMg==.pdf.
16. Ibid., 19.
17. Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (1942; new imprint, Washington, DC: Office of Air Force History, 1983), 9.
18. Moore, *Art of Aerial Warfare*, 68.
19. Sir Stanley Baldwin, "A Fear for the Future" (remarks to the House of Commons, London, 10 November 1932). See "The Bomber Will Always Get Through," *Air Force Magazine* 91, no. 7 (July 2008): 72, http://www.airforce-magazine.com/MagazineArchive/Documents/2008/July%202008/0708keeper.pdf.

20. Douhet, *Command of the Air*, 22–23.

21. Moore, *Art of Aerial Warfare*, 33.

22. John Stuart Mill, "The Contest in America," *Dissertations and Discussions*, vol. 1 (Boston: W. V. Spencer, 1868), 26.

23. David R. Mets, *The Air Campaign: John Warden and the Classical Airpower Theorists*, rev. ed. (Maxwell AFB, AL: Air University Press, 1999), 39, http://aupress.au.af.mil/digital/pdf/book/Mets_Air_Campaign.pdf.

24. Benjamin S. Lambeth, "Airpower, Spacepower, and Cyberpower," *Joint Force Quarterly*, issue 60 (1st Quarter 2011): 47, http://www.ndu.edu/press/lib/images/jfq-60/JFQ60_46-53_Lambeth.pdf.

25. Joint Publication (JP) 5-0, *Joint Operation Planning*, 11 August 2011, III-9, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.

26. US Army War College, *Campaign Planning Handbook, AY 08 Final Working Draft* ([Carlisle Barracks, PA]: US Army War College, Department of Military Strategy, Planning, and Operations, 2008), vii, http://www.au.af.mil/au/awc/awcgate/army-usawc/campaign_planning_primer.pdf.

27. JP 5-0, *Joint Operation Planning*, IV-43.

28. Maj Eric D. Trias, PhD, USAF, and Capt Bryan M. Bell, USAF, "Cyber This, Cyber That . . . So What?," *Air and Space Power Journal* 24, no. 1 (Spring 2010): 95, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj10/spr10/aspj_en_2010_1.pdf.

29. JP 5-0, *Joint Operation Planning*, IV-41.

30. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 101.

31. "Cyber Command Achieves Full Operational Capability," news release no. 1012-10, US Department of Defense, 3 November 2010, http://www.defense.gov/releases/release.aspx?releaseid=14030.

32. Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations," *Joint Force Quarterly*, no. 61 (2nd Quarter 2011): 12, http://www.ndu.edu/press/lib/images/jfq-60/jfq-61/JFQ61.pdf.

33. GEN Keith B. Alexander, USA, "Building a New Command in Cyberspace," *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 4, http://www.au.af.mil/au/ssq/2011/summer/alexander.pdf.

34. Nicolas Falliere, Liam O Murchu, and Eric Chien, *W.32 Stuxnet Dossier*, Symantec Security Response, Version 1.4 (Cupertino, CA: Symantec Corporation, February 2011), 1–2, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

35. Ralph Langner, *Stuxnet Deep Dive*, video, 01:03:38, 31 January 2012, http://www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video/.

36. Yaakov Katz, "Stuxnet May Have Destroyed 1,000 Centrifuges at Natanz," *Jerusalem Post*, 24 December 2010, http://www.jpost.com/Defense/Article.aspx?id=200843.

37. Langner, *Stuxnet Deep Dive*.

38. Ellen Messmer, "Stuxnet Could Have Caused 'New Chernobyl,' Russian Ambassador Says," *Network World*, 27 January 2011, http://www.networkworld.com/news/2011/012711-stuxnet-chernobyl.html.

39. Biony Kampmark, "Cyber Warfare between Estonia and Russia," *Contemporary Review* 289, no. 1686 (Autumn 2007): 288–93; and John Markoff, "Before the Gunfire, Cyberattacks,"

New York Times, 12 August 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1.

40. Jason Ryan, "CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor," *ABC News*, 11 February 2011, http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905#.T5M2ABHoK5I.

41. Charlie Rose, "Charlie Rose Talks to General Keith Alexander," *Bloomberg Businessweek*, 21 July 2011, http://www.businessweek.com/magazine/charlie-rose-talks-to-general-keith-alexander-07212011.html.

42. Boldizsár Bencsáth et al., *Duqu: A Stuxnet-Like Malware Found in the Wild*, Technical Report by Laboratory of Cryptography and System Security (Budapest: Budapest University of Technology and Economics, Department of Telecommunications, October 2011), 6–7, http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf.

43. "W32.Duqu: The Precursor to the Next Stuxnet," Symantec, 24 October 2011, http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.

44. "Kaspersky Lab Experts: Duqu and Stuxnet Not the Only Malicious Programs Created by the Responsible Team," Kaspersky Lab, 29 December 2011, http://www.kaspersky.com/about/news/virus/2011/Kaspersky_Lab_Experts_Duqu_and_Stuxnet_Not_the_Only_Malicious_Programs_Created_by_the_Responsible_Team.

45. Rob Waugh, "Lethal Stuxnet Cyber Weapon Is 'Just One of Five' Engineered in Same Lab—and Three Have Not Been Released Yet," *Daily Mail*, 29 December 2011, http://www.dailymail.co.uk/sciencetech/article-2079725/Lethal-Stuxnet-cyber-weapon-just-engineered-lab.html.

46. Greg Masters, "Duqu Variant Uncovered," *SC Magazine*, 23 March 2012, http://www.scmagazine.com/duqu-variant-uncovered/article/233385/.

47. TSgt Richard A. Williams Jr., "CSAF Stresses Importance of Ready Future Force," Official Web Site of the US Air Force, 24 February 2012, http://www.af.mil/news/story.asp?id=123291264.

48. Eloise Lee, "Electronic Warfare Weapons," *Business Insider*, 15 March 2012, http://www.businessinsider.com/electronic-warfare-weapons-2012-3.

49. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012): 29.

50. Thomas Rid and Peter McBurney, "Cyber-Weapons," *RUSI Journal* 157, no.1 (February 2012): 8, http://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354.

51. Kevin Coleman, "Shortage of Adequately Trained Cyber Pros Puts US at Risk," *Defense Systems*, 22 June 2011, http://defensesystems.com/articles/2011/06/08/digital-conflict-cyber-worker-shortage.aspx.

52. Brian Donohue, "Experts Tell Senate: Government Networks Owned, Resistance Is Futile," *Threatpost*, 21 March 2012, http://threatpost.com/en_us/blogs/experts-tell-senate-government-networks-owned-resistance-futile-032112.

53. David H. Onkst, "Explorers, Daredevils, and Record Setters—an Overview," US Centennial of Flight Commission, accessed 20 September 2012, http://www.centennialofflight.gov/essay/Explorers_Record_Setters_and_Daredevils/EX_OV.htm.

54. David H. Onkst, "The First U.S. Airshows—the Air Meets of 1910," US Centennial of Flight Commission, accessed 20 September 2012, http://www.centennialofflight.gov/essay/Explorers_Record_Setters_and_Daredevils/Early_US_shows/EX4.htm.

55. David H. Onkst, "Air Shows—an International Phenomenon," US Centennial of Flight Commission, accessed 20 September 2012, http://www.centennialofflight.gov/essay/Social/airshows/SH20.htm.

56. Tate, *Army and Its Air Corps*, 27.

57. "Official DEF CON FAQ," DEF CON, accessed 20 September 2012, https://www.defcon.org/html/links/dc-faq/dc-faq.html; and "Registration," Hacker Halted, accessed 20 September 2012, http://www.hackerhalted.com/2011/Registration.aspx.

58. "Registration," US Department of Defense, Cyber Crime Conference, 2013, http://www.dodcybercrime.com/12CC/registration.

59. Andrea Shalal-Esa, "Ex-U.S. General Urges Frank Talk on Cyber Weapons," Reuters, 6 November 2011, http://uk.reuters.com/article/2011/11/06/us-cyber-cartwright-idUKTRE7A514C20111106?mid=520.

60. Bruce Rolfsen, "3,000 Officers Switch to Cyberspace Specialty," *Air Force Times*, 17 May 2010, http://www.airforcetimes.com/news/2010/05/airforce_cyber_careers_051710/.

61. Gen Norton A. Schwartz, chief of staff, to all Airmen, memorandum, 8 March 2012.

62. Tate, *Army and Its Air Corps*, 192.

63. Alexander, "Building a New Command," 9.

1st Lt Robert M. Lee, USAF

Lieutenant Lee (USAFA) is a flight commander at an intelligence squadron in Germany, working under the Air Force Intelligence, Surveillance, and Reconnaissance Agency. A graduate of the Air Force's Undergraduate Cyber Training technical school at Keesler AFB, Mississippi, he will receive an MS in cybersecurity / computer forensics from Utica College in the spring of 2013. Building on his passion for education, Lieutenant Lee founded a group that teaches free classes in cybersecurity, forensics, and hacking to on-base personnel in Germany. He has written articles on control-system cybersecurity, cyber warfare, nation-state cyber weapons of the future, and advanced cyber threats for publications such as *Control Global*, *SC Magazine*, *Australia Security Magazine*, and *Hong Kong Security Magazine*. He has also presented cyber-related topics at conferences in Miami, Florida; Seattle, Washington; Washington, DC; Prague, Czech Republic; Ramstein, Germany; Vienna, Austria; and London, England. Routinely consulted for his expertise on such subjects, Lieutenant Lee is an active cyber advocate.

Let us know what you think! Leave a comment!

In Defense of the *Defense*

The Continuing Political Value of "Denial of Enemy Aims"

Dr. Michael Ryan Kraig

> *Our discussion of the limited aim suggests that two kinds of limited war are possible: offensive war with a limited aim, and defensive war.*
>
> *Here lies the origin of the distinction that dominates the whole of war: the difference between attack and defense.*
>
> —Clausewitz, *On War*

Introduction:
Air-Sea Battle in a Contested Geopolitical Environment

This article seeks to answer one very large question: how should the United States prepare to use military power during peacetime deterrence, protracted crises, and even war to resolve conflicting interests with another powerful state, such as China, when both powers also have substantial shared and interconnected interests? The answer to this question could affect future crisis stability in East Asia,

billions of dollars of interconnected interests, and billions in US military spending.

Traditionally, the ideal military goal in airpower theory calls for the United States to use superior or overwhelming firepower in tandem with coordinated mobility, speed, and precision at an operational-tactical level of warfare, or the level of "battle," to produce such decisive effects that the enemy is virtually "disarmed" before he can even mount effective operations.[1] Crucially, we assume that this type of *battle-level military strategy* would then deliver *strategic-level military victory*—often implicitly equated with *total political victory* over a thoroughly defeated, demoralized opponent who, as largely accepted by such military planning, will surrender or capitulate entirely to US demands.[2] This strategy of battle, further described below, has focused in particular on destroying or "interdicting" targets behind the military front lines, often on a preemptive or preventive (i.e., offensive) basis. The presumption of such thinking is that the most effective use of airpower involves strategically and offensively incapacitating the adversary's military machine via the systematic disabling or destruction of high-value targets on his home soil,[3] an approach we dub "strategic offensive interdiction" throughout the rest of the article.

Divorced from contextual political realities, the emphasis on strategic offensive interdiction makes eminent military sense. However, not all political and territorial rivalries lead to wars over completely opposed political stakes. In advising military and political leaders on how to discriminate on the use of force in strategic situations involving peer competitors, military theorist Carl von Clausewitz argued that they must strive to understand the actual political nature of the conflict at hand by answering the question, What war are we fighting? "Generally speaking," wrote Clausewitz, "a military objective that matches the political object in scale will, if the latter is reduced, be reduced in proportion. . . . Thus it follows that . . . *wars can have all degrees of importance and intensity*, ranging from a war of extermination down to simple armed observation" (emphasis added).[4] Indeed, in several pages

of oft-ignored discourse on the differences between Napoleonic-style, revolutionary "total war" versus the average, more bounded, and limited war aims of sovereign leaders both before 1789 and after 1815, Clausewitz implicitly argues that leaders must identify the prevailing policy goals, beliefs, and norms of interaction among major powers in any given era of competition among them and tailor the threat and use of force accordingly.[5] This, in turn, raises the question, What international system are we currently living in?

As this article shows, today's East Asian security environment is much more fluid than the one during the Cold War, in which the global and European theaters were defined by two rigid, largely unchanging ideological blocks of states that refused each other trade, technological sharing, and finance, and which sat poised on the brink of World War III. Nor is it like the constant confrontation with Saddam Hussein from 1990 to 2003, or like that with Slobodan Milošević in the former Yugoslavia from the early 1990s through the 1999 bombing campaign. Instead of the "reinforcing cleavages" seen with these adversaries—in which all economic, political, moral, and military issues became directly counterposed—US conflicts of interest with today's rising China are partial in scope and mediated strongly by dense and complex financial, trade, and diplomatic relations. Conceivably, this more nuanced twenty-first-century geopolitical reality may introduce significant constraints on the ideal airpower goal of full strategic offensives against an opponent's home territory during a crisis or militarized dispute.

To move forward in the debate, the article first describes in greater detail the overall characteristics and thrust of strategic offensive interdiction, followed by a brief examination of today's international system. It then draws upon Clausewitz's often overlooked analysis of the restrained application of force during limited interstate conflicts between great powers. As the article demonstrates, Clausewitz's analysis of variations in both political stakes and levels of warfare goes well beyond his concept of "centers of gravity" that contemporary readers so often cite to justify effects-based weaponry in airpower targeting theories.[6]

That said, one major obstacle to contemporary application of Clausewitz is his back-and-forth style both within and across sections. He disperses myriad points on wars of limited versus "absolute" political stakes alongside an equal dispersion of arguments pitched variously at the grand-strategic policy level, the military-strategic command level, and the lower levels of campaigns, battles, and, ultimately, individual combats and engagements. This constant variance between wars of absolute and limited political stakes, between the offense and the defense, and between different levels of warfare planning and employment, can easily obfuscate Clausewitz's quite clear overall distinction between the strategic offensive and strategic defensive in wars between peer competitors who are not all-out ideological competitors.[7] The article rectifies this problem by systematically bringing together and interweaving his mutually supporting analytic statements on limited great-power wars to arrive at new concepts for military strategy and operational planning for future weapons systems in an evolving Asian geopolitical environment.

The Central Role of Strategic Offensive Interdiction in Traditional Airpower Theory

Airpower advocates have a long history of arguing that offensive, strategically decisive operations are the most efficient and appropriate use of airpower. Despite acknowledgement of its defensive aspects, traditional notions are built on the idea of delivering quick victories at very low cost in US treasure and lives through decisive offensives that virtually disarm the adversary militarily and politically without having to fight his frontline forces indefinitely.[8]

In other words, the presumed, overriding military-strategic goal of customary airpower doctrine entails avoiding the high costs of prolonged, attritional action. In turn, airpower theory traditionally has considered grinding, protracted attrition warfare the logical consequence of using airpower to destroy frontline enemy forces alone,

leaving all of their logistics, population, industrial, energy, food, communications, and political command capabilities intact behind the lines. The latter reality allows the enemy to replenish and replace forces with new troops and supplies at will, backed up by continued intelligence monitoring and command instructions via intact communications facilities.[9]

Consequently, the US Air Force's procurement, employment policies, operational planning, and, ultimately, doctrine have generally focused on hitting or interdicting "strategic" targets behind the front line, in many cases involving complete destruction of infrastructure with heavy civilian as well as military uses. Since the early days of flight, airpower theorists from Giulio Douhet, B. H. Liddell Hart, and Billy Mitchell through Operation Desert Storm's John Warden have envisioned air forces as providing the decisive "knockout blow" that generations of military leaders have sought after studying the classic Napoleonic-era works of Henri Jomini and Clausewitz.[10] For instance, during the American bombing campaigns in Europe and Japan during World War II, "strategic" bombing sought to destroy the enemy's economic infrastructure and even to punish and demoralize his population to the point where either the people would rise up and depose their leaders or simply find themselves completely unable to resist invasion forces on the ground.[11] The more complex of these arguments became known as the "industrial web theory," which held that disrupting, weakening, or destroying the right strands would collapse the entire systemic web needed to support the Nazi war effort.[12] During the Cold War, the apparent war-winning importance of the strategic bombing campaign in World War II transformed into the early organizational and technological rise of Strategic Air Command over Tactical Air Command.[13] In short, putting pressure on the civilian populace and/or the leadership in order to persuade enemy elites in the capital city to submit to maximal US political demands has never been far from airpower theorizing, whether attributed to Douhet at the beginning of the twentieth century or Warden more recently.[14]

Especially in the latest round of airpower theorizing, arguably initiated by Warden, the theory has addressed in one way or another the potentially revolutionary ability of airpower to range across the battlefield and enemy's larger home territory, hitting both tactical and strategic targets simultaneously via "parallel strikes," unblocked by major defensive hurdles.[15] This, in turn, allows airpower (and only airpower) to strike simultaneously key war-supporting nodes or targets in the enemy's "system"—that is, his overall socioeconomic and military organization. The latter includes factories, electric power facilities, industrial production facilities, transport nodes such as bridges, and—most important of all—top leadership centers and/or other intermediate levels of war command that would (in theory) yield far more intense and effective operational effects than dropping those same munitions on frontline forces.[16]

As Clausewitz famously argued, however, it is risky for military planners to decontextualize the notion of effects-based weaponry from the most likely political goals that politicians will seek in the threat and use of force when confronting a peer competitor. Ultimately, everything depends on the level of political stakes or, in Clausewitz's terms, the nature of the "political object."[17] The policy goals of the United States in any given geopolitical dispute, whether it threatens or uses force, will demand certain effects towards certain ends. In other words, what exactly is the strategic political context for military planning and procurements?

The Strategic Operating Environment: Global Integration, Regional Fragmentation

The modus operandi of the future is accommodation between leading powers at certain times and deterrence at others—a flexible combination of the main actors emerging to thwart the excessive ambitions of one of them.

—Dilip Hiro, *After Empire: The Birth of a Multipolar World*

The world is entering a globalized age of "pragmatic multipolarity"—a loose network of interactions based on tactical cooperation among states to bolster their domestic identities and further their shared international interests, rather than a system of competing, well-defined blocs based upon utterly hostile ideological worldviews. At a global level, the reality of unprecedented interstate and transstate socioeconomic networks creating an internationalized form of national wealth makes rising powers in all continents fear the societal costs of upsetting financial and trade flows. Furthermore, the interelite agreement on norms of sovereignty and self-determination of peoples along ethnic, religious, ideological, and linguistic lines now makes the idea of territorial transfer via warfare nearly incomprehensible in any rational economic or cultural sense. The transfer of material resources, manufacturing wealth, and population-based rural productivity via warfare is no longer profitable, as it demonstrably was in European international orders past.[18] If a ruler today tried to act like Napoleon or Frederick the Great by "grabbing territory," he or she almost immediately would face—among members of the nationalistic population who identify culturally, ideologically, and economically with their own society—a highly motivated, hateful, rebellious enemy citizenry or "ready-made insurgency."

In particular, a key part of the US triumph over communism in the Cold War involved the production of a seemingly ingrained, durable, and lasting transnational socioeconomic class with cultural implications. These global elites speak the same professional language of business and high finance, can translate pervasive demands for internal products and resources into a domestically understood local cultural idiom, and can transform local mores and customs regarding money, trade, and information exchange into the globalized, Westernized language of commerce.[19] This general, universal dynamic is already strongly evident—and growing—in Chinese society, in which "new wealth barons" and a rising middle class spur and sustain the continued growth of higher-education systems based on the Western model.[20]

Granted, high levels of general-deterrence stability among major powers exist worldwide. Nevertheless, clashes in strategic perceptions, political ideologies, and territorial claims can still very much matter at the regional level, for several reasons. First, there is a lack of domestic, elite cultural commonality among very disparate sovereign leadership circles within the major or rising powers of the twenty-first century, accompanied by little shared strategic culture on issues of war, peace, interests, attitudes, and perceptions. Brazil, India, China, Russia, South Africa, Turkey, and any other possible rising power do not share the same domestic cultural histories, the same conflict histories at a geopolitical level, or the same experience with domestic politics and the formation of strategic elites over time. This is true because none of them shares completely the same region, with the partial exception of Asian and Eurasian overlaps in contiguity between Russia and China as well as China and India. Second, in ways similar to those of old European international systems, rising powers all harbor some level of nationalist-based territorial claims based on legacy disputes in which the identity of peoples overlaps with swaths of disputed territory.[21] Third, and finally, the latter leads to the paradox that, although the value of territorial conquest in economic terms has become almost nil due to the transnational and international nature of capital, labor, and manufacturing assets, the value of territory in nationalist terms (i.e., domestic identity) has absolutely skyrocketed.[22] The United States therefore faces a subtle geopolitical equation in the Asia-Pacific: a reality wherein both countries are in general strategic accord at the level of the globalized socioeconomic order but where both may have value-based disagreements at the regional level of political stakes.

For instance, in regard to China, one Japanese scholar and policy analyst has argued that in the 1990s, "the government needed nationalism for national integrity, leadership consolidation, and legitimacy, and prevention of what they saw as negative Western influence upon the minds of the people."[23] As a direct result, today "China's rise has imbued the public with self-confidence, which interacts with China's remaining sense of inferiority and is expressed in the form of aggressive

nationalism. . . . The economic rise of China has provided the basis on which a sentiment of love for and pride in the Chinese nation has grown notably since the mid-1990s."[24] Chinese leadership, for example, has

> step[ped] up . . . "patriotic education" in August 1994 [by distributing] . . . the *Guidelines for Implementing Patriotic Education* . . . [to reinforce] the power of national integrity . . . [by] uniting people of all ethnicities. . . . Since the late 1990s[, in short, the domestic political and developmental goal of Chinese leaders] has been "The Great Revival of the Chinese Nation." . . .
>
> . . . [For instance,] Jiang [Zemin] stated that the purpose of such education is to " . . . prevent the rise of the worship of the West."
>
> . . . Methods of patriotic education included designating museums and relics as "patriotic education bases," and making patriotic thoughts the main theme of society by creating a social atmosphere in which "people can be infected and permeated with patriotic thought and spirit any time, any place, in all aspects of daily life." This was to be achieved by utilizing contemporary media, including newspapers, journals, radio, television and films.[25]

Given such nationalist sentiments and accompanying territorial disputes regarding Taiwan and the South China Sea, the United States seeks to deter any strategic expansion of Chinese political interests and military capabilities in ways that could undermine South Korean, Japanese, and Southeast Asian nations' sovereign economic and political security. In this regard, how Beijing treats Taipei, including use of coercive diplomacy backed by military exercises, deployments, and threats, is increasingly becoming an implicit bellwether for how the People's Republic of China (PRC) may treat its other neighbors in the future as it grows financially and technologically. Equally, however, the United States does not want to create in the PRC's mind a threat of radical expansion of Japanese military and political power in the present or future Asian balance since such fears could spark arms races, again undermining the prosperity flowing from a globalized system. Finally, neither the PRC nor the United States (nor Asian friends and

allies) wants Taiwan's leaders to create an unhelpful international precedent of unilateral declarations of political autonomy.[26]

In this environment, the populations of important East Asian powers such as Japan and South Korea are, in essence, "sitting on a fence." Their economies have become so interlinked with China's that one Japanese international relations scholar opined that

> the Japanese economy was lifted by the rapid growth of demand in the Chinese market, and in Japan the economic threat of China is hardly talked about any more. In 2004, China became the largest trading partner of not only Japan, but also South Korea, Taiwan, and Vietnam. In 2004, for the first time in post–World War II history China surpassed the United States as Japan's largest trading partner.[27]

Yet, according to one comprehensive RAND study of Asian elite and popular attitudes, interests, and security perceptions vis-à-vis the United States and China, no country wants to be the party to "buck" the status quo by becoming entangled in disputes between the PRC and its neighbors or the PRC and the United States. Further, no country wishes to jeopardize its prosperity by undertaking a more explicit and expanded East Asian military role. That said, the same RAND analysis showed that the popular viewpoints of foreign policy issues among the populations and leadership circles of both countries could "swing" if tension, pressures, or threats escalate in any one direction—and if the PRC seems to become more bellicose and assertive.[28]

All of this points to a deceptively simple fact: US political and territorial conflicts of interest with China are innately partial or limited in scope, not total. For example, although the United States, China, and Taiwan do not share a single "strategic culture" at the elite or popular level as to norms about the uses of force, none of them is interested in upsetting the complex financial, manufacturing, and trade ties that have evolved among all three sides, and none wants to cause an escalation to all-out warfare. Instead, the threat from China will likely take the form of demands for relatively limited or partial geopolitical gains. As put by the US Air Force's own Center for Strategy and Technology,

"Significant Chinese force projection beyond Southeast Asia will be difficult" even though "China's military will be sufficient to deter and even repel almost any attempt at preemptive action against its mainland or territories or in its immediate vicinity."[29] Instead of true "global reach" as defined by the United States, the service's research team concluded that "China's military capability will be greatest from the mainland out to the 'second island chain'—the region extending south and east from Japan to Guam in the Western Pacific."[30] In terms of actual operational military patterns, it determined that "as a regional air and naval power, China will routinely cruise these waters with its carrier strike groups."[31] The ultimate political strategic goal of the PRC, then, would not be "policing the global commons" but policing the regional commons: "China will seek to assume the role of guarantor of the sea lines of communication in the region, including the strategic Straits [*sic*] of Malacca. They will also be capable of selectively impeding [regional] commerce if they choose."[32]

Given these myriad complexities, it behooves us to ask whether certain aspects of traditional notions of offensive strategic interdiction would serve the United States well in future disputes with this Asian rising power. As Clausewitz pointed out 180 years ago, the political aims of limited war require a different application of force than do wars of unconditional capitulation.

Back to the Future: Clausewitz and Limited War between Major Powers

It follows, too, that war can be a matter of degree.

—Clausewitz, *On War*

One could summarize Clausewitz's most basic theoretical argument in one dictum of particular importance for today's US joint force structure: military leaders should not fight wars with limited political stakes as if they are "absolute" wars over unlimited political goals. Or in his

own words, "Obviously, wars waged by both sides to the full extent of their national strength must be conducted on different principles from wars in which policy was based on the comparative size of the regular armies."[33] In his own day, Clausewitz consistently made the empirical observation that, beyond the continent-spanning, revolutionary, highly ideological, and idealist "absolute wars" of Napoleonic France, most wars were fought between major powers that did *not* necessarily harbor any grand designs against the international system itself:

> Only with the rise of Bonaparte have there been campaigns . . . where superiority has consistently led to the enemy's collapse. Before his time, every campaign had ended with the winning side attempting to reach a state of balance in which it could maintain itself. At that point, the progress of victory stopped. . . . This culminating point in victory is bound to recur in every future war in which the destruction of the enemy cannot be the military aim, and this will presumably be true of most wars [between great powers].
>
> If one were to go beyond this point, it would not merely be a *useless* effort which could not add to [political] success. It would in fact be a *damaging* one, which would lead to a reaction [from the enemy]; and . . . such reactions usually have completely disproportionate effects.[34] (emphases in original).

Thus, in terms of what we now call the tactical and operational levels of war, or what Clausewitz referred to as the "engagement" and "campaign," respectively, he argued that "an attacker can overshoot the point at which, if he stopped and assumed the defensive, there would still be a chance of success—that is, of equilibrium. It is therefore important to calculate this point correctly when planning the campaign. An attacker may otherwise take on more than he can manage and, as it were, get into debt."[35]

But Clausewitz's life's work did not start out with notions of purposefully constrained offensives, a reality that often confuses the debate. In the beginning sections and chapters of *On War*, Clausewitz initially seemed to verify the main threads in Jominian reasoning—that is, the collapsing of the tactical-combat, operational-battle, and military-strate-

gic levels into one grand military-political level of action and deed, thought, and decision making:

> War is an act of force, and there is no logical limit to the application of that force. Each side, therefore, compels its opponent to follow suit; a reciprocal action is started which must lead, in theory, to extremes. . . .
>
> Theory . . . has the duty to give priority to the absolute form of war and to make that form a general point of reference, so that he who wants to learn from theory becomes accustomed to keeping that point in view constantly, to measuring all his hopes and fears by it, and to approximating it *when he can* or *when he must*.[36] (emphases in original)

Ultimately, though, Clausewitz was not content merely to describe this already-popular mode of thought, epitomized by historical colleague Jomini in his claims of having reached an objective theory of war. Instead, Clausewitz felt obliged and compelled to critique it severely, based on his own quite extensive wartime experience in command of Prussian forces in the counteroffensives against Napoleon. Indeed, the main difference between them—and a crucial one for air and sea power debates today—is that Jomini's "theory of war" was, in fact, a detailed discourse on "grand tactics" or what we may today call the "theater-strategic" level of war, which simply assumed the goal of complete military disarming of the enemy at the outset.[37] In marked contrast, Clausewitz, in bringing in the idea of political stakes, truly was writing an overarching theory of war-as-a-whole, at all levels of decision making. In ways that bear on today's airpower debates concerning United States–China competition, Clausewitz launched his own real-time, intellectual counteroffensive against Jominian thinking in two major sections titled "Modifications in Practice" and "War Does Not Consist of a Single Short Blow":

> Would this [total military effort in one giant battle] ever be the case in practice? Yes, it would if: (a) war were a wholly isolated act, occurring suddenly and not produced by previous events in the political world; (b) it consisted of a single decisive act or a set of simultaneous ones; (c) the decision achieved was complete and perfect in itself, uninfluenced by any previous estimate of the political situation it would bring about.[38]

Naturally, Clausewitz here sets up three conditions probably impossible to realize concretely in the political world, but he does so in a way that aptly describes in three short points the basic underlying assumptions of Jominian theorizing.[39] In the end, Clausewitz disagreed with not only the simultaneity of large military battles, single combats, or several concurrent campaigns in a purely technological sense (arguably, something that is now achievable with modern technologies), but also the popular military-planning assumption that political decision makers would be so hasty and war hungry as to sign onto such offensive schemes at all times, in all wars. As Clausewitz cautioned military leaders in his own period,

> The interaction of the two sides [enemies] tends to fall short of maximum effort. Their full resources will therefore not be mobilized immediately. . . .
>
> . . . It is contrary to human nature to make an extreme effort, and the tendency therefore is always to plead that a decision may be possible later on. . . .
>
> Warfare thus eludes the strict theoretical requirement that extremes of force be applied.[40]

In turn, Clausewitz argued that this inevitable feature of most wars was due to the political stakes involved between the two sides, as well as the very diffuse nature of military strength, the latter of which by definition would never become completely mobilized at any given moment, given the rise of modern nationalism: "The resources in question are *the fighting forces proper, the country*, with its physical features and population, and its *allies*. The country—its physical features and population—is more than just the source of all armed forces proper; it is in itself an integral element among the factors at work in war" (emphases in original).[41]

In essence, Clausewitz was clearly wending his way towards a complex theory of warfare that did not allow for one simple, linear, and fixed definition of terms such as *military object*, *victory*, or *objective and decisive points* at the strategic level of military planning. For instance, once having admitted that the population itself was a factor in warfare—as Napoleonic wars and revolutions had amply demonstrated

throughout a highly nationalistic Europe—one had to acknowledge that the question of mobilization would introduce not only "total wars" of absolute offensives but also "limited wars" based on the mood and needs of the populations themselves, as interpreted by central decision makers. Thus, one could not assume that an adversary (or one's self) who possessed a large army and a firm plan for a major offensive thrust in a giant battle would necessarily use all of that force in (1) the war overall or, equally, (2) in one humongous, clash-of-wills battle based on totally destructive combat.[42]

In Clausewitz's view, if grassroots popular will were left to its own devices, the masses of one's population, ruled by "passions," would prefer to fight a Napoleonic battle and a Napoleonic war that knew no political or military boundaries or limits.[43] However, masses and passions do not often directly make high-level strategic policy, a point that Clausewitz attempted to drive home: "Since war is not an act of senseless passion but is controlled by its political object [as seen by political leaders], the value of this object must determine the sacrifices to be made for it in *magnitude* and also in *duration*. Once the expenditure of effort exceeds the value of the political object, the object must be renounced and peace must follow" (emphases in original).[44]

Thus, because political goals are partial in an international system in which major powers held interests not only in dispute but also in common, political leaders (statesmen) would likely want to feel their way forward during a crisis. They would test with one set of combats or engagements to see the opponent's response and then reformulate military intentions and plans along the way, with the "political object" in sight at each tit-for-tat iteration during hostilities. Again, as Clausewitz put it, "If war consisted of one decisive act, or of a set of simultaneous decisions [as Jomini portrays], preparations would tend toward totality, for no omission could ever be rectified. . . . But if the decision in war consists of several successive acts, then each of them, seen in context, will provide a gauge for those that follow."[45]

Political decision makers are so cautious, not because of an irrational or overly sensitive fear of using military force to its full potential but because of the near-chronic uncertainty about adversary goals, intentions, and strength or intensity of political will over any given issue in dispute. An anarchic international system that purposefully and closely guards secrets about such variables virtually guarantees the latter.[46] Again, Clausewitz—long before the advent of political science terminologies about "power balances" and "anarchy"—presciently drew out the existence and implications of this kind of political-level uncertainty:

> If you want to overcome your enemy you must match your effort against his power of resistance, which can be expressed as the product of two inseparable factors, viz. *the total means at his disposal* and *the strength of his will*. . . . But the strength of his will is much less easy to determine [than his available means] and can only be gauged approximately by the strength of the motive animating it. Assuming you arrive in this way at a reasonably accurate estimate of the enemy's power of resistance, you can adjust your efforts accordingly. . . .
>
> One could [for example] . . . conceive of a state of balance in which the side with the positive aim (the side with the stronger grounds for action) was the one that had the weaker forces. The balance would then result from the combined effects of aim and strength.[47] (emphases in original)

The key phrase in this quotation is, "Assuming you arrive in this way at a reasonably accurate estimate of the enemy's power of resistance," the latter of which depends upon, as Clausewitz notes, a complex combination of both the adversary's means and the "strength of his will." Given that a haze almost always surrounds the second factor in this equation, it should come as no surprise to Air Force planners that US politicians often fail to live up to the dictates and expectations of traditional airpower theory. The following point of Clausewitz's bears repeating: "But if the decision in war consists of several successive acts, then each of them, seen in context, will provide a gauge for those that follow." Due to the need to assess the enemy's strength of will, it is exactly this incremental decision-making method that has nearly always defined the political approach to the use of force against peer competitors. Barring the completely certain intelligence of political will or the

wars of ideological genocide carried out by obvious megalomaniacs such as Adolf Hitler, it probably always will.

Here, Clausewitz represents a firm philosophical body of thought separate from the more purist versions of offensive strategic interdiction—specifically, his recognition that, in warfare between major powers, *disarming the enemy* could mean an infinite number of physical realities, depending upon the opponent's strength of will, which in turn would directly relate to the political aims sought:

> We can now see that in war many roads lead to success, and that they do not all involve the opponent's outright defeat. They range from *the destruction of the enemy's forces, the conquest of his territory, to a temporary occupation or invasion, to projects with an immediate political purpose, and finally to passively awaiting the enemy's attacks* [emphasis in original]. *Any one of these may be used to overcome the enemy's will* [emphasis added]: the choice depends on [political] circumstances.[48]

This political definition of war and victory potentially runs contrary not only to early offensive airpower theorists in the 1920s and 1930s (the Air Corps Tactical School) but also to the primary mode of thought of Air Force policy makers since that time. The latter have overwhelmingly emphasized offensive strategic interdiction of key socioeconomic and military-supporting centers of gravity via quick parallel attacks on linked target sets, all towards the purpose of total victory or defeat of the enemy.[49] Specifically, Clausewitz argued that there could never be one schema or conceptual framework for decisive, low-cost, offensive victory in battle that would always equal both military victory and political victory at a strategic level of decision making. In the end, it depended upon the political war being fought, as represented in each side's demands of the opponent after military defeat—with the demands themselves determining what the concept of "defeat" actually would mean in final physical terms:

> When we attack the enemy, it is one thing if we mean our first operation to be followed by others until all resistance has been broken; it is quite another if our aim is only to obtain a single victory, in order to make the enemy insecure, to impress our greater strength upon him, and to give

> him doubts about his future. If that is the extent of our aim, we will employ no more strength than is absolutely necessary.[50]

In Clausewitz's mind, no such typology as "routine" attacks (what some Air Force verbiage tends to disparage as "attrition warfare") versus "special" attacks (what twentieth-century military theorist J. F. C. Fuller dubbed "brain warfare") could exist.[51] Rather, attacks would be less or more useful, depending upon political goals. As Clausewitz argued, in regards to the European continental flurry to adopt the "objective" French way of war,

> the French are always writing about *guerre d'invasion* [italics in original]. What they understand by it is any attack that penetrates deep into enemy territory, and they would like if possible to establish its meaning as the opposite of a routine attack—that is, one that merely nibbles at a frontier. . . . *[But] whether an attack will halt at the frontier or penetrate into the heart of the enemy's territory* [emphasis added], whether its main concern is to seize the enemy's fortresses or to seek out the core of enemy resistance and pursue it relentlessly, is not a matter than depends on form [technologies, doctrine]: it depends on [political] circumstances. Theory, at least, permits no other answer.[52]

So, Clausewitz was already arguing during his lifetime (in direct response to Jomini as well as many practicing military colleagues in Europe) about an idea increasingly lost in both theorizing and concrete military planning in the immediate post-Napoleonic era.[53] This notion held that, although tactical combats and engagements needed to be well planned and decisive in and of themselves, ultimately they were merely ingredients in larger battles. The latter, in turn, could be part of very different macrolevel military strategies in service to the policy goals of war. That is, any given engagement and any given battle could itself be part of larger, more extensive campaigns of strategic offense or strategic defense over protracted periods, spread out over many separate fronts between two adversaries, together adding up to the grand strategic level of the war as a whole (see figure).

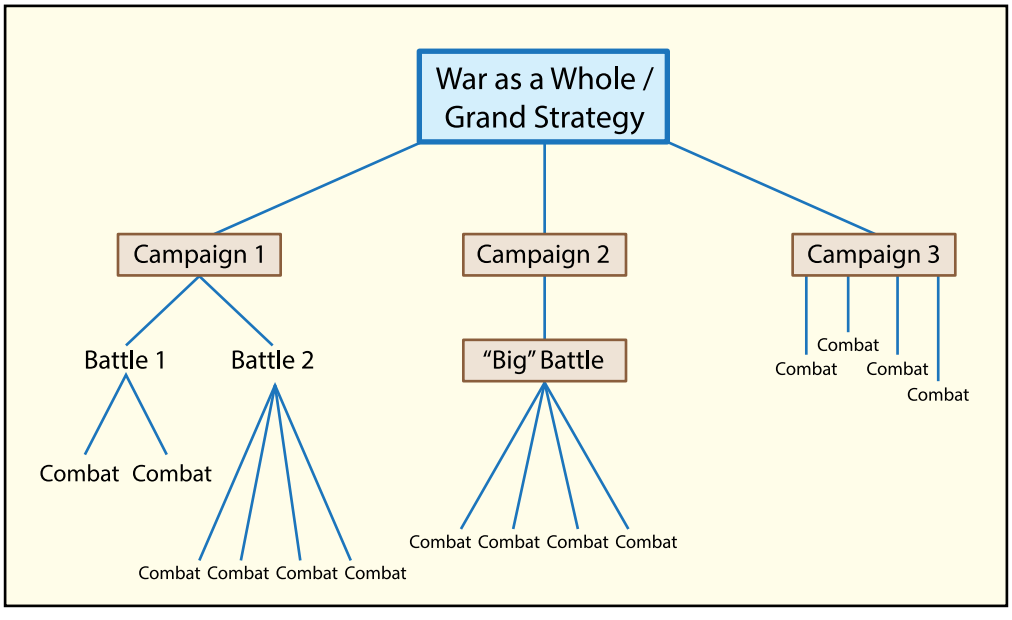


Figure. Mapping Clausewitz's "levels of warfare"

With this in mind, it is hard to refute Clausewitz's characterization of a full-scale war between actual peer competitors at the great-power level:

> If a state with its fighting forces is thought of as a single unit, a war will naturally tend to be seen in terms of a single great engagement [in accordance with the arguments of Jomini]. . . . But our wars today consist of a large number of engagements, great and small, simultaneous or consecutive, and this fragmentation of activity into so many separate actions is the result of the great variety of situations out of which wars can nowadays arise.
>
> Even the ultimate aim of contemporary warfare, the political object, cannot always be seen as a single issue. Even if it were, action is subject to such a multitude of conditions and considerations that the aim can no longer be achieved by a single tremendous act of war. Rather it must be reached by a large number of more or less important actions, all combined into one whole.[54]

Again, it is important to point out *why* Clausewitz argues that war consists of different levels of decision and different types of planning. One might argue that much of this early theorizing is no longer relevant because it was so inextricably based on the reality of "land war" and crude offensive technologies of the time. However, this would be misreading. Clearly, Clausewitz argues that war is nearly always a halting, hesitant, and mixed beast, not because of technology or terrain but because of politics, both domestic and international: "This fragmentation of activity into so many separate actions is the result of the great variety of situations out of which wars can nowadays arise."[55] The word *situations* does not mean simply different technologies or terrain but different political contexts.

Amending Notions of "Victory" in Wars of Limited Aims between Major Powers

Eventually, Clausewitz prescribed a different approach to "victory" in cases of "limited wars" between peer great-power competitors, which he saw as emerging from partial, rather than total, conflicts of interest with the adversary. In interstate disputes based on only partially conflicting values or material goals, the parties could skillfully use individually decisive (tactical) "engagements" or combats towards rather less decisive, less definitive campaigns and the overall war as a whole. By the end of his unfinished tome, Clausewitz had begun to delineate a type of warfare so limited in political goals that military means and military objects would also, in tandem, become directly influenced and indeed severely constrained in their employment against the adversary—at least at an operational or a campaign, if not tactical, level of fighting:

> Suppose one merely wants a small concession from the enemy. One will only fight until some modest *quid pro quo* [italics in original] has been acquired, and a moderate effort should suffice for that.
>
> . . . Neither side makes more than minimal moves, and neither feels itself seriously threatened.

> Once this influence of the political objective on war is admitted, as it must be, there is no stopping it; consequently we must also be willing to wage such minimal wars, which consist in *merely threatening the enemy*, with *negotiations held in reserve*.[56] (emphases in original)

That is, one *could* choose the destruction of the adversary at a strategic political level via disarming his entire military machine alongside, perhaps, pure "punishment" strikes meant to wear down the populace. Both of the latter would argue for decisive, offensive, campaign-level invasions of the adversary's territory and attacks on his strategic "objective points." Alternatively, one could choose to let the opponent strike first and bear those costs via mounting a purely strategic defense, even as one's own combats and battles themselves would have mainly offensive characteristics at a lower level of action and military decision making:

> What do we mean by the defeat of the enemy? Simply the destruction of his forces . . . either completely or enough to make him stop fighting. . . .
>
> Engagements mean fighting. The object of fighting is the destruction or defeat of the enemy. The enemy in the individual engagement is simply the opposing fighting force. . . .
>
> . . . The complete or partial destruction of the enemy must be regarded as the sole object of all engagements. . . .
>
> . . . By direct destruction we mean tactical success. We maintain therefore that only great tactical successes can lead to great strategic ones. . . . Tactical successes are of *paramount importance* in war.[57] (emphasis in original)

As one can see, therefore, Clausewitz's focus on the "strategic defense" in wars of "limited objects" did not derive at all from military passivity at the level of counterposed forces in the battlespace. We must not confuse his argument for strategic defensive wars of limited aims with some claim that all wars should be fought halfheartedly or, perhaps more accurately, that individual combats or "engagements" should be lacking in offensive fervor and results. Clausewitz clearly states, repeatedly across separate chapters, that one core thread binds all military and political planning together—the destruction of an adversary's fighting forces at the lowest tactical or operational level.

> So much then for the ends . . . in war; let us now turn to the means.
>
> There is only one: *combat* [emphasis in original]. However many forms combat takes, however far it may be removed from the brute discharge of hatred and enmity of a physical encounter, however many forces may intrude which themselves are not part of fighting, it is inherent in the very concept of war that everything that occurs *must originally derive from combat* [emphasis in original].
>
> . . . *Whenever armed forces, that is armed individuals* [emphasis in original], are used, the idea of combat must be present. . . .
>
> . . . *The fact that only one means exists constitutes a strand that runs through the entire web of military activity and really holds it together* [emphasis added].[58]

Or in sum, "It would be a fundamental error to imagine that a negative [defensive] aim implies a preference for a bloodless decision over the destruction of the enemy. . . . Everything is governed by a supreme law, the *decision by force of arms*. If the opponent does seek battle, this recourse can never be denied him" (emphasis in original).[59]

The key to understanding Clausewitz on this score, in short, involves separating the tactical from operational (campaign) and strategic (policy) levels of both decision making and actions in war. Much of classic and even contemporary airpower theory concerns the necessity of melding or fusing all such levels together to allow for the revolutionary, victory-delivering effects of parallel and simultaneous strikes against all parts of the adversary's war machine. Clausewitz is saying, however, that in wars of limited policy aims, since one does not seek all-out victory against the adversary, striking behind the front lines may actually cause an escalation one does not even want. That is, if we do not wish to literally occupy an enemy (as in Germany and Japan in 1945, Kosovo in 1999, or Iraq in 2003), why do we want to collapse his entire economic, war-supporting "system" or "organization"? Instead, one might, for political reasons, want to wage brutal combat within a purposefully constrained battlespace along the frontiers of each side's outer perimeters (i.e., the outer limits of each side's spheres of power projection):

> What is the concept of defense? The parrying of a blow. . . . A campaign is defensive if we wait for our theater of operations to be invaded. . . . In other words, our [operational] offensive takes place within our own positions or theater of operations. . . . But if we are really waging war, we must return the enemy's blows. . . . So the defensive form of war is not a simple shield, but a shield made up of well-directed blows.[60]

Putting all of this together, one uses combined offensive-defensive campaigns (operational level of decision making) via offensive combats within well-ordered engagements of enemy forces (tactical level) to serve a larger military and political strategy of denial of enemy aims during a crisis or limited war (strategic level). According to Clausewitz, "The second question is how to influence the enemy's expenditure of effort; in other words, how to make the war more costly to him. The enemy's expenditure of effort consists in the *wastage of his forces*—our *destruction* of them" (emphases in original).[61] He then refers to this defensive form of war (at a level of campaigns) as one with a "negative aim" in which "victory" simply means that the opponent does not himself win: "If a negative aim—that is, the use of every means available for pure resistance—gives an advantage in war, the advantage need only be enough to *balance* any superiority the opponent may possess: in the end his political object will not seem worth the effort it costs" (emphasis in original).[62] Thus, one uses very clear offensive victories at the level of combats and engagements to serve a more defensive campaign and war goal of "balancing" the adversary's fighting power, making his objectives costly or perhaps even impossible to achieve.

When Offensive Strategic Interdiction Is Not an Option

In a US-PRC crisis over any imaginable geopolitical issue, whether Taiwan's status or the South China Sea's mineral, oil, gas, and military navigation issues, US political leaders probably will need offensive force options at a tactical and perhaps even operational (campaign) level of planning. However, we must funnel all such offensive combats towards strategically defensive political goals, in which diplomats will

not want to disarm and defeat China but bargain for new issue settlements that leave the overall Asian balance of power in place for the most part. Therefore, in any future great-power crisis in the Asia-Pacific theater, rather than think in terms of offensive parallel operations involving simultaneous strikes meant to degrade the enemy's ability to communicate with (or command) his forces in the field, US decision makers would likely proceed along the lines of Clausewitz's description of political-military linkages:

> Thus there are many reasons why the purpose of an engagement may not be the destruction of the enemy's forces, the forces immediately confronting us. Destruction may be merely a means to some other end. In such a case, total destruction has ceased to be the point; the engagement is nothing but a *trial of strength*. In itself it is of no value; its significance lies in the outcome of the trial.[63] (emphasis in original)

The simple truth is that in a world of rising powers defined by complex interdependence, neither side will be particularly interested in completely disarming the other. In a limited war, the United States eventually may want to denude Chinese capacities for power projection in its near abroad, but US decision makers almost certainly will not want to treat China as it did Japan during World War II—or Saddam in 2003 or Milošević in 1999 in Kosovo Province—by forcing China to retreat from positions on its own internationally recognized sovereign territory. Instead, politically likely offensive and defensive actions will occur in China's near abroad over issues that do not entail regime change or complete capitulation. Thus, with these partially competitive and partially cooperative aspects of US-China relations well in mind, smart military planners today will indeed focus their efforts on the reality of incremental, halting, and "fragmented" political edicts during the protracted course of a given crisis or conflict in the Asia-Pacific. Ultimately this means planning for campaigns and wars defined as "defense by denial of enemy aims." ✪

Notes

1. Phillip S. Meilinger, *10 Propositions Regarding Air Power* (Maxwell AFB, AL: Air Force History and Museums Program, Air University Press, 1995), 8–48.
2. Scott A. Cooper, "Air Power and the Coercive Use of Force," in *Immaculate Warfare: Participants Reflect on the Air Campaigns over Kosovo, Afghanistan, and Iraq*, ed. Stephen D. Wrage (Westport, CT: Praeger, 2003), 12–13; and Dag Henriksen, *NATO's Gamble: Combining Diplomacy and Airpower in the Kosovo Crisis, 1998–1999* (Annapolis, MD: Naval Institute Press, 2007), 31.
3. Meilinger, *10 Propositions*, 8–19, 28–40.
4. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 81.
5. Ibid., 586–94.
6. See, for instance, Henriksen, *NATO's Gamble*, 40–41.
7. Specifically, see Clausewitz, *On War*, 601–2, 614–15.
8. Meilinger, *10 Propositions*, 8–12, 16–19, 34–40.
9. Beatrice Heuser, *The Evolution of Strategy: Thinking War from Antiquity to the Present* (Cambridge, UK: Cambridge University Press, 2010), 314–45. See also Henriksen, *NATO's Gamble*, 31–62.
10. For the century of inspiration ignited by Napoleon and the immediate post-Napoleonic works of Clausewitz and Jomini, *and* the "cult of the offensive" generally, see Heuser, *Evolution of Strategy*, 137–52.
11. Ibid., 320–21.
12. Henriksen, *NATO's Gamble*, 42–43.
13. Col Mike Worden, *Rise of the Fighter Generals: The Problem of Air Force Leadership, 1945–1982* (Maxwell AFB, AL: Air University Press, 1998), 1–132, http://aupress.au.af.mil/digital/pdf/book/Worden_Rise_of_the_Fighter_Generals.pdf.
14. Heuser, *Evolution of Strategy*, 297–356.
15. Meilinger, *10 Propositions*, 34–40.
16. Henriksen, *NATO's Gamble*, 31–35; and Heuser, *Evolution of Strategy*, 334–36, 342–45.
17. Clausewitz, *On War*, 80–81.
18. Robert Art, "The United States and the Rise of China: Implications for the Long Haul," in *China's Ascent: Power, Security, and the Future of International Politics*, ed. Robert S. Ross and Zhu Feng (Ithaca, NY: Cornell University Press, 2008), 264–65; and Stephen Van Evera, "Primed for Peace: Europe after the Cold War," in *The Cold War and After: Prospects for Peace*, ed. Sean M. Lynn-Jones and Steven E. Miller (Cambridge, MA: MIT Press, 1993), 200–202.
19. Van Evera, "Primed for Peace," 219–36.
20. Col John P. Geis II, PhD, "Harmonious Discordance: China in 2030," in *Discord or "Harmonious Society"? China in 2030*, ed. Col John P. Geis II, PhD, USAF, et al., Occasional Paper no. 68 (Maxwell AFB, AL: Center for Strategy and Technology, Air War College, Air University, February 2011), 94–98, 101–2, http://www.au.af.mil/au/awc/awcgate/cst/csat68.pdf.
21. On "bisecting borders," see Bikash A. Roy, "Bisecting Borders: Neo/Realism, Issues, and War" (presented at the Annual Meeting of the American Political Science Association, Chicago, 1995).

22. For the case of Chinese nationalism specifically, see Andrew Scobell, *China's Use of Military Force: Beyond the Great Wall and the Long March* (Cambridge, UK: Cambridge University Press, 2003), 15–39. For the rise of nationalism as a broad sociopolitical and socioeconomic movement in states all across the globe, see Benedict Anderson, *Imagined Communities: Reflections on the Origins and Spread of Nationalism* (London: Verso Books, 1983), 1–46, 155–85; Hein Goemans, "Bounded Communities: Territoriality, Territorial Attachment, and Conflict," in *Territoriality and Conflict in an Era of Globalization*, ed. Miles Kahler and Barbara F. Walter (Cambridge, UK: Cambridge University Press, 2006), 25–61; and David Newman, "The Resilience of Territorial Conflict in an Era of Globalization," in Kahler and Walter, *Territoriality and Conflict*, 85–110.

23. Akio Takahara, "A Japanese Perspective on China's Rise and the East Asian Order," in Ross and Zhu Feng, *China's Ascent*, 235.

24. Ibid., 219, 230.

25. Ibid., 230–31.

26. Art, "United States and the Rise of China," 260–92.

27. Takahara, "Japanese Perspective on China's Rise," 218.

28. Evan S. Medeiros et al., *Pacific Currents: The Responses of U.S. Allies and Security Partners in East Asia to China's Rise* (Santa Monica, CA: RAND Corporation, 2008), http://www.rand.org/pubs/monographs/2008/RAND_MG736.pdf.

29. Geis, "Harmonious Discordance," 103.

30. Ibid., 104.

31. Ibid.

32. Ibid. For similar points made within the same overall study, see Lt Col Ralph A. Sandfry, "China's Military Modernization," in Geis et al., *Discord or "Harmonious Society"?*, 71–92.

33. Clausewitz, *On War*, 220.

34. Ibid., 570.

35. Ibid., 572.

36. Ibid., 77, 581.

37. Gérard Chaliand, *The Art of War in World History: From Antiquity to the Nuclear Age* (Berkeley: University of California Press, 1994), 724–43.

38. Clausewitz, *On War*, 78.

39. John Shy, "Jomini," in Peter Paret, *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (Princeton, NJ: Princeton University Press, 1986), 148, 154–55, 159, 161, 168–70, 174–75.

40. Clausewitz, *On War*, 79, 80.

41. Ibid., 79.

42. One infers these broad points from his argumentation (ibid., 87–89).

43. Ibid., 89, 591–93.

44. Ibid., 92.

45. Ibid., 79.

46. In broad terms, this is the entire argument of James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (Summer 1995): 379–414. See also Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1984), 82–90.

47. Clausewitz, *On War*, 77, 82.

48. Ibid., 94.

49. See, for instance, the summation of the arguments in Henriksen, *NATO's Gamble*, 30–57.
50. Clausewitz, *On War*, 92.
51. See, for instance, the discussion of Meilinger, *10 Propositions*, 34–40, 51–53.
52. Clausewitz, *On War*, 565.
53. See the summation of the military officer debates of the time in Heuser, *Evolution of Strategy*, 113–14, 137–52.
54. Clausewitz, *On War*, 227.
55. Ibid.
56. Ibid., 604.
57. Ibid., 227, 228.
58. Ibid., 95, 96.
59. Ibid., 98, 99.
60. Ibid., 357.
61. Ibid., 93.
62. Ibid., 94.
63. Ibid., 96.

Dr. Michael Ryan Kraig

Dr. Kraig (BA, Minnesota State University–Moorhead; PhD, University of Buffalo) is an assistant professor of national security studies in the Department of International Security and Warfare Studies, Air Command and Staff College, Maxwell AFB, Alabama. He served in several senior capacities with the Stanley Foundation, a nonprofit, nonpartisan operating foundation in Muscatine, Iowa, devoted to researching and advocating multilateral policy options for solving global security challenges. His work included creation and implementation of broad-based "track-two" dialogues in Washington, DC; Berlin; Dubai; and Muscat among a wide range of national officials and policy analysts from the United States, the Middle East, Europe, and Asia. Dr. Kraig's recent publications include "US Policies toward Tehran: Redefining Counter-proliferation for the Twenty-First Century," in the Air Force journal *Strategic Studies Quarterly* (Winter 2011).

Let us know what you think! Leave a comment!

The Symbiotic Relationship between the Air Force's Active and Reserve Components

Ensuring the Health of the Total Force

Col Bruce K. Johnson, USAF
Lt Col Scott Kniep, USAF
Mr. Sean F. Conroy

Following most major conflicts in our nation's history, the military services downsized, and their active component (AC) and reserve component (RC) faced similar dilemmas. Specifically, they had to maintain personnel readiness, modernize equipment, and retain enough force structure to meet defense strategy on a reduced budget. That situation hasn't changed. The war in Iraq is over, and major combat operations in Afghanistan remain on track to end in 2014. In the wake of these conflicts, the Air Force's AC and RC find them-

selves locked in a zero-sum competition over the future structure of the service.[1] Driven by deep budget cuts, skyrocketing costs for readiness and modernization, and a new defense strategy, the Air Force proposed retaining capability and saving money by cutting force structure, primarily from the RC. Congress and the state governors, however, disagreed and placed the Air Force's plan on hold. They asserted that reserve forces were less expensive and attacked the Air Force's decision to cut the RC rather than the AC. The fact is that both the AC and RC can argue that they are less expensive, given the right set of assumptions and conditions. Such a position oversimplifies the complex interdependencies between the components that one needs to take into account when considering force-structure adjustments. The ongoing debate about cost drains time and energy from headquarters staffs, obscuring the real work necessary to ensure the health of the total force and its ability to meet national defense requirements as we adjust to a postwar drawdown.

This article introduces the concept of a symbiotic relationship between the AC and RC. It provides a means of elevating the component-centric cost debate that is driving the AC and RC apart by enabling a broader system-level dialogue on the health of the total force—a dialogue intended to bring the components back together. The concept of a symbiotic relationship seeks to describe the complex, interdependent nature of the AC and RC from the perspective of personnel investment. Analysis of this concept informs the dialogue by illuminating the effects of policy and resource decisions on the health of the total force.

Consequently, to enable the reader to gain an understanding of this symbiotic relationship, the article first defines the concept, the context in which it arose, external and internal factors that affect the health of the total force, and component perspectives on the Air Force's policy of total force integration (TFI)—a manifestation of the symbiotic relationship.[2] Second, to demonstrate the utility of the concept, it offers a vignette based on the 2011 Rated Summit plan to place inexperienced

AC fighter pilots and maintainers in RC units. Although the vignette is geared toward pilots and maintenance, the symbiotic relationship concept readily applies to other war-fighting communities resident in the AC and RC (e.g., intelligence, surveillance, and reconnaissance; civil engineering; and security forces). Third, the analysis includes a vision for AC and RC officers to follow as they translate this concept into an actionable personnel-management suite of tools that action officers can use to offer credible insights and recommendations to leaders and decision makers.

The Active and Reserve Components: Differing yet Complementary Functions Grounded in Policy and Law

One commonly uses the term *symbiotic relationship*, which denotes mutual benefit and dependence, to explain the association between two entities that need each other to survive and prosper. In other words, it provides a positive sum for those involved, in contrast to a zero-sum competitive relationship. By design, the relationship between the AC and RC is interdependent and symbiotic since both perform differing yet complementary functions that allow each to survive and thrive as part of a larger system. This is the basic premise that enables the AC and RC to transcend the component-centric zero-sum competition and reach a positive-sum view of the total force.

According to former senator John Warner (R-VA), "the Total Force Policy was never intended to make full-time active soldiers and part-time reservists mirror images of each other. Rather, it was a creative response to meeting the nation's post–World War II responsibilities as a global power and the fiscal and demographic realities facing the Department of Defense (DOD) after the Vietnam War."[3] Too often, people think of the RC simply as a smaller version of the AC. Yet, as Senator Warner notes, crafters of the total force policy never meant for this to be the case. A quick review of DOD policy and title 10 of the *United*

States Code highlights the differing yet complementary function of the AC and RC. DOD Directive 5100.01, *Functions of the Department of Defense and Its Major Components*, holds that the military departments are responsible for performing "functions necessary to fulfill the current and future operational requirements of the Combatant Commands, including the recruitment, organization, training, and equipping of interoperable forces."[4] The departments must also "establish and maintain reserves of manpower, equipment, and supplies for the effective prosecution of the range of military operations."[5] According to 10 *United States Code*, section 10102, "The purpose of each reserve component is to provide trained units and qualified persons . . . in time of war or national emergency, and at such other times as the national security may require, to fill the needs of the armed forces whenever more units and persons are needed than are in the regular components."[6] In other words, the AC and RC are not meant to be stand-alone entities. The military departments need both their AC and RC to complement each another as part of a self-reinforcing system. This is especially true from a personnel perspective.

The AC *invests* money and time to recruit, train, and develop experienced Airmen for most of its mission needs. Active duty service-commitment requirements represent the time needed to gain a return on this initial training investment. When they have completed their service obligations, AC personnel can choose to serve in either the participating or nonparticipating RC or separate from the service. Those who transfer to the RC represent a recurring *return* on the original AC *investment* for the taxpayer; thus, the Air Force avoids paying twice for the skilled Airmen it needs.[7] In this sense, AC and RC component functions are not mirror images of one another. Rather, they are different from a component point of view and complementary from the system-level perspective, thereby illustrating the symbiotic relationship.

When accessing a prior-service Airman, the RC gains the value of this individual's experience and skill but avoids the cost of having to

train a non-prior-service Airman. The experience and skill that the RC brings to the total force team are critical to meeting training and operations requirements—now and in the future. As such, views that consider cost alone oversimplify the relationship between the components and artificially place them in competition. From this blinkered point of view, the discussion focuses on gaining scarce resources for the benefit of the individual component rather than on maintaining the health of the Air Force, manifested by its ability to carry out current and future demands for national defense.

Concept: Considering the Symbiotic Relationship a System

The symbiotic relationship concept treats the AC and RC as an open system influenced by external and internal factors within these environments.[8] The system responds to external changes in the strategic, operational, economic, and technological spheres (fig. 1). It also responds to internal law, policy, and resource decisions made by the president, Congress, secretary of defense, and service secretaries and chiefs. To analyze this system, we assume that we can determine such AC and RC personnel matters as annual training costs, demand for training slots, attrition, accession, experience, and demand for experience. By monitoring, measuring, and analyzing these six indicators, we expect to be in a better position to judge the long-term viability and sustainability of the total force (health), determine the ability to meet demand (performance), and gauge the return on taxpayer investment (efficiency).

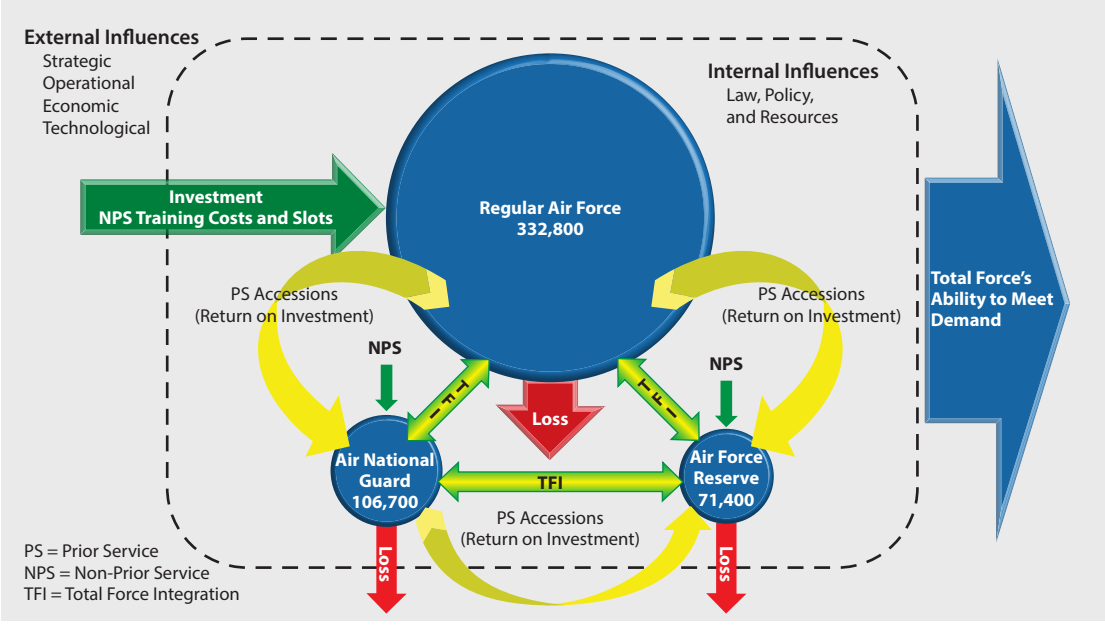


Figure 1. Personnel flow in the symbiotic relationship between the AC and RC

The solid green arrows in figure 1 represent the flow of non-prior-service Airmen, their accompanying training costs, and the demand for training slots among the components. The solid red and yellow arrows indicate Airmen attrition and accessions. The mixed green and yellow arrows represent AC/RC interaction in TFI associate units—interaction that leverages RC experience to help train and develop AC Airmen and executes operational requirements. Finally, the large blue output arrow indicates the combined ability of the components to meet national security demands. Thus, figure 1 helps conceptualize the interdependencies that bring the components together. Understanding these interdependencies will assist in supplying the necessary insight to avoid legal, policy, and resource decisions that adversely affect the three-component Air Force's ability to meet future training and operational demands. It also recasts the cost competition between components as a mutually supporting effort that meets warfighter demands, ensures the long-term health of the total force, and improves the return on taxpayer investment.

Theoretically, this system is at its optimal point in terms of investment / return on investment when the green non-prior-service arrows pointing to the Air National Guard and the Air Force Reserve do not exist. In this condition, the RC would receive all of its personnel as prior-service Airmen—already trained and experienced. In practice this theoretical absolute is neither attainable nor entirely desirable. There is value in accessing non-prior-service Airmen directly into the RC, especially those who enter the force with unique skill sets such as cyber proficiency and specialized medical expertise. That said, the Air Force should make every effort to retain prior-service Airmen when possible, given the enormous amount of time and money it has invested in them.

For example, the Air Force invests as much as $15 million in 10 years to train and develop an AC F-16 pilot, assuming no break in flying assignments. According to the fixed and variable costs contained in Air Force Instruction 65-503, *Cost Factors*, the service invests $5.9 million in the initial two years of training and $9.1 million in eight years of flying experience, including operations and maintenance, military personnel, and munitions expended only during training.[9] When this AC Airman enters the civilian world, eight years of operational experience and a $15 million investment go with him or her. If the Airman joins the RC, every time that individual fills an operational requirement or helps train and develop less experienced Airmen, the American taxpayer receives a recurring return on investment. The Airman maintains currency and readiness for a fraction of the cost of bringing a new person into the service. The same line of thinking holds true for the entire spectrum of Air Force career fields. The Air Force spends less money training and developing the majority of Airmen than it does on aviators; however, considering the large number of Airmen resident in other career fields, the magnitude of the total obligation of time and resources necessary to train and develop maintainers, civil engineers, and security forces may be equally significant. There is an exception to every rule—take, for example, individuals with unique

skill sets, mentioned above. In such cases, either industry or the individual—not the Air Force—bears much of the initial investment.

Context: The Road to Symbiosis

To understand the increasing dependence upon the RC—and the DOD's efforts to enable greater RC participation—we must first examine the history of the total force for proper context. The Air Force's road to symbiosis began with creation of the Air National Guard in 1947 and the Air Force Reserve in 1948. In the early years, the RC was solely a strategic reserve, characterized by its inferior equipment and lower readiness levels, compared to the AC.[10] It sought to mobilize, fight the "big one," and then demobilize. Two major events spurred the DOD to supply the RC with better equipment and integrate it with the AC.

First, the Korean War exposed the weaknesses of US military reserve programs because many of the units mobilized for combat were not ready.[11] Second, President Lyndon Johnson's refusal to activate the RC during the Vietnam War "undercut [its] fundamental purpose and mission."[12] Responding to the president's unwillingness to employ the RC and anticipating the post-Vietnam drawdown, the DOD took steps to ensure that the country would depend upon both the AC and RC to fight its future wars: "The President's Commission on the All-Volunteer Armed Force gave considerable attention to the potential contributions of the Guard and Reserve, which set the stage for what would be known as the Total Force concept."[13] In 1970, Secretary of Defense Melvin Laird first articulated that concept, and in 1973, Secretary James Schlesinger adopted it as formal policy calling for "reduced expenditures . . . in overall strengths and capabilities of active forces and increased reliance on combat and combat support units of the Guard and Reserves."[14]

Since the implementation of this policy, each secretary of defense has steadily increased reliance on the RC, further deepening and strengthening the AC and RC's symbiotic relationship: "In 1982 Secretary of Defense Caspar Weinberger continued to support the Total

Force Policy. Weinberger added the 'First to Fight' principle for resource allocation, according to which 'units that fight first shall be equipped first, regardless of component.' "[15]

Secretary of Defense William Cohen further refined the policy during the Clinton administration: "Cohen's Sept. 4, 1997, seamless Total Force policy memorandum recognized the increased reliance on the nation's Reserve forces since the end of the Cold War. He called on the Department's military and civilian leadership to create an environment that eliminates 'all residual barriers,' both structural and cultural, to effective integration of the Reserve and active forces."[16]

More recently, Secretary of Defense Robert Gates's "Utilization of the Total Force" policy memo defined exactly how the AC and RC would support sustained military operations.[17] This policy recognizes the DOD's full reliance on both the AC and RC to fight our nation's wars. It directs one-year mobilizations at a 1:5 mobilize-to-dwell for the RC and a 1:2 deploy-to-dwell for the AC, additional compensation for personnel who deploy at a greater tempo, review of the hardship waiver program, and elimination of stop loss.[18]

According to the Defense Science Board Task Force, "To cope with the increased demands and reduced resources the services developed new and innovative programs, such as the Air Expeditionary Force developed by the Air Force. The primary objective of these changes was to preserve maximum military capabilities for the nation given a reduction in resources of over $750 billion (actual versus planned spending) in the decade following the fall of the Berlin Wall."[19] The services also implemented policies to further the total force; specifically, the Air Force developed the air and space expeditionary force to leverage capabilities organic to both the AC and RC as a way of meeting operational requirements and establishing a predictable process for rotating forces.[20] Predictability is especially important to obtaining RC participation in the absence of mobilization authority by allowing members of the RC to plan and prepare their families and employers for their

absences. Doing so improves the likelihood of retaining people in the RC and maintaining support for their continued service.

The birth of the air and space expeditionary force marked a significant milestone in the RC's transformation from a strategic reserve to an operational entity. It became a powerful driving force behind the integration of the AC and RC components, one that intensified following the terrorist attacks of 11 September 2001 and that led to the mobilization of tens of thousands of members of the RC to serve in Afghanistan and Iraq.

Pressured by more than 10 years of combat, Congress made significant changes to the law while the DOD and military services enacted policies and made resource decisions that firmly established the RC as an operational force on par with the AC—at significant cost. For example,

> per capita compensation for part-time reservists, who comprise about 91 percent of the reserve force, increased nearly 52 percent, from $14,400 in fiscal year 2001 to $22,000 in fiscal year 2007. Per capita compensation for full-time reservists increased about 13 percent, from $107,000 in fiscal year 2001 to $121,000 in fiscal year 2007. Of the three cost areas that comprise compensation—cash, noncash, and deferred—deferred compensation costs, such as retiree health care and pensions, grew the fastest, increasing by nearly 28 percent.[21]

The trend toward component integration continues. In an effort to increase member participation and generate a better return on the taxpayer's investment, the Office of the Secretary of Defense created the *continuum of service* construct to reduce legal and policy barriers between the components. This construct mandates "a Human Capital strategy allowing military and civilian members to seamlessly transition in and out of active service to meet mission requirements and encouraging a lifetime of service to the nation."[22] Additionally, on 15 October 2010, the secretary of the Air Force initiated the "3-1" Integrated Personnel Life Cycle Project, designed to reduce waste and enhance the continuum of service by combining the three separate regular, Air Force Reserve, and Air National Guard personnel systems into one and

standardizing Air Force instructions among the components where possible. This action should make it easier for Air Force personnel to transition between the AC and RC, thereby improving the return on the taxpayer's investment.

External and Internal Factors Affecting AC-to-RC Transition

Many factors influence the availability and willingness of an AC Airman to transition to the RC—some internal and some beyond the control of the Air Force. External factors such as a high operations tempo, a weak economy, a decreasing force structure, and an increasing demand for airline pilots and maintenance technicians certainly lie beyond the scope of the service. Others, such as resource and policy decisions that affect incentives or the lack thereof for AC members to transition to the RC, do fall within the Air Force's ability to influence, if not control outright.

High operations tempo and the health of the economy work hand-in-hand to influence an Airman's decision to move from the AC to the RC. The latter's operations tempo, though less than that of the AC, may still cause problems for an individual who desires a civilian career.[23] The Military Officers Association of America, representing both Reserve and Guard members, recognizes that "civilian employers are increasingly reluctant to hire reservists who may be subject to repeated, extended absences from the civilian workplace."[24] From an economic perspective, when jobs are plentiful, people have less incentive to join the military, just as those who do join have less incentive to stay.[25] The opposite is true when the economy is weak and jobs are scarce. Under these conditions, AC retention tends to increase, thus reducing the RC's accessions of prior–service Airmen.[26] Currently, both of these factors contribute to the decrease in the number of AC Airmen transitioning to the RC.

A diminishing AC force structure leaves fewer Airmen available to move to the RC. Between 1988 and 2011, AC end strength dropped by 42 percent while the Reserve and Guard reduced by 13 percent and 8

percent, respectively.[27] In the past, managing the total force was not as sensitive to inefficiencies induced by component-centric management because of the larger force structure. Today, our reduced structure has us living on the margins of sustainability.

Forecasts indicate that the airline industry will require a significant number of pilots and maintainers in the near future. According to an industry report by the Boeing Corporation, "To operate and maintain the airplanes that will be added to the fleet over the next 20 years, the world's airlines will need an additional 466,650 trained pilots and 596,500 maintenance personnel."[28] That equates to 97,320 pilots and 137,000 maintainers for North America alone.[29]

Internal factors, such as the lack of incentives specifically designed to capture AC talent and place it in the RC, reduce the appeal of transitioning from the AC to the RC.[30] In 2011 the AC attempted to coordinate with the RC as it cut some 2,000 officers from its rolls, but it did so without any monetary encouragement to attract those people to the RC. The Air Force did give Airmen incentive to leave the service altogether by offering voluntary separation pay calculated at 1.25 times base pay.[31]

These factors combine to pose a challenge to the health of the total force and its ability to remain viable and sustainable as the budget contracts. Although the Air Force cannot influence many of these factors, it does control force-management policies. To the point, component-centric personnel policies and component choices made to address component-perceived needs can lead to negative second- and third-order effects on the total force. These inefficiencies drive higher costs and may ultimately imperil our ability to perform the national defense mission. If we properly address the symbiotic relationship as a system, it can inform personnel-management policies that can help mitigate the need for the RC to continue investing more of its scarce resources to recruit, train, and develop a growing number of non-prior-service Airmen to fill its ranks. Doing so will better leverage the AC's invest-

ment function along with the RC's return on investment function, thus increasing the overall efficiency of the total force.

Perspectives: Total Force Integration, a Necessity with Benefits

Faced with using declining resources to meet requirements, the AC supports the TFI policy and the various associated constructs out of necessity.[32] It recognizes the capability resident in the RC as a pool of highly experienced Airmen capable of fulfilling unmet AC training and operational demands:

> Starting in March of 1968, the [AC] began tapping the Guard and Reserve to perform Military Airlift Command operational missions through the Reserve Associate Program. . . . The integration concept is quite simple. Reserve crews fly operational missions with [AC] aircraft that otherwise would remain inactive between [AC] missions. The initial associate concept increased the operational capacity of the Air Force and helped lay the foundation for further component integration . . . years later.[33]

Initially developed for the air mobility mission, the associate construct now covers all of the Air Force's core functions.

From the RC's point of view, the TFI benefits are numerous. First, TFI demands that the RC remain a category-one (C-1) trained and ready force with access to AC equipment that is interoperable with RC equipment.[34] The combination of C-1 readiness and interoperable equipment ensures that the RC remains relevant in peace and war. In TFI units, the RC—and, to a greater extent, the total force—benefits from its close contact with the AC, a situation that can facilitate future accessions of prior-service Airmen. Furthermore, Airmen who previously served in TFI units are more likely to understand the differences between the AC and RC. They will have an appreciation for the citizen-Airman construct—the RC member's need to balance a part-time military career, a full-time civilian career, and family. They will also have greater appreciation of the transferable civilian skills that an RC member offers to the AC. Airmen with experience in associate units arguably are better prepared to lead those units and deployed wings that

combine AC and RC assets. Moreover, they can assume senior leadership roles on the high-level staffs that create policy and make resource decisions affecting the total force. Ultimately, those with TFI experience find themselves in a better position to maximize the combat capability of associate units and manage an increasingly integrated Air Force.

2011 Rated Summit Plan: Fighter Pilot Absorption Plan versus Reduced Reserve Component Experience

After the 2011 Rated Summit, the Air Force made a series of decisions intended "to ensure the viability and sustainability of the rated force."[35] Addressing AC pilot absorption is necessary to pave the way for the F-35 conversion. Gen Norton Schwartz, former chief of staff of the Air Force, directed the "increase of fighter pilot production to 278 pilots per year" and the establishment of "active associations at each RC fighter base with the goal of providing no less than 171 absorbable pilot billets."[36] The plan's success relies on leveraging greater RC experience to develop the skills of the AC's less experienced Airmen. This also holds true for aircraft maintainers, without whom the pilots could not fly.

Experience levels across the total force are declining, driven by retirements and a large influx of non-prior-service Airmen.[37] This dynamic is most pronounced in the Reserve, which suffered a 10 percent drop in total experience for all Air Force specialty codes from 2007 to 2011, compared to 2.1 percent for the Air National Guard and 4.5 percent for the AC.[38] If we drill down to the logistics career field, which houses aircraft maintenance, we find a 14.5 percent decline in the Reserve compared to 3.3 percent for the Guard and 2.9 percent for the AC.[39] These statistics alone do not tell us if this trend is a potential problem or part of a manageable cycle—we need more analysis if we wish to fully understand the impact of experience levels on the health of the total force. However, this dynamic should raise a red flag, given

the fact that the RC must train and develop the AC's Airmen even though its own force's experience is declining.

During the past decade, the global war on terrorism and overseas contingency funds enabled the operational Reserve to fulfill combatant commanders' requirements. They also helped the RC gain needed experience and hone the skills of its non-prior-service Airmen during multiple wartime deployments. Going forward, the Air Force will not have this additional money to develop a significant portion of its force, thereby requiring the Reserve and Guard to dedicate a significant amount of their own money to do so.[40] From 2006 to 2011, the Guard's yearly outlay for training non-prior-service Airmen more than doubled, from $52.4 million to $113.9 million.[41] On top of that, the Guard needs an additional $63.4 million for its seasoning program, which allows non-prior-service Airmen to become proficient at their jobs upon completion of initial technical training.[42] In 2011 the Reserve spent nearly $400 million on recruiting, training, and seasoning non-prior-service Airmen, including more than $300 million on enlisted personnel. The Reserve accounts for its non-prior-service costs somewhat differently than the Guard, preventing a clear "apples-to-apples" comparison. Nevertheless, the magnitude of expenditures in both components is significant and invites close attention.

Over time, concurrent AC and RC demands for training time and dollars may cause an unsustainable condition to arise in the active associate fighter units if RC experience levels drop below 70–75 percent.[43] More important than these percentages is that the components work together to establish these experience thresholds and tipping points to draw a line beyond which the health of the total force finds itself at risk. Maintaining higher RC experience levels is integral to getting the most out of the associate unit construct in terms of combat power and the development of less-skilled personnel. This means that decision makers must put into place policies and resources that will arrest the decline in RC experience levels. These decisions should concentrate on increasing prior-service accessions from the AC and other

services. Doing so will also save money and preserve combat capability in the long run.

Vision of the Symbiotic Relationship

As a means of realizing the symbiotic relationship's vision, members of the AC and RC are working together to leverage this concept to gain specific insights that will support law, policy, and decision making. This involves finding ways to monitor, measure, and analyze that relationship. Figure 2 details a systems dynamics approach which approximates AC and RC interdependencies, illustrating important metrics for system performance and health. Finally, it envisions linking these metrics to the chairman of the Joint Chiefs of Staff's risk matrix for force management and operational risk.[44]

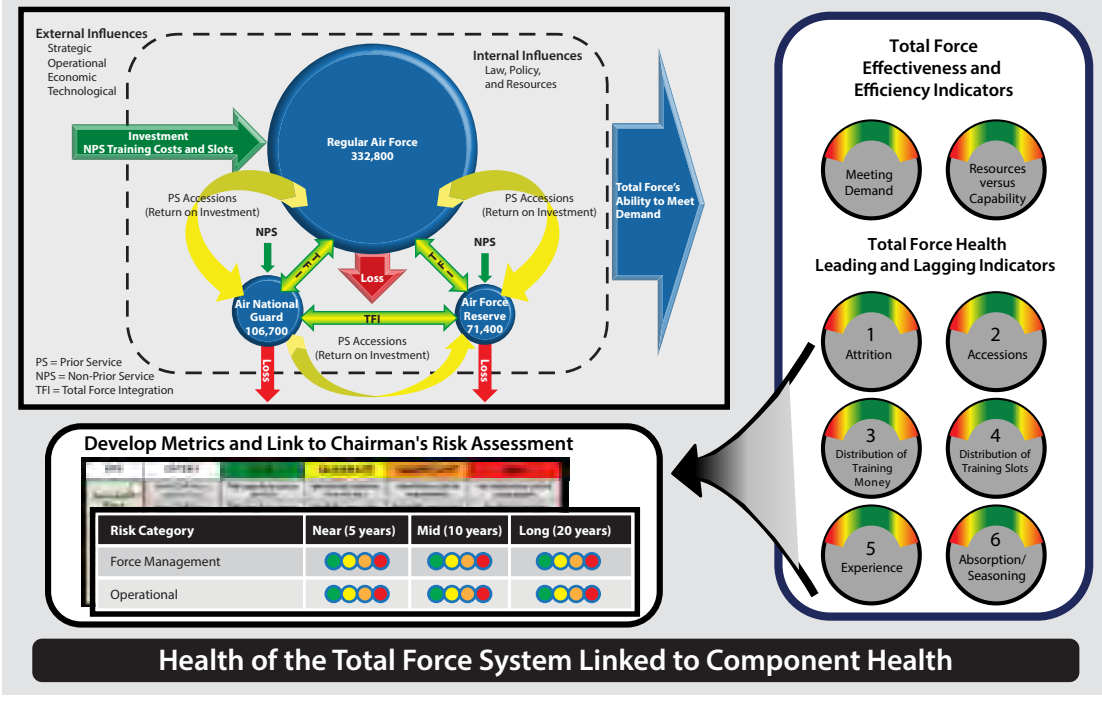


Figure 2. Vision of the AC/RC symbiotic relationship

Linking the analysis to the matrix delivers comparable information on many different issues vital to support sound decision making. It not only provides a scalable, standardized, and analytically rigorous framework for Headquarters Air Force and the Joint Staff to discuss risk but also measures key resource, schedule, and other performance goals.[45] Moreover, the matrix incorporates qualitative factors such as leadership, total force education, the triad (Air Force career, family, and civilian career), community connections, and civilian skills—all of which play a critical role in determining long-term sustainability of the total force.[46] Creating risk metrics based upon the indicators of sustainability and linking them to the chairman's risk-management matrix on force management and operations (figs. 2 and 3) give leaders a way to monitor, measure, analyze, and communicate the system health of the Air Force to the chairman. This, in turn, offers civilian and military decision makers a solid foundation for gauging future effects of law, policy, and resources on various force-management courses of action. Linking the indicators to the chairman's risk assessment helps identify information that leadership needs to know (well-defined and defensible assessment). It also provides civilian and military leaders with success and failure points based on defined thresholds that produce concise, consistent interpretation of results. Furthermore, metric end points and assessments developed via data analysis and evaluations of subject-matter experts will enable senior leaders to defend the decisions they make with the assistance of this process.[47]

Risk Category	Near (5 years)	Mid (10 years)	Long (20 years)
Force Management			
Operational			

Figure 3. Chairman of the Joint Chiefs of Staff's risk matrix

To put the symbiotic relationship into action, we are analyzing interdependencies between the AC and RC by using a systems dynamics approach. This entails gathering information from all three components, including accession and attrition data, funds spent on training, demand for training slots, and experience levels. Lastly, we are creating metrics consistent with and linked to the chairman's risk-assessment process, an activity that requires developing a dashboard to display trends from the six key sustainability indicators and associated (short-term, midterm, and long-term) risk.

Conclusion

This effort seeks to equip Air Force senior leaders with a means to elevate the component-cost debate to a dialogue on system health, which will allow efficient and effective management of the total force, now that military personnel have withdrawn from Iraq and during the drawdown from Afghanistan. It enables them to consider current and proposed law, policy, and resource choices affecting personnel from a holistic approach—one that maximizes the service's combat effectiveness and ensures maximum return on the taxpayer's investment. The symbiotic relationship concept offers a process for increasing transparency and inclusiveness between the AC and RC—a concept that will address complaints directed against the Air Force during deliberations over the president's budget in fiscal year 2013 (FY 13).[48] Members of all three components originated the concept and presented it at the highest levels of Air Force leadership. The chief of staff of the Air Force, chief of the Air Force Reserve, and director of the Air National Guard all received personal briefings. Additionally, senior Air Force leaders articulated the value of the symbiotic relationship with regard to the secretary of the Air Force's 3-1 effort to improve the continuum of service; total force management; rated management; hollow force initiative; plans, programs, and budgeting process; total force enterprise; and identification of roles and missions between the AC and RC. Currently, all three components are working in an open, transparent man-

ner to translate the concept, using a systems dynamics approach with the intent to better understand the interdependent relationship between the AC and RC. The basic analysis of these interdependencies is complete, and an effort to produce a more sophisticated look is ongoing. The goal involves having actionable insights ready in time to inform and defend the FY 15 budget along with the array of law and policy decisions needed to ensure the health of the US Air Force and its ability to meet the demands placed upon it to defend the nation. ✪

Notes

1. According to *United States Code*, title 10, the Air Force consists of the regular Air Force, Air National Guard, and the Air Force Reserve. This article refers to the regular Air Force as the AC and to the Guard and Reserve collectively as the RC.

2. Air Force Policy Directive 90-10, *Total Force Integration Policy*, 16 June 2006, http://www.af.mil/shared/media/epubs/AFPD90-10.pdf.

3. Department of Defense, *Total Force Policy: Interim Report to the Congress*, AD-A235 382 (Washington, DC: Department of Defense, September 1990), 3–4, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA235382.

4. Department of Defense Directive 5100.01, *Functions of the Department of Defense and Its Major Components*, 21 December 2010, 26, http://www.dtic.mil/whs/directives/corres/pdf/510001p.pdf.

5. Ibid.

6. *United States Code*, title 10, subtitle E, pt. 1, chap. 1003, sec. 10102, accessed 7 November 2012, http://www.law.cornell.edu/uscode/text/10/10102.

7. The Air Force pays once to recruit, train, and develop an AC Airman. It pays a second time for the RC to recruit, train, and develop a non-prior-service Airman to fill a position that could have been filled by a transitioning prior-service AC Airman.

8. "Open System," Principia Cybernetica Web, accessed 17 March 2012, http://pespmc1.vub.ac.be/Asc/OPEN_SYSTE.html.

9. Air Force Instruction (AFI) 65-503, *Cost Factors*, 22 March 2012, tables A34-1, A34-2, https://www.my.af.mil/gcss-af/USAF/ep/browse.do?categoryId=p6925EC163B560FB5E044080020E329A9&channelPageId=s6925EC1350500FB5E044080020E329A9.

10. Charles J. Gross, *Prelude to the Total Force: The Air National Guard, 1943–1969* (Washington, DC: Office of Air Force History, 1985), 54.

11. "ANG Heritage: Missions, Wars and Operations," Air National Guard, accessed 22 January 2012, http://www.ang.af.mil/history/heritage.asp.

12. John T. Correll, "Origins of the Total Force," *Air Force Magazine* 94, no. 2 (February 2011): 94, http://www.airforce-magazine.com/MagazineArchive/Documents/2011/February%202011/0211force.pdf.

13. Ibid., 96.
14. Ibid., 96–97.
15. Alice R. Buchalter and Seth Elan, *Historical Attempts to Reorganize the Reserve Components* (Washington, DC: Library of Congress, Federal Research Division, October 2007), 15–16, http://www.loc.gov/rr/frd/pdf-files/CNGR_Reorganization-Reserve-Components.pdf.
16. US Department of Defense, Office of the Assistant Secretary of Defense (Public Affairs), "Hamre Assesses 'Seamless Total Force' on First Anniversary," news release, 4 September 1998, http://www.defense.gov/releases/release.aspx?releaseid=1825.
17. Secretary of Defense Robert Gates, memorandum, subject: Utilization of the Total Force, 19 January 2007.
18. Ibid.
19. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Defense Science Board Task Force on Deployment of Members of the National Guard and Reserve in the Global War on Terrorism* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, September 2007), 2, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA474519.
20. Bruce K. Johnson, "Rebalancing the Air Force: A Comprehensive Solution" (master's thesis, Air War College, 16 February 2011), 8.
21. Government Accountability Office, *Military Personnel: Reserve Compensation Has Increased Significantly and Is Likely to Rise Further as DOD and VA Prepare for the Implementation of Enhanced Educational Benefits* (Washington, DC: Government Accountability Office, 6 July 2009), 3, http://www.gao.gov/assets/100/96269.pdf.
22. Department of Defense Human Resources Management, "Human Resources Management (HRM) Community of Interest (COI) Meeting Session: 08-04" (Washington, DC: Department of Defense, 22 July 2008), slide 10, https://www.mpm.osd.mil/documents/072208_HRMCOI_Briefing.pdf.
23. Rick Maze, "Hiring Bias Linked to Veterans' Joblessness," *ArmyTimes*, 14 September 2011, http://www.armytimes.com/news/2011/09/military-unemployment-reservists-hiring-bias-091411w/.
24. "National Guard and Reserve Benefits," Military Officers Association of America, 2012, http://www.moaa.org/MAIN_MENU/TAKE_ACTION/TOP_Issues/Serving_in_Uniform/National_Guard_and_Reserve_Benefits.html.
25. Beth Asch et al., *Military Recruiting and Retention after the Fiscal Year 2000 Military Pay Legislation* (Santa Monica, CA: RAND, 2002), 67, http://www.rand.org/pubs/monograph_reports/2005/MR1532.pdf.
26. AF/A9RP analysis of data from 1997 to 2011 shows a strong inverse relationship between employment and AC retention.
27. Air Force end-strength data, 1988–2011. See *US Air Force Statistical Digest*, SAF/FMC, multiple years; and Automated Budget Interactive Data Environment System (ABIDES), 2010–11. Analysis provided by Headquarters US Air Force/A9RI, 25 September 2012.
28. Boeing, *Current Market Outlook, 2010–2029* (Seattle, WA: Boeing Commercial Airplanes, Market Analysis, 2010), 12, http://www.boeing.com/commercial/cmo/pdf/Boeing_Current_Market_Outlook_2010_to_2029.pdf.
29. Ibid.
30. In some cases, the opposite is true—specifically, a monetary incentive to leave the AC which members must pay back if they join the RC.

31. Michelle Tan, "AF Details Plan to Cut up to 2,000 Officers," *AirForceTimes*, 21 February 2012, http://www.airforcetimes.com/news/2011/02/air-force-details-plan-to-cut-officers-022111w/.

32. Three types of associate units exist: classic, active, and Air Reserve Component. In classic associate units, the AC owns the hardware, and the RC provides some combination of embedded and additional manpower. Regarding active units, the RC owns the hardware and the AC supplies some manpower, whereas in Air Reserve Component units, either the Air National Guard or Air Force Reserve owns the hardware, and the other provides the manpower. For some weapon systems, active associations give the AC more access to RC aircraft and equipment that it needs to fulfill its operational taskings and develop inexperienced Airmen.

33. Johnson, "Rebalancing the Air Force," 9.

34. Category or "C" levels "reflect the degree to which unit resources meet prescribed levels of personnel, equipment, and training. . . . [C-1 indicates that] the unit possesses the required resources and is trained to undertake the *full wartime mission(s)* for which it is organized or designed" (emphasis in original). AFI 10-201, *Status of Resources and Training System*, 13 April 2006, 16, pars. 1.10, 1.10.1, http://www.e-publishing.af.mil/shared/media/epubs/afi10-201.pdf.

35. Gen Norton A. Schwartz, memorandum, subject: 2011 Rated Summit Decisions, 2 November 2011.

36. Ibid.

37. "Advancing the AC/RC Symbiotic Relationship (SymRel)," version 16, draft, Headquarters US Air Force/A9R, September 2012, slide 6.

38. Ibid.

39. Ibid., slide 16.

40. Mr. Dirk Palmer, AFRC/RS, indicated that Air Force Reserve Command's non-prior-service Airmen should stabilize at approximately 5,000 annually (about 50 percent of all accessions), based on a smaller steady-state AC and slightly larger steady-state RC end strengths. Conversation with the authors, 7 March 2012.

41. Lt Col David Lowery, "Air National Guard Formal School Program," NGB/A1DU, 24 August 2012, slide 3.

42. Ibid.

43. The experience threshold of 70–75 percent comes from discussions with senior RAND analysts who specialize in pilot absorption. Exchange between RAND and AF/A9, RAND office, Washington, DC, 18 September 2012.

44. The matrix defines four levels of risk: low (green), moderate (yellow), significant (orange), and high (red). Low risk considers attainment of a goal or activity highly likely, holding that all expenditures of vital resources and schedules will execute at or near planned levels or time frames. Moderate risk considers realization of a goal or activity likely, maintaining that some resource expenditures or schedules may deviate moderately from planned levels or time frames. Significant risk considers reaching a goal or activity questionable, holding that some resource expenditures or schedules may deviate significantly from planned levels or time frames. High risk considers achievement of a goal or activity highly unlikely, maintaining that at least one vital resource expenditure or schedule is nearing failure and that little margin remains for error in planning or execution.

45. "USAF Risk Assessment Framework: Instructional Brief," US Air Force Analysis and Lessons Learned Directorate (AF/A9A), 20 December 2011, 2.

46. Johnson, "Rebalancing the Air Force," 23.
47. "USAF Risk Assessment Framework," 4, 6.
48. "Confirmation Hearing Set for AF Chief Nominee," *AirForceTimes*, 12 July 2012, http://www.airforcetimes.com/news/2012/07/air-force-mark-welsh-confirmation-hearing-chief-of-staff-nominee-071212/.

Col Bruce K. Johnson, USAF

Colonel Johnson (BSME, University of Wisconsin–Milwaukee; MS, Troy University; MSS, Air University) is deputy director of resource analyses, studies and analyses, assessments, and lessons learned, Pentagon, Washington, DC. Previous staff assignments include Headquarters US Air Force / A9 deputy director of analyses foundations and integration; Air Force Reserve chief of strategic communication plans; Air Force Reserve chief of assessment and future concepts; and Air Force Reserve chief of combat forces, Pentagon, Washington, DC. Colonel Johnson is a master navigator with more than 3,000 hours in both the F-111F and C-130H aircraft. He served in a variety of operational capacities as radar strike officer, weapons and tactics officer, operational planner, information warfare / tactical deception officer, current operations officer, chief navigator, assistant operations officer, senior offensive duty officer at a combined air operations center, and deployed mission commander. While serving in these capacities, Colonel Johnson took part in a wide range of global operations, including Desert Shield, Desert Storm, Coronet Oak, Nomad Vigil, Shining Hope, and Iraqi Freedom.

Lt Col Scott Kniep, USAF

Lieutenant Colonel Kniep (MBA, Touro University; Master of Counseling and Leadership, University of Colorado–Colorado Springs) is chief of the Force Balance Assessment Division, Resource Analysis Directorate, Studies and Analyses, Assessments and Lessons Learned, Headquarters US Air Force. He is an A-10 pilot with operational assignments in Germany, South Korea, and North Carolina; he also served as an Air Force Weapons School instructor at Nellis AFB, Nevada. He deployed in support of Operations Deny Flight, Joint Endeavor, Southern Watch, Northern Watch, Iraqi Freedom, and Enduring Freedom. Lieutenant Colonel Kniep is a graduate of the Air Force Weapons School.

Mr. Sean F. Conroy

Mr. Conroy (BA, University of Maine; JD, St. John's University; MA, Stony Brook University; MA, University of New Orleans; MMS, Marine Corps University; MAAS, Air University) is chief of analysis in the National Guard Bureau's Air Plans and Programs Directorate, responsible for developing studies and analyses on issues affecting the Air National Guard and its place within the total force. He is also a drill-status national guardsman serving as commander of the 159th Security Forces Squadron (Louisiana Air National Guard). Mr. Conroy deployed numerous times following the terrorist attacks of 11 September 2001 to the First Air Force, Third Air Force, and CENTAF combined air operations centers. He led troops in preparation for and response to Hurricanes Katrina and Isaac. Following Hurricane Isaac's landfall, he served as the commander responsible for commodities distribution in St. Bernard and Plaquemines Parishes, Louisiana. Mr. Conroy is a graduate of Squadron Officer School, Marine Corps Command and Staff College, and the Air Force School of Advanced Air and Space Studies.

Let us know what you think! Leave a comment!

A Case for a Cyberspace Combatant Command

Blending Service and Combatant Command Responsibilities and Authorities

Lt Col Shawn M. Dawley, ANG

The next draft of the *Unified Command Plan* should redesignate US Cyber Command as a functional combatant command (COCOM). In much the way that significant contingents of leadership in the US Army wished to relegate the Army Air Corps to a mere supporter of land warfare operations, today's military routinely exercises cyberspace capabilities in supporting roles that enable operations in other domains. Placing US Cyber Command (USCYBERCOM) on the same level as other geographic and functional COCOMs and granting it authority to organize, train, and equip its subordinate forces will allow it to more readily build, harness, and exploit capabilities within this newest field of warfare.

Although man-made, cyberspace remains a domain in which participants can act and react, thus resembling the air, space, maritime, and land domains. As in preceding conflicts, back to antiquity, any tribe, criminal element, or nation-state that fails adequately to weaponize its abilities in the available war-fighting domains may find itself unable to wage combat successfully across the spectrum of warfare. Because of the principally nonkinetic nature of cyberspace, institutional and doctrinal battles over the organization and employment of US cyber's capabilities have tended to focus on its enabling characteristics rather than its offensive capacity. The Department of Defense's (DOD) organizational, procurement, and deployment policies place airpower in the air domain, sea power in the maritime domain, and land power in the land domain. As articulated by Gen Peter Pace, USMC, retired,

former chairman of the Joint Chiefs of Staff, "the integration of offensive and defensive cyberspace operations, coupled with the skill and knowledge of our people, is fundamental" to ensuring strategic superiority in the cyber domain.[1]

Whereas the other war-fighting domains existed long before people's ability to operate within them, an inexorable link exists between the cyber domain and the capabilities within it—just as the tools and doctrine evolve, so does the medium. This evolutionary component likely will cause cyber to become the most unpredictable area within the full spectrum of conflict. Embracing this reality possibly requires an approach and organizational structure that not only accepts but also encourages nonconformity and less-than-conventional warriors.

Large-scale kinetic warfare typically rewards forces that are steadfastly disciplined and grounded in sound doctrine (given the number of combatants involved and the close coordination necessary for execution). A much smaller force, however, can prosecute cyber warfare, rewarding speed and agility in the cyber domain on a magnitude greater than in traditional battlespaces. Thus, if these assumptions are valid, a cyber enterprise may call for operators less inclined to stand firm in established doctrine *and* for an entity to organize and employ them unlike traditional service or COCOM constructs. The current organizational model within the *Unified Command Plan* places the newly formed joint USCYBERCOM as a subunified command under US Strategic Command. The military needs a construct that blends service and war-fighting authorities into a single body *and* elevates that organization to a level where it can fully exploit cyberspace. Toward that end, it should make USCYBERCOM a full, functional COCOM *and* grant the command budgetary authorities under title 10, *United States Code*, to organize, train, and equip its unique contingent of warriors.

Strategy and Execution

Although long-standing customs, international norms, and armed conflicts have established nearly universal recognition of physical sovereignty, the nation-state notion of physical dominion is less exacting in discussions of the cyber domain. Since the Peace of Westphalia in the mid-seventeenth century, sovereignty has been viewed as a legitimate authority over territorial possessions.[2] Thus, for over 300 years, governments, whether monarchies or republics, could physically delineate encroachments on their territories by land, sea, and—eventually—air forces. Further, physical destruction of a fortress or financial institution inarguably constituted an act of war. In the cyber domain, nonkinetic actions produce the same effects, leaving the aggrieved without the same sense of hostile activity. But a computer network attack rendering a fire-brigade command post unable to fix targets or a virus "zeroing out" a banking system's accounts is not *completely* unlike munitions leveling either one. The principal distinction is that a kinetic attack provides for a tangible "CNN effect" while one that simply uses binary code lacks the appeal to passion so critical to calls for retaliation.

Because attacks or probes can (and do) happen within the cyber domain—but not in the same way they occur in the other domains—nation-states must update the doctrinal tradition of just war theory. Particularly as it relates to *jus ad bellum*, "which concerns the justice of resorting to war in the first place," many international affairs scholars hold that only in the aftermath of a threat, existential or otherwise, should a nation-state resort to conflict.[3] To date, such threats have typically been directed against physical possessions. The presence of every computer, cellular telephone tower, and communications grid on the front line in any cyber war prevents defense in depth.[4] Principally, since cyber's vulnerabilities include its reliance on nonproprietary, civilian-operated, and interconnected network systems, "we have no early warning radar system or Coast Guard to patrol the borders in cyberspace."[5] Therefore, consistent with the Bush doctrine, which sees preemptive warfare as the necessary counter to asymmetric threats

posed by hostile actors leveraging weapons of mass destruction, a successful approach to cyber melds defensive posturing with offensive, preemptive capabilities.

Cyber Operations and Strategic Guidance

Most of the attention given to cyber and cyber warfare in strategic planning guidance addresses threats posed to the United States and its allies rather than the necessity of weaponizing friendly cyber capacity. In the most recent *National Security Strategy*, *National Defense Strategy*, and *National Military Strategy of the United States of America*, senior government and military leaders strongly emphasize the dangers posed by state and nonstate actors capable of conducting cyber attacks against the United States and its allies. They pay less attention to developing a robust "strike" capability. Naturally, since these publications are available to both a domestic and international audience, one would not expect them to contain any specifics regarding offensive capabilities. At the same time, the degree to which these documents explore our nation's vulnerabilities in the cyber domain far exceeds the attention paid to generating combat power.

In the *National Security Strategy* (2010), President Barack Obama acknowledges the importance of cybersecurity, listing it as one of just six strategic imperatives for safeguarding US national interests: "In addition to facing enemies on traditional battlefields, the United States must now be prepared for asymmetric threats, such as those that target our reliance on space and cyberspace."[6] This and other excerpts prepared by his national security staff and presented in that document deal for the most part with US vulnerabilities. The strategy accurately captures and portrays the nature of future cyber threats as existing across the continuum of potential adversaries. However, it presents the facilitating role of cyber exclusive of its offensive ability: "The threats we face range from individual criminal hackers to . . . terrorist networks to advanced nation states. . . . Our digital infrastructure, therefore, is a strategic national asset. . . . We will deter,

prevent, detect, defend against, and quickly recover from cyber intrusions and attacks."[7]

Like the *National Security Strategy*, the *National Defense Strategy* (2008) acknowledges that the susceptibility of cyberspace to malicious operations is a strategic vulnerability. Further, it also lacks strong and significant guidance in the way of furthering offensive engineering of cyber capabilities: "The United States . . . and our partners face a spectrum of *challenges*, including . . . emerging space and cyber threats" (emphasis added).[8] Cyber dangers are rightly grouped with the array of potential nonconventional threats, but the *National Defense Strategy* presents them solely as a *challenge*—not as an opportunity for exploitation. Further, the strategy has a tendency to think even more narrowly than the president's strategic guidance in that it more readily associates cyber threats with asymmetric warfare against the United States by a weaker adversary: "Small groups or individuals . . . can attack vulnerable points in cyberspace . . . causing economic damage, compromising sensitive information and materials, and interrupting critical services such as power and information networks."[9]

Finally, the *National Military Strategy of the United States of America* (2011) contemplates cyberspace not simply as a prospective "Achilles' heel" but as a domain in which the United States can and should *prosecute* operations. It readily accepts the impending challenges to the enabling capability of cyber when it stipulates that "assured access to and freedom of maneuver within the global commons—shared areas of sea, air, and space—and globally connected domains such as cyberspace are being increasingly challenged by both state and non-state actors."[10] However, the strategy departs from its parent documents issued by the president and secretary of defense when it establishes that "enabling *and war-fighting domains* of space and cyberspace are simultaneously more critical for our operations, yet more vulnerable to malicious actions" (emphasis added).[11] Here, a reader of senior strategic policy guidance gets a first mention of cyberspace as an arena in which warfare, albeit principally nonkinetic, takes place. This dual-purpose con-

text is comparable to that of any other domain. For example, in the air domain, one can perform aerial resupply of forward operating bases (an enabling function) or bombing strikes of armored columns (a war-fighting function). More to the point, the *National Military Strategy* declares that "space and cyberspace enable effective global war-fighting in the air, land, and maritime domains, *and have emerged as war-fighting domains in their own right*" (emphasis added).[12]

Further downstream from the chairman of the Joint Chiefs of Staff's strategy document, the outlook in the *Joint Operating Environment* makes comparable assessments about the unfolding dynamics of cyberspace. It addresses threats *within* cyber, such as its becoming a "main front in both irregular and traditional conflicts," as well as the range of *adversaries* from "states and non-states . . . from the unsophisticated amateur to highly trained professional hackers."[13] One finds a more direct call to action, however, in the *Universal Joint Task List* (under "Manage Cyberspace Operations"), which charges "services and agencies [to] ensure *offensive* and defensive capabilities are fielded and ready to further DOD and United States . . . national security objectives in cyberspace" (emphasis added).[14] Although lacking the *Joint Task List*'s demand for offensive capability within cyberspace, the *Joint Operating Environment* does issue a challenge—as does the *National Military Strategy*—to rethink the organizational and doctrinal construct of the DOD's cyber enterprises.

In the *Joint Operating Environment*, one reads that "while progress toward defining requirements and advocating for Service cyberspace forces has been made, cyber threats will demand a new mindset to ensure agility in adapting to new challenges."[15] Similarly, but with more emphasis on the organizational issues ahead, the *National Military Strategy* posits that "we will carefully review legacy personnel systems. . . . The emerging war-fighting domain of cyberspace requires special attention in this regard."[16] Within the parameters of these strategic vectors of "new mindset," "agility," and manpower, there is latitude to approach cyber capabilities, roles, and missions *not* as extrapolations of

existing organizations and doctrines but as unique problems worthy of innovative solutions.

At the COCOM and service levels, bottom-up approaches to cyber warfare have been divided more appropriately between maintaining access to the enabling functions of cyber (defense) and the ability to exploit and attack adversary networks (offense):

> USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations . . . in order to ensure U.S. and allied freedom of action in cyberspace, *while denying the same to our adversaries*.[17] (emphasis added)

The phrase "denying the same" conveys a deliberate and active application of cyber capability against an enemy to create effects in a manner consistent with effects-based operations, which are "planned, executed, assessed, and adapted to influence or change systems or capabilities in order to achieve desired outcomes."[18] Linking actions to objectives, one can generate effects either kinetically or nonkinetically. The utilization of cyber capabilities to affect nodes within a system—especially within a system-of-systems—can create effects whose outcomes far exceed the inputs. Especially because warfare is complex and nonlinear, a small cyber action against a nodal construct can produce disruptive consequences.

A Combatant Command Model

According to Joint Publication 1, *Doctrine for the Armed Forces of the United States*, functional COCOMs are "responsible for a large functional area requiring single responsibility for effective coordination of the operations therein. These responsibilities are normally global in nature."[19] Beyond this operational orientation, US Special Operations Command (USSOCOM) also merges *service-like* authorities and responsibilities with those typically associated with other functional COCOMs. Like a hybrid of a service and a COCOM (e.g., the US Navy and

US Central Command), USSOCOM prepares forces for fielding and then plays a role when they go into battle.

Following the passage of the Defense Reorganization Act of 1986, USSOCOM was established as a four-star unified command "responsible for preparing Special Operations Forces to carry out assigned missions and, if directed by the President or Secretary of Defense, to plan and conduct special operations."[20] The first charge, "preparing Special Operations Forces," is comparable to that of any service; the second, "to plan and conduct special operations," falls within the realm normally associated with a COCOM.

The *Unified Command Plan* of 2004 "assigned USSOCOM responsibility for synchronizing Department of Defense plans against global terrorist networks and, as directed, conducting global operations [against those networks]."[21] To do so, the command "receives, reviews, coordinates and prioritizes all DoD plans . . . and then makes recommendations to the Joint Staff regarding force and resource allocations to meet global requirements."[22]

If USSOCOM performs both service-like duties to build a force and COCOM-like authorities to employ it, then the command provides for an organization that

1. develops strategy and doctrine to address unique challenges;
2. has budgetary authority to recruit, organize, train, and equip select personnel;
3. can provide resources to COCOMs in a supporting role; and
4. can conduct operations worldwide in a supported role.

This blending of service-style title 10 responsibilities with COCOM-style authorities allows for an organization with a worldwide mandate that can marry the right personnel to its mission; develop nimble tactics, techniques, and procedures; and wage war against the enemy along the spectrum of conflict. USCYBERCOM should adopt this model.

Recommendations

A functional COCOM that recruits, organizes, trains, equips, and employs cyber capabilities as weapons in warfare's newest domain is essential to contemporary conflict. Just as Air Force Special Operations Command, Marine Special Operations Command, Army Special Operations Command, and Navy Special Warfare Command are component commands of USSOCOM, so would Army Forces Cyber Command, Twenty-Fourth Air Force, Fleet Cyber Command, and Marine Forces Cyber Command retain their affiliations as service components of USCYBERCOM.[23] Like the components currently comprising USSOCOM, the components of the elevated USCYBERCOM should include personnel uniquely and thoroughly suited to its core mission.

Existing manpower models demonstrate the effectiveness of a long "tooth-to-tail" ratio for certain force constructs. Of the nearly 60,000 members of USSOCOM, only about 20,000 of them are "operators"—individuals recruited, trained, and retained as special forces.[24] Looking at another community for context, that of remotely piloted aircraft, one sees that the number of pilots and sensor operators represents but a fraction of the overall required manpower. This model reinforces the concept of a centrally controlled cyber operations center, given that mission operators of these aircraft can perform global functions from a geographically separated garrison installation.

The ratio of support personnel to cyber operators needs further research, but, more than likely, the operators would receive support from a larger number of administrative and technical specialists. Similar to the US Army's "SOF [special operations forces] Truths" that "quality is better than quantity" and that "humans are more important than hardware," not every "cyber soldier" need be a hunter-killer.[25] Rather, the majority of USCYBERCOM would include the various administrative and logistics support personnel that make up any other command, with emphasis on deliberately recruiting, training, equipping, and retaining those select men and women best suited to the dual missions of cyber defense and cyber attack.

Following, or in conjunction with, a revision of the *Unified Command Plan*, legislative action would provide budgetary authority to USCYBERCOM—like that of the services and USSOCOM—and would specify roles and missions, necessitating a change to title 10 *United States Code* (Armed Forces), part 1 (Organization and General Military Powers), chapter 6 (Combatant Commands). Aside from devising regulations to incorporate the above-mentioned statutory change in the status of USCYBERCOM, the DOD would need to revise its planning, programming, budgeting, and execution process.[26] Like Major Force Program 11, Special Operations (MFP-11) in the *Future Years Defense Program*, the DOD should establish a dedicated major force program (e.g., "MFP-12 Cyber Operations"), along with a budgetary entry for USCYBERCOM (similar to what USSOCOM, the services, and DOD agencies currently have).[27]

Finally, to wage cyber warfare, a standing joint cyber task force (JCTF) should be established within USCYBERCOM. Acting as both a fusion cell for worldwide monitoring of cyber threats and a command authority through which the secretary of defense, in communication with the Joint Chiefs of Staff, can direct USCYBERCOM to conduct its COCOM mission, this JCTF would plan for and direct offensive and counterattack operations within cyberspace against the spectrum of adversaries threatening US national interests, cyber or otherwise.

Conclusion

A USCYBERCOM empowered to organize, train, and equip its forces *and* employ them against adversaries can more fully build and exploit capabilities within warfare's newest domain. So long as a cyber force remains subordinated to potential service or traditional war-fighting parochialism, it will be hindered in weaponeering its capacity to inflict effects in the battlespace. By providing its leaders more freedom of movement within the DOD bureaucracy, USCYBERCOM will allow them to develop and maintain combat power in a way that is less hampered by the conventional focuses of their respective branches—just as

airpower underwent reexamination as a capability that transcended its supporting effects to the Army's battlefield doctrine. Once its forces are fully developed and available, a USCYBERCOM with functional COCOM authority to conduct operations against nodal systems is positioned to create disproportional and potentially catastrophic effects. These effects—some of which can be "undone," given their often nonkinetic nature—can be produced through surgical application by a standing JCTF. ✪

Notes

1. Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations* (Washington, DC: Chairman of the Joint Chiefs of Staff, December 2006), vii, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.
2. Eleonore Kofman and Gillian Youngs, eds., *Globalization: Theory and Practice* (New York: Pinter, 1996), 111.
3. *Stanford Encyclopedia of Philosophy*, Fall 2008 ed., s.v. "War," http://plato.stanford.edu/archives/fall2008/entries/war/.
4. US Joint Forces Command, *The Joint Operating Environment* (Suffolk, VA: US Joint Forces Command, Joint Futures Group, 18 February 2010), 34–36, http://www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf.
5. Forrest Hare, "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers, Cryptology and Information Security Series, vol. 3 (Fairfax, VA: Ios Press, 2009), 5.
6. President of the United States, *National Security Strategy* (Washington, DC: White House, May 2010), 17, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
7. Ibid., 27.
8. Department of Defense, *National Defense Strategy* (Washington, DC: Department of Defense, June 2008), 1, http://www.defense.gov/news/2008%20national%20defense%20strategy.pdf.
9. Ibid., 7.
10. Joint Chiefs of Staff, *National Military Strategy of the United States of America* (Washington, DC: Joint Chiefs of Staff, 2011), 3, http://www.jcs.mil//content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf.
11. Ibid.
12. Ibid., 9.
13. US Joint Forces Command, *Joint Operating Environment*, 36.

14. *Universal Joint Task List*, version 7.1, 17 July 2012, [244], http://www.dtic.mil/doctrine/training/ujtl_tasks.pdf.

15. US Joint Forces Command, *Joint Operating Environment*, 36.

16. Joint Chiefs of Staff, *National Military Strategy*, 17.

17. "U.S. Cyber Command," United States Strategic Command, December 2011, http://www.stratcom.mil/factsheets/Cyber_Command/.

18. Air Force Doctrine Document 2, *Operations and Organization*, 3 April 2007, 13, http://www.e-publishing.af.mil/shared/media/epubs/afdd2.pdf.

19. Joint Publication 1, *Doctrine for the Armed Forces of the United States*, 2 May 2007 (Incorporating Change 1, 20 March 2009), I-14, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

20. "U.S. Special Operations Command—SOCOM," US Department of Defense, accessed 9 November 2012, http://www.defense.gov/OrgChart/office.aspx?id=62.

21. "About USSOCOM," United States Special Operations Command, accessed 9 November 2012, http://www.socom.mil/Pages/AboutUSSOCOM.aspx.

22. Ibid.

23. "U.S. Cyber Command Fact Sheet," US Department of Defense, 25 May 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf.

24. Senate, *Hearings before the Committee on Armed Services to Authorize Appropriations for Fiscal Year 2012 for Military Activities of the Department of Defense and for Military Construction, to Prescribe Military Personnel Strengths for Fiscal Year 2012, and for Other Purposes*, 112th Cong., 1st sess., http://www.gpo.gov/fdsys/pkg/CHRG-112shrg68084/html/CHRG-112shrg68084.htm. In this document, see US Special Operations Command and US Central Command, 1 March 2011, and posture statement of Adm Eric T. Olson, USN, commander, US Special Operations Command.

25. "SOF Truths," US Army Special Operations Command, accessed 9 November 2012, http://www.soc.mil/USASOC%20Headquarters/SOF%20Truths.html.

26. "Planning, Programming, Budgeting & Execution Process (PPBE) (Biennial Driven)," Defense Acquisition University, 27 September 2012, https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=10fdf6c0-30ca-43ee-81a8-717156088826.

27. Department of Defense, *Future Years Defense Program (FYDP) Structure* (Washington, DC: Department of Defense, Office of the Director, Program Analysis and Evaluation, April 2004), 6, http://www.dtic.mil/whs/directives/corres/pdf/704507h.pdf; and Maj Robert Siau, commander, 143rd Combat Communications Squadron Detachment, Washington Air National Guard, discussion with the author, March 2011.

Lt Col Shawn M. Dawley, ANG

Lieutenant Colonel Dawley (BS, MBA, Embry-Riddle Aeronautical University; MA, Marine Corps University; MA, American Military University) is commander of the 165th Airlift Squadron, Kentucky Air National Guard. A C-130 pilot who has flown combat and combat-support sorties in support of Operation Enduring Freedom, Operation Iraqi Freedom, Operation Joint Forge and Joint Guard, and Operation Southern Watch, he most recently served as commander of the 737th Expeditionary Airlift Squadron in Southwest Asia. Lieutenant Colonel Dawley has completed Squadron Officer School, Air Command and Staff College, Marine Corps Command and Staff College, Air War College, and the Joint Force Staff College's advanced joint professional military education.

Let us know what you think! Leave a comment!

A New Chief of Staff, a Golden Opportunity

Building the Right Force over the Next Decade

Maj Timothy B. Murphy, USAF

With budget cuts beginning to take effect and sequestration looming, yesterday's carefully laid plans are quickly fading into oblivion. During constrained times, it is easy to reject ideas as unattainable, but we must remember to keep events in context. Even a brief glimpse into our service's history reveals that fiscal and political issues should not derail foundational concepts. Consider the state of the United States Air Service in the months directly following the end of World War I. After the Air Service played a major role in Germany's defeat and unequivocally demonstrated the potential of airpower, its leaders endured a drawdown which turned that fledgling organization into a hollow shell. The service contracted from 185 aero squadrons and 197,338 total personnel to 22 squadrons and 9,596 personnel—decreases of 88 and 95 percent, respectively![1] Yet, even in the midst of draconian cuts and an inhospitable political environment, the Air Service incrementally laid the groundwork for a phenomenally successful Air Corps and independent Air Force.

Today, Gen Mark A. Welsh III, the new chief of staff of the Air Force, faces a similar situation, though far less extreme than the one that confronted Air Service leaders after World War I. Budget cuts and political obstacles threaten the Air Force's recent progress toward balancing its capabilities in both conventional and irregular warfare (IW). Procurement of fifth-generation aircraft is essential for the Air Force, but this should not deter the new chief from building the right force over the next decade. One of the major issues for the service involves developing a balanced force capable of *efficiently* responding to threats across

the spectrum of warfare. The Air Force adapted very well to the conflicts of the last decade, but it still lacks an appropriately proportioned and agile force structure and organization. Historically, the Air Force has planned, prepared, and equipped its force to deal with conventional threats and adapted as necessary in irregular conflicts. In 2008 Secretary of Defense Robert Gates famously admonished military leaders for failing to deploy needed assets to the theatre: "Because people were stuck in old ways of doing business, it's been like pulling teeth."[2] Rather than constantly adapting and enduring scathing comments from defense secretaries, the Air Force should begin now to lay the foundation for a balanced force capable of both fighting our nation's high-intensity wars and countering IW's threats to the legitimacy of friendly nations.

This article demonstrates how to build the right force even in an uncertain fiscal and political environment. It briefly discusses the Department of Defense's (DOD) current strategic guidance and the Air Force's plans to implement it with regard to IW; identifies the gaps between that guidance and Air Force implementation; and then suggests a series of incremental steps that the service should take to fill the gaps, developing the right force for the future in the process. The key to the latter entails empowering operational wings with a far greater ability to fight and win both conventional and irregular conflicts. Continuing to segregate IW missions and execution in disparate units throughout the Air Force will only prolong institutional apathy and unpreparedness for IW.

The Current Environment

The DOD's strategic guidance of January 2012 articulates new priorities for sustaining US global leadership in the twenty-first century. Although the guidance directs a rebalance toward the Asia-Pacific region, it also warns of destabilizing threats and violent extremists worldwide, particularly in the Middle East.[3] Granted, the new "pivot to Asia" commonly evokes thoughts of greater roles for conventional forces, but at

the same time, it involves a significant need for irregular forces. If the Asia-Pacific region truly has substantial strategic value, then the United States will likely become engaged in countering threats to the legitimacy of its partner nations in the region. The strategic guidance anticipates this involvement by initiating an expansion of the United States' partnership with aligned nations to fulfill national priorities.[4] Thus, the shift from Iraq and Afghanistan to Asia may actually increase the importance of countering irregular threats over the next decade.

Before the new strategic guidance came down from the DOD, the Air Force had worked for several years to improve its ability to operate in an IW environment. Airmen have labored tirelessly over the last decade to provide world-class close air and intelligence, surveillance, and reconnaissance (ISR) support to ground troops as well as use global mobility to sustain conflicts in multiple theatres. As the conflicts progressed, the Air Force experienced unprecedented advances in combat medical care and made available thousands of individual augmentees to ground commanders and joint headquarters across the globe. During this time, Air Force Special Operations Command expanded its role, offering unequaled support to special operators throughout the joint force. The service also improved its capacity to supply air advisors who help shape air forces in partner nations. Finally, the Air Force developed detailed plans to acquire both light attack and light mobility aircraft that would further its efforts in building partnership capacity (BPC).

In light of the publication of the DOD's strategic guidance, the service is now in the final stages of preparing an operational road map for IW that will outline its contributions to the department's efforts in both BPC and IW. The document refers to this type of warfare as a struggle for legitimacy and influence over a relevant population rather than the coercion of key political leaders or the defeat of their military forces.[5] It includes several goals, such as creating an institutional air-advisor capability in the general-purpose force, training Airmen to become equally proficient and capable in conventional warfare and IW,

equipping them for countering irregular threats, and developing the capacity of willing partner nations' security forces.[6] Two objectives—fielding small teams of regionally oriented, expert trainers and establishing regionally aligned IW-capable forces—seek to attain some of the goals laid out in the road map, just as other goals and corresponding objectives are designed to improve the Air Force's capabilities in IW and BPC.

The Gaps

Sections of Headquarters Air Force have outlined excellent plans to assist these two efforts in the DOD's guidance, but without corresponding changes in the service's organization and structure, the road map will probably fall short of its aims. The fact that the bulk of the Air Force's general-purpose force consists of operational fighter, bomber, and mobility units reflects a service organized primarily to fight in conventional conflicts. However, these units—the backbone of the Air Force—will have little involvement in air advising and BPC unless leadership forces a shift in mind-set. Fighter, bomber, and mobility units care about what appears on their designed operational capability (DOC) statement—essentially a narrative description of a unit's wartime missions. If air advising, BPC, and other IW efforts are tasked only to specialized units in the general-purpose force, then the foundational units of the Air Force will have little to no role in the process. In fact the service has historically assembled ad hoc units for IW and then disbanded them when it perceived they had become unnecessary.[7] Generating an institutional air advisor capability in the general-purpose force will prove difficult if it does not include units that carry out the Air Force's primary missions.

Another major area—the Air Force's structure—will likely cause IW and BPC efforts to fall short. Gen Norton Schwartz, former chief of staff of the Air Force, argued in 2010 that the service had only a limited need for a light attack platform because current aircraft could service any close air support requirement.[8] He advocated acquiring 15 light

attack aircraft for BPC, and the Air Force included both those platforms and light mobility aircraft in its budget requests for fiscal years 2012 and 2013. Unfortunately, the service recently cut both programs, and the future of both aircraft is very much in question. Congress also expressed skepticism about these programs, but its concerns had to do with the plan to use the aircraft only for BPC missions.[9]

The Air Force eliminated the light aircraft program even though it has no dedicated capability within the general-purpose force to conduct IW. This is not to say that the service cannot perform in an IW environment—today's fighter, bomber, ISR, and mobility units effectively conducted their missions during the last decade. However, using advanced weaponry in an irregular conflict has its costs—and they are significant. An Air Combat Command study of 2008 concluded that replacing just one-and-a-half squadrons of deployed fighters with light attack aircraft would save well over $300 million per year in fuel and operations costs.[10] These are enormous savings, especially considering the fact that for most of the past 10 years, the Air Force had more than four fighter squadrons deployed in Central Command's theatre *at the same time*. These expenses do not even include degradation of the service life of fighters and bombers caused by the extremely high operations tempo since 2001.[11]

Clearly, the Air Force could benefit from a change in mind-set, allowing it to alter its organization and structure to pursue BPC and IW more effectively. But we must ask ourselves whether such change is a worthy task—and if so, is it possible in the midst of significant budget cuts and political uncertainty? The answer to both questions is yes, but such action will demand a firm commitment from Air Force leadership, not to mention a specific (and cost-effective) plan for cultivating the right force over the next decade.

The Way Ahead

The plan to balance the force outlined below draws on two major premises. First, air and space superiority will and should always be the top priority of the Air Force. The other important core functions, such as global attack, rapid global mobility, and agile combat support, all depend upon that superiority. Buying the aircraft and support infrastructure to assure superiority is an expensive but a necessary priority for the Air Force, and this should not change. Second, the service could balance the force by taking incremental steps over the next several years. At present it has very little dedicated capability to conduct IW and expeditionary BPC within the general-purpose force, but the Air Force does not need to acquire these capabilities in the short term. The last decade proved that its current organization and structure can adapt to irregular conflict, so changes can safely take place over the long term. The service should set a goal of developing a proportional force over several years, but it should not view the latter in terms of dollars but in terms of *capability* and *efficiency*. Conventional missions, aircraft, and equipment will always involve considerable cost, but the Air Force needs to acquire new resources and personnel that will balance its capability to carry out both irregular and conventional warfare.

To produce the right force, the service should implement three successive stages: (1) make its operational wings responsible for IW and BPC missions, (2) resurrect the light attack aircraft and light mobility aircraft programs, and (3) work toward supplying most of its operational wings with indigenous personnel and light aircraft intended for BPC and IW missions. The Air Force can do so by spreading the costs of implementation over several years.

Stage One: Shifting Responsibility to Operational Wings

The first step in building the right force should focus on improving the IW and BPC capabilities of operational wings—more a shift in mind-set than in personnel and resources. Currently, operational wing commanders must fill, among others, individual augmentee or joint expe-

ditionary taskings, the latter directly supporting Army units and the former filling non-service-specific positions on the joint manning document. Wing commanders receive these deployment taskings and identify members within their unit to fill each assigned position. The wing is responsible for equipping its members, but most predeployment training occurs elsewhere. If an entire unit within the wing (such as a fighter squadron) receives deployment orders, most of its members typically prepare together and then deploy together. Unit deployments always mirror missions designated on the wing's DOC statement. Thus, the wing spends most of its time preparing and training personnel for deployments that will support potential missions on that statement.

To fully institutionalize IW and BPC missions within the general-purpose force, the Air Force should include these various missions on the DOC statements of operational wings. As indicated above, those wings already send their members on such missions, but changing the statement will formalize the process. Instead of relying almost exclusively on outside agencies to train members quickly, prior to deployment, the wing should have a cadre of personnel trained, equipped, and prepared for IW and BPC missions.

Furthermore, the Air Force should move responsibility to operational wings in a way that minimizes costs. Forming a cadre of wing-level personnel dedicated full-time to these two missions is unrealistic and, frankly, unnecessary. Instead of creating new units or organizations, the service should model its IW/BPC cadre after a functional organization like Wing Safety, whereby each wing could have an IW office that would develop and sustain the aforementioned cadre. Like Wing Safety, this office should have one field grade officer and a few dedicated noncommissioned officers to administer and oversee the program. Each squadron within the wing should have two or three IW personnel. The IW cadre would consist of subject-matter experts who prepare the rest of the squadron for IW missions. Like a squadron's safety tasks, its IW tasks should be additional duties, and IW personnel

should still perform the unit's primary mission. Ideally, the Air Force would track IW personnel through career-field designation prefixes and offer incentives such as ribbons or badges.[12]

After the experience of the last 10 years, constructing an IW program at the wing level would prove comparatively straightforward. Thousands of Airmen have deployed as individual augmentees or have done so to fill positions for joint expeditionary taskings; consequently, each operational wing already has a large pool of experienced personnel. If the Air Force waits to leverage this experience, it will miss a valuable opportunity. The three designated people in the IW office, mentioned above, should receive specialized instructor training at the Air Advisor Academy so they can teach quarterly IW refresher training to the wing's IW personnel. Wing commanders should then have squadron commanders solicit volunteers to fill the squadron's IW positions, giving preference to experienced individuals, sending them to initial training at the academy, and having them undergo quarterly training from the wing's IW office. The latter instruction should help these personnel prepare their unit members for deployment taskings. Ideally, when the wing receives such a tasking, its IW office (in conjunction with squadron commanders) should deploy IW personnel who match the career fields requested in the tasking. Even if IW personnel are not available, regular IW training at the unit level will better prepare all unit personnel for IW taskings.

Giving operational wings the responsibility for these taskings has several benefits. For example, the Air Force can capitalize on the experience gained by many of its members during the last decade. Thousands of Airmen have a great deal of combat experience outside the normal scope of their duties, and the service should work hard to capture that experience. Fostering a cadre of IW personnel at the wing level and providing quarterly training for them will enhance the preparation and quality of Airmen that the Air Force sends to fill these tasks. Rather than trying to quickly prepare Airmen just prior to a deployment, the service will have an abundance of well-trained personnel for these

missions. The greatest benefit, however, will come from innovation at the wing level. Shifting responsibility for these missions from centralized, specialized units to the larger Air Force will allow for greater ingenuity and innovation. Decentralization provides additional opportunities such as forming regionally aligned wings and allocating funds for classroom instruction in language and culture for IW personnel at the wing level. Regional alignment would further enhance the capabilities of IW personnel who receive deployment orders. As global combatant commanders begin to see the benefits of well-trained IW Airmen, they likely will encourage further innovation and improvement.

Stage Two: Reinstate the Light Attack and Light Mobility Programs

As the Air Force moves greater responsibility for IW and BPC to the wing level, it must renew the light attack aircraft and light mobility aircraft programs. The service will never truly balance its conventional and IW capabilities without making such an investment. Rather than compartmentalize these programs in specialized units, it should base the aircraft at wings tasked with conventional missions, sending light attack aircraft to fighter and bomber wings and light mobility platforms to mobility wings. Basing these aircraft at wings tasked with conventional mission sets will further institutionalize a balance between conventional and IW missions.

The Air Force could reduce the costs and personnel involved in fielding light aircraft by allowing wing pilots to become dual-qualified in both these and primary aircraft. For example, it could base light attack aircraft at an F-16 wing, which could qualify some or all of its pilots on them—a decision that would drastically lessen the expense of building additional squadrons and give pilots a greater breadth of experience. The Air Force could model the light attack and light mobility dual-qualification program on similar programs at U-2 and B-2 bases, as well as the old Accelerated Copilot Enrichment program, both of which offer a much cheaper way of developing flight experience in aircraft other than their primary ones.

Additionally, fighter and bomber wings could maintain a limited number of dedicated light attack pilots and dual-qualify the remainder, who could then fly either airframe and gain experience where the wing deems necessary. If the wing is tasked with missions in a permissive air environment, it could deploy its light attack aircraft and pilots instead of the high-cost, less-efficient fighters or bombers. Maintaining unit readiness with pilots dual-qualified on two combat airframes might present problems, but solutions certainly exist. Squadrons could designate certain pilots to maintain a higher state of readiness in light attack aircraft for a period of time and then periodically rotate those personnel. Dual-qualification would also alleviate concerns that pilots of the light attack or light mobility squadrons are junior or inferior partners of those who fly more advanced aircraft.

Operational wings would also have an excellent additional asset for training sorties and an organic outlet for cuts in flying hours. Fighter and bomber squadrons could use the light attack aircraft as support for a variety of their combat missions. Indeed, pilots could even carry out some missions, such as close air support, in either aircraft. During periods of budget cuts or limitations on flying hours, the wing could keep its pilots flying by shifting more sorties to the light attack aircraft since flying hours for these platforms cost only a fraction of those for fighters or bombers. Pilot readiness might decrease slightly in the wing's primary aircraft, but the pilots could continue to accumulate useful hours in the light aircraft. Most of the benefits described above would also apply to mobility wings with light aircraft.

Furthermore, such aircraft are far more feasible with regard to BPC in developing countries. In March 2010, Gen James Mattis promoted light attack aircraft as a "means to build partner capacity with effective, relevant air support."[13] Many partner nations need reliable, capable, and easily maintained platforms from the United States instead of the high-tech aircraft that the Air Force currently operates.[14] The service requires organic light aircraft and trained pilots to conduct BPC missions effectively. If operational wings already possess light attack

and light mobility aircraft, then they can realize that objective. By adding the ideas from stage one, wing commanders could deploy several light aircraft and trained IW personnel in relevant career fields. These IW teams, having their own aircraft, would perform well in a variety of regions and countries around the world.

The Air Force should quickly initiate the process of balancing conventional and IW capabilities at the wing level. To begin, it should procure 15–30 light attack and light mobility aircraft in the budget for fiscal year 2015. Fifteen of the former (including acquisition and research and development) would cost approximately $289 million, and an equal number of the latter would amount to about $73 million.[15] The service should then base the light mobility platforms with the two mobility support advisory squadrons already tasked with BPC missions and use the light attack aircraft to quickly develop an initial cadre, basing them at a fighter wing to test the dual-qualification concept. Once the Air Force validates the idea behind using these aircraft, it can move on to the final stage.

Stage Three: Balancing the Force over Time

Modest, incremental changes over the long term are essential to creating the right force. If combatant commanders embrace the concept of wing IW cadres, the Air Force should expand the program as necessary to meet future needs. Ideally, every operational wing should have a cadre of IW personnel and the associated capability of immediately deploying fully trained and equipped individuals for IW or BPC missions. It should also plan to field larger numbers of aircraft after validating the light attack and light mobility concepts, preferably basing light mobility platforms at many operational mobility wings and light attack squadrons at numerous operational fighter and bomber wings. The Air Force should attempt to do so over several years and adjust the end state if it needs either more or fewer of these aircraft. Such a configuration would give the service the right force—proportional and capable of efficiently conducting both conventional and IW missions.

Addressing Concerns

The proposals offered here certainly raise valid concerns, such as the associated effects of reduced combat capability and elevated manning requirements.[16] The combat issue should not prove too problematic since light aircraft are intended only for permissive air environments or partnership missions. The actual costs of these aircraft are minuscule compared to those of typical Air Force acquisitions and are easily manageable if spread out over several years. The service can minimize manpower expenses if it allows pilots to dual-qualify on their primary aircraft and light aircraft, but additional manpower and maintenance costs will remain. However, it should view these marginally higher outlays in terms of the increased capabilities of light aircraft and well-trained IW personnel. By adding approximately six aircraft, five pilots, and 18 maintenance personnel per unit, the Air Force could fully equip multiple squadrons for operations across the conflict spectrum, expand the pilot pool to meet a variety of needs, and produce experienced pilots more quickly and cost-effectively.

The range, response time, and risk of light attack aircraft also represent legitimate concerns, the former two considered a measure of how quickly the Air Force can respond to ground forces' call for support. A fighter jet can be on station to provide such support much faster than a light aircraft, but viable solutions to these issues exist. Specifically, the service must move beyond the recent model of centralizing all of its combat assets at one or two bases in-theatre—a necessity for advanced jet aircraft but not for light aircraft, which can operate out of smaller airfields closer to ground forces and thus improve response times and range considerations. Just as the Army and Marine Corps always station aviation assets close to their corresponding maneuver units, so could the Air Force expand these helicopter-centric bases into small airfields capable of accommodating both rotary-wing and light aircraft.

With regard to the risks associated with employing light aircraft in permissive air environments where surface-to-air threats still operate, one must understand that all combat environments entail risks. Rotary

aircraft from all of the different services already operate in these environments, and light aircraft are far more survivable than helicopters. Such risk-based arguments against light aircraft are disingenuous and overlook the substantial dangers that rotary aircrews successfully deal with in combat zones every day.

Perhaps the greatest concern is that expanding IW capabilities will threaten primary Air Force core functions such as air and space superiority, rapid global mobility, and global strike. Granted, these functions will always have priority over IW—and rightly so—but this should not prevent the service from gradually balancing its force over the long term.

Conclusion

No doubt, General Welsh will confront a number of challenges during his tenure as chief of staff. To continue its mastery of the air, the Air Force must acquire the F-35 and replace or upgrade other aging airframes. However, the task of updating an aging fleet need not supplant all other priorities. In the future, our nation will call on its armed forces to perform missions across the spectrum of warfare; consequently, the Air Force should build a force capable of efficiently answering any such request. Budget issues will exist in the near future, but the service can afford to build up its IW capabilities incrementally. Maintaining the status quo will permit the Air Force to continue its conventional superiority, but it will be forced to send F-22s and F-35s, instead of A-10s and F-16s, to austere, permissive locations. Twenty-five years from now, costs associated with flight hours and service life of fifth-generation fighters will prove astronomical in an irregular conflict. Is this really what we want when we can start changing now? ✪

Notes

1. "Air Force History Overview," Official Web Site of the United States Air Force, accessed 13 June 2012, http://www.af.mil/information/heritage/overview.asp.

2. Michael Hoffman, "Gates Puts Pressure on Call for More UAVs," *Air Force Times*, 21 April 2008, http://www.airforcetimes.com/news/2008/04/airforce_uav_callout_042108/.

3. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: Department of Defense, 2012), 2, http://permanent.access.gpo.gov/gpo18079/DefenseStrategicGuidance.pdf.

4. Ibid., 3.

5. "United States Air Force Irregular Warfare Operations Roadmap FY12–FY16," draft (Washington, DC: Headquarters US Air Force, July 2012).

6. Ibid.

7. Lt Col George H. Hock Jr., "Closing the Irregular Warfare Air Capability Gap: The Missing Puzzle Piece; Rugged Utility Aircraft and Personnel," *Air and Space Power Journal* 24, no. 4 (Winter 2010): 61, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj10/win10/2010_4.pdf.

8. Michael Hoffman, "Schwartz: No Light Attack Aircraft in Combat," *Air Force Times*, 7 May 2010, http://www.airforcetimes.com/news/2010/05/airforce_irregular_warfare_050710/.

9. An internal Air Force memo dated 12 February 2010 outlined legal concerns that the light attack aircraft would not meet the "Purpose Statute" of 31 *United States Code*.

10. Col Russell J. Smith, "Common Sense at the Crossroads for Our Air Force," *Air and Space Power Journal* 26, no. 2 (March/April 2012): 106, http://www.airpower.maxwell.af.mil/digital/PDF/Issues/2012/ASPJ-Mar-Apr-2012.pdf.

11. The costs briefly outlined above will increase astronomically in the future if the Air Force can respond only with F-22s, F-35s, and B-2s.

12. Flying and ground-safety officers in certain career fields are tracked by including an "S" prefix in their Air Force specialty code.

13. "Statement of General James N. Mattis, USMC Commander, United States Joint Forces Command before the Senate Armed Services Committee, March 9, 2010," USJFCOM, accessed 15 October 2012, http://www.jfcom.mil/newslink/storyarchive/2010/sp030910.html.

14. Smith, "Common Sense," 97–98.

15. Briefings, A5 Plans to Air Force chief of staff, Pentagon, subject: Headquarters Air Force Internal Light Attack / Armed Reconnaissance and Light Mobility Aircraft, 11 January 2011 and 28 February 2011.

16. Maj Steven T. Tittel, "Cost, Capability, and the Hunt for a Lightweight Ground Attack Aircraft" (master's thesis, US Army Command and General Staff College, Fort Leavenworth, KS, 2009), 64–65, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA510947.

Maj Timothy B. Murphy, USAF

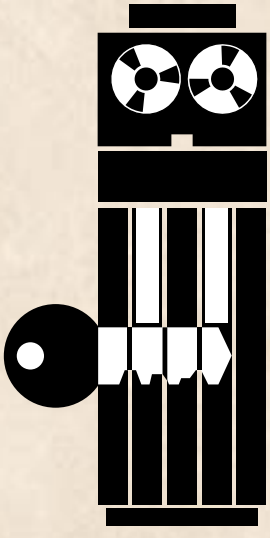
Major Murphy (USAFA; MA, Troy University; MA, National Defense University) is an AFPAK Hand assigned to the Irregular Warfare Strategy, Plans, and Policy Division for the director of operations, Headquarters US Air Force, Washington, DC. He is responsible for developing strategy, plans, and policy to organize, train, and equip the Air Force's air, space, and cyberspace forces for irregular warfare. An F-16 pilot who has already completed one AFPAK Hand tour in Afghanistan at International Security Assistance Force Joint Command, he previously served as an evaluator for the 56th Operations Group. Major Murphy is a graduate of Squadron Officer School, Air Command and Staff College (by correspondence), and the College of International Security Affairs at National Defense University.

Let us know what you think! Leave a comment!

Computer Security

*the Achilles' heel of the electronic Air Force?**

Lieutenant Colonel Roger R. Schell



The KGB officer addressed the select group of Soviet officials with his usual tone of secrecy but an unusual air of excitement:

> Comrades, today I will brief you on the most significant breakthrough in intelligence collection since the "breaking" of the "unbreakable" Japanese and German cyphers in World War II—the penetration of the security of American computers. There is virtually (if not literally) no major American national defense secret which is not stored on a computer somewhere. At the same time, there are few (if any) computers in their national defense system which are not accessible, in theory if not yet in fact, to our prying. Better still, we don't even have to wait for them to send the particular information we want so we can intercept it; we can request and get specific material of interest to us, with virtually no risk to our agents.

*Reprinted from *Air University Review* 30, no. 2 (January–February 1979): 16–33.

> The Americans have developed a "security kernel" technology for solving their problem, but we need not be concerned—they recently discontinued work on this technology. They are aware of the potential for a computer security problem, but with their usual carelessness they have decided not to correct the problem until they have verified examples of our active exploitation. We, of course, must not let them find these examples.

Your first reaction to this scenario may be, "Preposterous!" But before you reject it out of hand, recognize that we know it could happen. The question is: Will we apply sound technology and policy before it does happen? To be sure, there are things we do not know about the probability of success of such an effort, but we can rationally assess the most salient controlling factors:

• The high *vulnerability* of contemporary computers has been clearly indicated in the author's experience with undetected penetration of security mechanisms. In addition, security weaknesses are documented in both military and civil reports.

• The *capability* of the Soviets (or any other major hostile group) to accomplish the required penetration is quite evident. In fact, no particular skills beyond those of normally competent computer professionals are required.

• The *motivation* for such an information collection activity is apparent in prima facie evidence. The broad scope and high intensity of Soviet intelligence efforts in areas such as communication interception are frequently reported.

• The potential *damage* from penetration is growing with the ever increasing concentration of sensitive information in computers and the interconnection of these computers into large networks.

Through computer penetration an enemy could, for example, compromise plans for employment of tactical fighters or compromise operational plans and targeting for nuclear missiles.

• The *opportunity* for hostile exploitation of these vulnerabilities is increasing markedly both because of the increased use of computers and the lack of a meaningful security policy controlling their use. In the name of efficiency many more people with less (or no) clearance are permitted easier access to classified computer systems.

We have a problem and a solution in hand. Detailed examination of a hostile nation's (e.g., Soviet) capability and motivation in those areas is properly in the realm of the intelligence analyst and largely outside the scope of this article. However, it will trace the outlines of the computer security problem and show how the security kernel approach meets the requirements for a workable solution—although recent termination has nipped in the bud very promising work toward a solution.

What Makes Computers a Security Problem?

Although a certain appreciation of subtlety is needed to understand the details of the computer security problem, our objective here is to illuminate the basic underlying issues. To understand these issues, I will examine not only the capabilities and limitations of computers themselves but also their uses.

First, we take for granted the fundamental need to protect properly classified sensitive military information from compromise. Security has long been recognized as one of the basic principles of war, and throughout history security or its lack has been

a major factor of the outcome of battles and wars. We can and do strictly control information when the dissemination is on paper. It is, therefore, illogical to ignore the fact that computers may disseminate the same information to anyone who knows how to ask for it, completely bypassing the expensive controls we place on paper circulation.

Second, we must appreciate that "exploitation of the phenomenal growth of computer science is a major area of technological emphasis within DoD."[1] We currently lack quantitative superiority (or even parity) in several force level areas, and computers appear to be able to provide the qualitative superiority we must have. The need for these capabilities is clear when we realize that "good C3 [command, control, and communications] capabilities can double or triple force effectiveness; conversely, ineffective C3 is certain to jeopardize or deny the objective sought."[2] Indeed, we have in a very real sense become an "electronic Air Force"[3] with computers at our heart.

Finally, we need to recognize that some major vulnerabilities may accompany the substantial benefits of computer technology. Most decision-makers cannot afford the time to maintain a thorough understanding of explosively developing computer technology. But they can even less afford to be ignorant of what the computer can do and also of how it can fail. In particular, a commander responsible for security must ensure that dissemination controls are extended to computers. He must be able to ask proper questions—to surface potential vulnerability for critical and unbiased examination.

historical lessons in emerging technology

It is not new to find that an emerging technology is a mixed blessing. In particular, the threat facing computers today is illustrated in the evolution of military electrical communications—an earlier revolutionary technology. Our compromise of the security of Axis communications was fundamental to the outcome of World War II, and computers now offer our enemies the opportunity to turn the tables on us.

Military communication specialists early recognized the vulnerability of electrical transmission to interception, e.g., through wire taps or surreptitious listening to radio signals. The solutions were simple and effective but drastic: restrict transmission only to relatively unimportant (viz., unclassified) information or to transmission paths physically guarded and protected from intrusion. Likewise, for several years the Air Force restricted computer use to either unclassified data or to a protected computer dedicated to authorized (cleared) users. In both instances the security solutions limited use of the technology where most needed: for important information in potentially hostile situations, such as battlefield support.

The communication security restrictions gave rise to various cryptographic devices. These devices were to encode information into an unintelligible and thus unclassified form so that protection of the entire transmission path was not required. But (of paramount importance to us here) this dramatically changed the very nature of the security problem itself: from a question of physical protection to a question of technical efficacy. The effectiveness of the cryptographic devices was argued, based not on careful technical analysis but rather on the apparent absence of a known way to counter

them. Presently, computer technology is in a position analogous with a similar argument for its effectiveness against unauthorized access to computerized information. In both instances, the arguments seem to offer an acceptable risk in spite of a de facto weak technical foundation.

Technically weak cryptographic devices found widespread military use because of false confidence and the pressing operational need for electrical communications. One notable example was the Enigma machine used by the Germans during World War II. Their high-level national command and control network used it for communication security throughout the war. As *The Ultra Secret* records, "the Germans considered that their cypher was completely safe."[4] Yet, before the war really got started, the British had in fact "solved the puzzle of Enigma."[5] The Air Force is developing a similar dependency with each (formal or de facto) decision to accredit computer security controls. In either case policy decisions permit a technical weakness to become a military vulnerability.

Examples during World War II show how the tendency to defend previous decisions (to accept and use mere plausible techniques) assures the enemy of opportunities for exploitation. In Europe the broken Enigma signals (called Ultra) "not only gave the full strength and disposition of the enemy, it showed that the Allied [troops] could achieve tactical surprise."[6] In fact, General Dwight Eisenhower stated that "Ultra was decisive."[7] *The Codebreakers* describes a similar misplaced trust by the Japanese and notes that American cryptanalysts "contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."[8] To be sure, the Germans "must have been puzzled by our

knowledge of their U-boat positions, but luckily they did not accept the fact that we had broken Enigma."[9] Similarly, the Japanese "hypnotized themselves into the delusion that their codes were never seriously compromised."[10] The Axis establishment, it seems, would not acknowledge its security weakness without direct confirming counterintelligence—and this came only after they had lost the war. As for Air Force computer security, the absence of war has precluded ultimate exploitation; yet, the lack of hard counterintelligence on exploitation has already been offered as evidence of effective security.

Although technical efforts led to these devastating vulnerabilities, it was nonetheless the technical experts like William Friedman who provided a sound technical basis: "His theoretical studies, which revolutionized the science, were matched by his actual solutions, which astounded it [the scientific community]."[11] Today our military makes widespread use of cryptographic devices with confidence. For computers, as for communications, the nub of the problem is the effectiveness of the security mechanism. Recent logically rigorous work has resulted in a security kernel technology. However, DOD is not yet applying this technology.

The thrust of this historical review is captured in the maxim, "Those who cannot remember the past are condemned to repeat it." The historical parallels are summarized in Table I. The main lesson to be learned is this: Do not trust security to technology unless that technology is demonstrably trustworthy, and the absence of demonstrated compromise is absolutely not a demonstration of security.

Electrical Communications		Electronic Computers
	Limited Use	
unclassified only protected paths		unclassified only dedicated facility
	Plausible Security	
cryptographic technology crucial to security no known counter weak technical foundation		internal security controls crucial no known penetration weak technical foundation
	Unwarranted Dependence	
false confidence in cryptography policy acceptance		false confidence in internal controls policy acceptance
	Underestimated Enemy	
repeated and undetected interception advocates demand counterintelligence		repeated, undetected, and selective access advocates demand counterintelligence
	Adequate Technology	
information theory		security kernel

Table I. Comparative evolution of security problems

distinction between computation and protection

A given computer in one installation may securely handle sensitive data, and an identical machine may be totally insecure in another installation. The key to understanding the computer security problem is to distinguish when the computer provides only computa-

tion and when it must also provide security. These are two very distinct cases.

In the first case, commonly called "dedicated mode," the computer and all its users are within a single security perimeter established by guards, dogs, fences, etc. By the use of secure communications, this perimeter may be geographically extended to remote terminals. Only these external security controls are required to maintain the security of the system. Use of the computer is restricted so that at any time all the users, remote or local, are authorized access to all the computerized information. A potential attacker must overcome the external controls and penetrate the inner sanctum of cleared personnel. The computer provides only computation; no failure or subversion of the computer itself can compromise security because of the protected environment.

In the second case, commonly called "multilevel mode," the computer itself must internally distinguish multiple levels of information sensitivity and user authorization. In particular, the computer must protect some information from certain users. For multilevel mode, internal security controls of hardware and computer programs must assure that each user may access only authorized information. For multilevel security the computer itself must clearly provide protection as well as computation. For the potential attacker, simply gaining access to the peripheral users of the computer will suffice—if he can penetrate the internal controls.

Multilevel security controls function analogously to a cryptographic device; their effectiveness is central to information security. Because of the inherent structure of computers, a multilevel security weakness invites repeated exploitation. Furthermore, those security failures internal to the computer are almost certain

to be undetected. In contrast to communications where enemy access to important traffic is a matter of chance, in a penetrated computer he has selective access, not only for extraction but also for modification of information of his choosing. All the worse, the processing power of modern computers provides this information rapidly and completely.

If we are worried about protecting our cryptographic codes, then we are indeed foolish to neglect our computers. And we must realize that multilevel mode can aid the attacker unless the internal controls of the computer itself provide reliable protection.

evidence of weak security controls

The critical question then is this: Dare we trust the internal security controls of computer programs and hardware? The author's experience with security weaknesses indicates that contemporary computers do not provide reliable protection. Computers proposed as sufficiently secure to protect sensitive information were checked for security shortcomings. A formally sanctioned "tiger team" looked for weaknesses in these supposedly secure computers. (For accuracy the examples will be limited to those evaluations in which the author personally participated.)

The tiger team operated as a legitimate user with only limited access to a small part of the information in the system. The team objective was to penetrate internal security controls and demonstrate that unauthorized access could be gained. In every instance of the author's experience, serious security weaknesses were discovered after only a few hours or days of effort.

Passwords for the asking. A common element of protection is a secret password or key that the user must provide in order to receive services or information. To be effective the secrecy of the passwords must be preserved. An IBM 370 computer with the time-sharing option (TSO) had remote terminals in various uncontrolled areas; the secret passwords restricted the users' access. This particular computer contained sensitive Air Force procurement source-selection information with tightly controlled dissemination. The tiger team members found that they had merely to ask by name for the password file and the passwords for all the TSO users would be printed for them—without a trace that the passwords had been compromised. The designers had overlooked the relationship between security and the ability to print a file.

Good commercials not enough. In the Pentagon a General Electric system called "GCOS" provided classified (secret) computation for the Air Staff and others with secured remote terminals at selected locations. The manufacturer made an advertising thrust about his security. Air Force advocates proposed making a multilevel system by adding unsecured remote terminals, for unclassified uses, for better coordination and efficiency. Again, passwords were to protect the sensitive information. When a user presented his password to the computer, GCOS checked a list of passwords to verify the user's legitimacy. To make this check, GCOS copied part of the list into its main memory. Among other flaws, the tiger team found that GCOS left this copy of the passwords where it could be printed easily and without trace. The designers had overlooked the possibility of deliberate misuse of a necessary computer function.

Government designers not perfect. After the Pentagon penetration, some advocates claimed that government designers with a greater awareness of security could avoid such flaws. An organization that processed sensitive intelligence data spent a substantial effort "fixing" basically the same GCOS system. They were confident they could maintain multilevel mode security. The tiger team found that these "fixes" could easily be circumvented. In this case not only could any user get at any information in the system but also he could access the classified information in computers connected in a network with that computer!

A contract cannot provide security. Basically the same GCOS system was selected for a major command and control system. Advocates assured the users that it would be made multilevel secure because security was required by the contract. An extensive tiger team evaluation found there were many deep and complex security flaws that defied practical repair—the computer was finally deemed not only insecure but insecurable.

The best security is not good enough. Honeywell Information Systems, with DOD sponsorship, modified the GCOS computer in an effort to improve several areas substantially, including security. The resulting Multiplexed Information and Computing Service (Multics) was widely touted for its security. The tiger team used an Air Force laboratory computer to evaluate Multics as a potential multilevel secure computer for the Pentagon. Although it had the best security design of any system encountered, the tiger team found several implementation flaws.[12] In one case Multics first checked a prospective user's authorization for access to information and, when the request proved valid, executed the request. However, the user could change the request after the validity check

but before execution; Multics then executed the changed request, allowing unauthorized access. This penetration of Multics came from an implementation short cut made to improve efficiency.

Encrypted passwords retrieved. The Multics system internally encrypted its password list so that even if printed out the passwords were not intelligible. When a user presented his password, it was encrypted and then compared to the encrypted list. The tiger team used the penetration technique developed on the laboratory computer to access the encrypted password list of a large university and then broke the cypher to obtain all the passwords.

Trap door installed. The tiger team penetrated Multics and modified the manufacturer's master copy of the Multics operating system itself by installing a trap door: computer instructions to deliberately bypass the normal security checks and thus ensure penetration even after the initial flaw was fixed. This trap door was small (fewer than 10 instructions out of 100,000) and required a password for use. The manufacturer could not find it, even when he knew it existed and how it worked. Furthermore, since the trap door was inserted in the master copy of the operating system programs, the manufacturer automatically distributed this trap door to all Multics installations.

Audit record destroyed. Some have argued that a computer need not always prevent unauthorized access as long as it keeps an audit record of such accesses. The Multics system kept a protected audit record of access, and the tiger team's unauthorized accesses were recorded. However, the audit record was itself subject to unauthorized access. The tiger team merely modified the record to delete all trace of its actions, such as insertion of the trap door.

Even fixes have holes. Honeywell produced a new Multics computer that corrected all the implementation flaws reported by the tiger team. The tiger team used Honeywell's new computer at their Phoenix, Arizona, manufacturing plant and penetrated the security again.[13] This new flaw resulted from changes made to correct the previous ones! It was becoming increasingly clear that providing a multilevel secure computer was indeed difficult.

Trojan horse not dead. While some had recognized the problem, advocates in the Air Staff were commending an installation for their multilevel security solution on another computer. The solution consisted of programs to segregate the classified and unclassified information. There were no remote terminals, but users could submit unclassified jobs to the computer without security checks. From an unclassified job the tiger team penetrated the underlying computer operating system and modified the solution into a Trojan horse, an apparently useful program that concealed harmful capabilities. The Trojan horse hid an invisible copy of classified jobs. A later unclassified job retrieved the hidden information, compromising security. Thus the security solution was not only ineffective but it actually exacerbated the security problem.

The obvious moral. Few if any contemporary computer security controls have prevented a tiger team from easily accessing any information sought. These examples are by no means exhaustive; they must not be used to infer predominance of certain flaws or to associate particular weaknesses with only a few manufacturers. Others have comparable security problems.

futility of evaluation by penetration

In a very real sense the Air Force has been fortunate that security is so poor in current computers—the greater danger will come when the argument that a computer is secure because tiger teams failed to penetrate it appears plausible. Indeed, evaluating internal computer security controls is a most difficult challenge. As with cryptography, there are basically two approaches.

If the security controls are based on a carefully formulated, sound technology, then they may be subject to rational analysis of their effectiveness. As already noted, this is generally not true of contemporary computers. The security kernel approach, which is subject to such methodical technical analysis, will also be discussed.

Alternatively, an advocate can simply search for ways to penetrate a computer's controls; failing to penetrate, he can plausibly argue there is no way to penetrate since none is known (to him). If a security hole is found, it can first be patched before arguing for security. Obviously, this argument suffers acutely from both theoretical and practical difficulties.

In principle, one could test all possible programs to find any that led to a security penetration. This method of exhaustion would be effective but is far beyond the realm of feasibility. For any substantial computer this would take so long that before the evaluation was finished the sun would literally have burned out! Thus, a realizable evaluation by exhaustion must be so incomplete as to be ludicrous.

In fact the effort spent in penetrating and patching yields poor marginal return in terms of security. The tiger team examples indicate some of the difficulties:

First, experience shows that new penetrators tend to find new holes—even after previous teams have found all they could. It seems unlikely that a real attacker will not involve new people.

Second, holes do not generally result from rank stupidity but from human oversight in dealing with a difficult design problem. Thus the fixes themselves are likely to be flawed.

Third, it does not take a highly specialized expert to penetrate security. It is true that most computer professionals do not know ways to penetrate the systems they use; they want to do a job, not interfere with it. Yet when given the assignment, even junior and inexperienced professionals have consistently succeeded in penetration.

Fourth, the exposure to attack is frequently much greater than from just the known system users. Commercial telephone connections to military systems are increasing and give worldwide access. Communication taps also give access to unsecured direct connections; microwave intercepts by the Soviets in the U.S., as recently revealed by the White House, demonstrate this capability. Lack of strict security control on the submission of computer jobs allows attacks in the name of a legitimate user even for computers without remote terminals. Interconnection to other computers can add a large group of unknown users as well.

Fifth, the attacks can be developed and perfected on other than the target computer. A similar computer owned or legitimately accessed by the attacker can be used to minimize the risk of detec-

tion. Once perfected, the attack methods can be applied to the target computer.

Finally, to a hostile penetrator the trap door and Trojan horse approaches are probably the most attractive, and these deliberately created flaws in computer programs are the most difficult to detect. Most tiger teams concentrate on accidental flaws that anyone might happen to find, but the deliberate flaws are dormant until activated by an attacker. These errors can be placed virtually anywhere and are carefully designed to escape detection. Yet most military systems include programs not developed in a secure environment, and some are even developed abroad. In fact some systems can be subverted by an anonymous remote technician with no legitimate role in the system development. These errors can be activated by essentially any external interface—from an unclassified telegram to a unique situation set up for detection by a surveillance system.

On balance, penetrating and patching internal controls is not a promising security technique. Even without the prospect of trap doors and Trojan horses and without military security demands, "private companies have attempted to patch holes in so-called [secure] computer systems, and after millions of dollars and years of effort, they gave up in failure."[14] This approach is little more than a game of wits in which the designer must try to find (and patch) *all* the holes while the enemy need find (and exploit) but one remaining hole—a rather unbalanced contest.

The "bottom line" is simple. The commander responsible for security in a computer system needs an unequivocal answer to one crucial question: Is security dependent on internal controls? That is, is there any failure or subversion of the computer itself that

could degrade security? If so, with contemporary computers he has a root inconsistency in the laxity about computer security within the military environment that normally has strict controls on dissemination of sensitive information.

Computer Security Alternatives

We have seen that in contemporary computers the internal controls are not only ineffective but also defy assessment. Yet obviously we can choose to follow the path of the German and Japanese cryptographic experience—underestimating enemy exploitation of the technical weaknesses. This is the chance we have taken in each of several Air Force decisions to operate contemporary computers in a multilevel mode.

If we lose this gamble, the damage depends on what the computer is protecting. It can range from violation of personal privacy to fraud, battlefield damage, or pre-emptive surprise attack. For example, it has been proposed that the Air Force dynamically retarget its strategic ballistic missiles; this supports the national policy of flexible response and would allow application of retaliatory weapons to the most lucrative military targets. However, computers are at the heart of this capability; if they were penetrated, an enemy could retarget the missiles to impact on low-value or even friendly targets as part of a surprise attack!

We will not attempt to explore the numerous possible scenarios from dependence on weak techniques, but we will look at solution alternatives. Both technical and policy issues are involved. Basically, the Air Force has two alternatives other than to ignore

the problem: either limit computer use or use available adequate technology to make the internal controls reliable.

avoid dependence on internal controls

The obvious alternative is to deliberately restrict computer use to a dedicated mode so that the internal controls cannot affect security. There are three common ways to avoid dependence on internal controls.

First, a separate computer can be dedicated to each level of classified information. This is particularly attractive for an on-line or real-time system where the information must be immediately accessible. This approach can lead to duplicate or inefficiently used computers.

Second, each level of classified information can be scheduled to use the computer for a different time period. This requires purging of information from all the system memory at the end of a scheduled period. This usually cumbersome manual procedure lacks responsiveness and wastes computer resources while the change in classification level is completed.

Third, various classification levels can be processed together. All communication lines must be protected, and all the users would need to be authorized access to all the information. Since the internal controls are not dependable, all output from the system is tentatively classified at the highest level. For information with a lower classification, a competent authority must manually review the output for contamination and downgrade it before releasing it at the lower level.

These use restrictions can support good security, but they result in a substantial degradation of capability in a modern computer.

Added expense. These security restrictions significantly add to the cost. Additional communication security measures are needed, and additional manpower is required for the manual review of output. There is also the cost of security clearance investigations for the users whose information the computer may contaminate with information of a higher classification. Other costs include those for duplicate equipment and for additional capacity to compensate for wasted resources. For example, when one major computer system failed to deliver the promised multilevel security, major Air Force sites had to clear many users and make multimillion dollar purchases of additional equipment.

Increased risk. In practice the dedicated mode leads to a major increase in the exposure of information. The lack of internal controls effectively destroys the compartmentalization intended to limit the damage from subversion. The greater number of people requiring clearance increases the chance of granting access to an untrustworthy individual. Manual purge procedures are prone to errors that leave classified memory residues which can be extracted by unauthorized users. Furthermore, the manual review of large volumes of computer output may in fact be a bureaucratic ruse to transfer security responsibility (liability) from designers to users; the reviewer has little chance of detecting unauthorized classified information that has been accidentally or deliberately included in the output.

Foregone capabilities. Such security restrictions can seriously limit the operational capability of battlefield support systems. Modern weapons demand command and control systems with

rapid access to a large base of current and accurate information. This (necessarily shared and integrated) data base will typically contain information ranging from unclassified through top secret. Since many people who maintain the less classified information have limited clearances, and the volume of information requires that computers be used, we have the classical multilevel computer security problem. Internal computer controls are crucial to information protection, and avoiding dependence on the internal controls will seriously limit system capabilities.

The problem is exacerbated by interoperability with its interconnected network of computers with a large, diverse, and geographically dispersed user community. Command and control system computer networks are a prime example. Yet one military official observed that because of poor internal computer security in one such network, its 35 large-scale, general purpose computers would never truly be used for the purpose for which they were procured. The problem is even further intensified by the growing need for fusion of selected intelligence information (without compromise of sensitive sources) with tactical operations information.

In summary, the dedicated mode avoids many computer security problems but fails to meet the operational needs of a modern military force. These needs can only be met by effective multilevel protection in the computer itself.

apply adequate technology

Developing and applying reliable internal computer security are neither easy nor impossible. Although the need for multilevel operation is frequently recognized, the military has given only limited attention to developing the required technology. In fact, the

Air Force recently directed termination of its multilevel security development program, the largest in the Department of Defense.[15]

Before we examine the technological progress that has been made, it should be instructive to identify some of the reasoning that surfaced in the recent Air Force termination. The pattern of thought reflects that computer security is not currently a major focus.

• The prospect of industry's solving the computer security problem is overestimated by concluding that industry has the same security problem as the military. However, the communications analogy indicates a difficulty. In the civilian sector, communication security violations are subject to legislation, not prevention; wiretapping is outlawed, and there is legal redress for loss. In contrast, the military must resort to prevention (e.g., military approved cryptography), since we cannot sue the KGB! The computer situation is similar; there are legislative thrusts but limited commercial success toward demonstrably effective internal controls. The wait for spontaneous industry solutions is likely to be a long one, and it is unlikely that they will ever meet military security standards in areas such as protection from deliberate subversion.

• Inadequate research and development (R&D) funding was allocated to continue one element of the program at an optimal level. Yet portions of the program with funds available were also terminated. Eight million dollars of work was successfully completed. About $10 million of work over four years remained to complete development of a full prototype and the associated general basis for competitive procurement. Several estimates indicate that development costs could be recouped by avoiding the penalties of dedicated mode—not to mention the increased security and operational capability.

• The threat is minimized by seeking counterintelligence that is practically unavailable, e.g., actual examples of enemy agents caught in the act. The enemy may appear too ignorant for penetration, not interested in military secrets, or incapable of planned subversion and exploitation. A single number quantification of the probability of threat can implicitly assume a random incident rather than a planned penetration activity. This may indicate acceptable risk without an objective criterion of acceptability. These perceptions are generally not based on professional intelligence methods with "worked examples" (e.g., from communication security) of the methodology.

• Interest in developing solutions is limited by a lack of clear responsibility for the effectiveness of internal controls. Staff and policy offices can provide recommendations, guidance, and even approvals for computer security mechanisms without responsibility (liability) for any security compromise that might result. On the other hand, the security test and evaluation efforts and cost-effectiveness assessments of individual commanders are largely unrelated to the system's real protection. This is in marked contrast to military communication security where technical experts are responsible for certifying the security mechanisms.

• The computer security problem is difficult to recognize when policy does not clearly distinguish the cases where the computer simply provides computation and where the computer provides internal protection. Such policy focuses development on security controls that are "not necessarily certifiably perfect"—a rather ambiguous goal. In such a policy framework requirements analysis will not identify the need for internal controls. In fact, a computer may well satisfy all regulations and still be highly vulnerable.

• Confidence in weak controls grows from the assumption that expending resources on security will substantially improve security. In fact, the effort may be simply ineffective, as in the case of the penetrate and patch treadmill. Current policy enumerates computer design characteristics for internal security that are neither necessary nor sufficient for security.

• Attention to security gimmicks results in overlooking serious weaknesses. There are many mechanisms of minimal effectiveness in improving internal security controls—handprint analyzers, encryption of internal data, read-only memory for security information, etc. Some guidance has encouraged computer programs that sort out and label products by security level. Evaluation of these programs focuses on expected results with friendly users rather than on deliberate subversion of the programs or penetration of the underlying system. Pursuing such scattered efforts is frequently worse than doing nothing at all, since it gives a dangerous false sense of security.

These sorts of issues caused the Air Force to characterize its Electronic Systems Division's (recently terminated) development program as "controversial." But our previous examination of the problem makes it clear that multilevel operation without adequate technology is a high stakes gamble. Most charitably, it is strangely inconsistent with established standards in other areas (e.g., communications) of military security that hypothesize a deliberate, competent, and motivated hostile threat and respond with effective countermeasures. More likely it nullifies all other security measures, allowing damage limited only by the imagination of the enemy.

Security Kernel Technology

Fortunately, military R&D—in particular the recently terminated Air Force program,[16]—has made substantial progress toward adequate technology for multilevel security. A major step toward solution was the introduction in 1972 of the security kernel[17] technology, which provided a scientific foundation for demonstrably effective internal security controls. Although an explanation of the technical details is well beyond the scope of this article, one technical report summarizes the kernel approach this way:

> The approach to obtaining a secure system involves first defining the security requirements and then creating a conceptual design that can be shown to provide the required protection (i.e., a model). The model formally defines an ideal system (in our case one that complies with military security requirements), and provides a basis for testing a subsequent implementation. Once a [security kernel] that meets the requirements previously described has been implemented, computer security has been achieved. Of the software in the system, only the security kernel . . . need be correct. . . . The operating system proper and/or the application software can contain inadvertently introduced bugs or maliciously planted trap doors without compromising security.[18]

Under the Air Force program the security kernel demonstrated its technical feasibility, independent of any particular computer vendor or security policy. The kernel has also largely established its operational acceptability, with specific evidence for broad functionality, good efficiency, security certifiability, and supportability. In addition, the underlying technical requirements of the kernel have been successfully incorporated into military procurement specifications for both a commercial large-scale computer and an

embedded weapon system computer. In short, the basic technology is well in hand.

scientific foundation

A security kernel is a small set of computer program instructions and associated hardware that controls all access by users (viz., through their programs) to information. A given security kernel is usually unique to a particular computer. A security kernel for computers is in many ways conceptually analogous to a cryptographic device for communications.

Security kernel design is derived directly from a precise specification (viz., a mathematical model) of its function. (The kernel model is analogous to the algorithm that defines the mathematical function of a cryptographic device.) This mathematical model is a precise formulation of access rules based on user attributes (clearance, need to know) and information attributes (classification). System parameters control an installation's specific use (e.g., for the DOD classification policy, privacy protection, etc.).

The chief distinguishing characteristic (from whence its name) of the security kernel concept is that a kernel represents a distinct internal security perimeter. In particular, that portion of the system responsible for maintaining internal security is reduced from essentially the entire computer to principally the kernel. Thus the kernel is analogous to a cryptographic device that removes most of a communication path from security consideration. To be a bit more technical and concrete, a typical security kernel has several (say ten to twenty) small computer programs (viz., subroutines) that can be invoked by other programs (e.g., the operating system and individual user application programs). The kernel, and only

the kernel, controls and manages all the hardware components that store and access information. All other (viz., nonkernel) programs must invoke the kernel (i.e., call on its subroutines) in order to access information—the kernel checks the user and information attributes and provides only access that is authorized. Yet, in spite of these checks, there is minimal user impact. Figure 1 conceptually illustrates this structure.

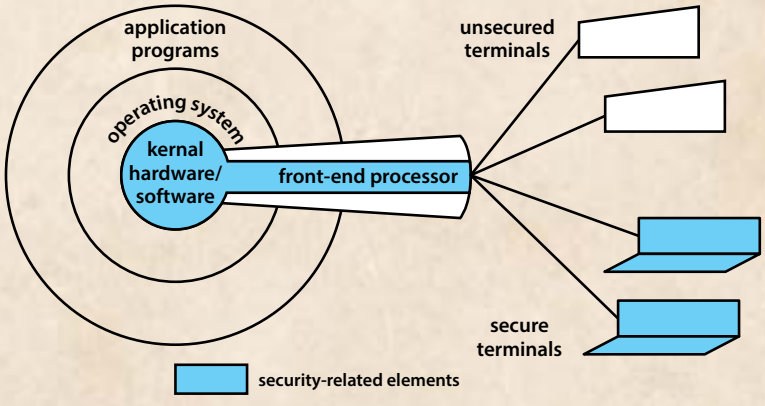


Figure 1. Secure computer system

The technical breakthrough was the discovery of a set of model functions and conditions that are provably sufficient to prevent compromise for all possible nonkernel computer programs. Each function of the model determines the design for a kernel program. In addition, the model imposes security conditions that must be met by the design. Security theorems have been proved showing that (since the kernel precisely follows the model) the kernel will not permit a compromise, regardless of what program uses it or how it is used. That is, the kernel design is penetration-proof—in

particular to all those clever attacks that the kernel designers never contemplated.

This foundation of mathematical completeness raises the kernel design and evaluation process above a mere game of wits with an attacker; this is analogous to information theory as a foundation for modern cryptanalysis. A dramatic effect is that the kernel facilitates objective evaluation of internal security. The evaluator need not examine the nearly endless number of possible penetration attempts; he need only verify that the mathematical model is correctly implemented by the kernel. In other words, the kernel provides the verifiably reliable internal controls needed for multilevel security.

engineering feasibility

To be useful the kernel concept must be not only mathematically sound but also feasible to implement. Successful implementation is based on three engineering principles:

Completeness. A security kernel must be invoked on every access to data in the computer.

Isolation. A security kernel and its data base must be protected from unauthorized modification.

Verifiability. A security kernel must be sufficiently small and simple that its function can be completely tested and verified.

A laboratory security kernel for a commercial minicomputer (Digital Equipment Corporation model PDP-11/45) showed feasibility in 1974. The "virtual memory" hardware of this computer was a significant aid in ensuring the completeness and isolation of

the kernel. This running kernel consisted of only about 1000 computer instructions. The experiment also established that it is much easier to introduce the kernel concept into an initial design than it is to retrofit it later.

The basis for the design (viz., kernel model) was mathematically verified. As with cryptographic devices, verification of the corresponding implementation was based more on careful engineering and extensive testing than on formal mathematics. Automated testing and program verification techniques indicated that the kernel implementation corresponded to the design. This laboratory prototype confirmed feasibility but was not oriented toward performance and efficiency evaluation. In passing, it is interesting to note that a tiger team tried and failed to penetrate its security.

performance

Performance was examined on a larger computer system. Negligible performance degradation (less than 1 percent) was experienced when the commercial Multics (for the Honeywell 6000 line) was modified to the kernel model. This Multics version was not implemented as a true kernel, i.e., the controls were distributed rather than collected into a small, verifiable entity; however, this version made all the security checks required in a kernel and thus confirmed that the kernel was not inherently inefficient.

The good security features of the kernel hardware were a major aid to performance, and these features are vendor-independent. The version was so successful that Honeywell included the resulting Access Isolation Mechanism in commercial Multics offerings for protection of privacy and business information. This system was used as the foundation for the terminated Air Force prototype;

the prototype development was implementing a true, verifiable kernel.

functionality

A security kernel forces the computer user to be security-conscious but does not seriously degrade the capabilities of the computer. This was clearly demonstrated when the Multics modifications were successfully installed for those demanding users in the Pentagon: the constraints of the kernel design had minimal adverse impact on the users. Just as cryptography allows the secure use of standard commercial communication equipment, the kernel concept allows the secure use of standard commercial computer equipment and programs. The Pentagon facility with its classified processing confirmed the concepts for supporting a kernel-based computer in a total system security context.

Operational utility of the kernel was further demonstrated with the initial minicomputer prototype. A demonstration showed the secure interface of operations and intelligence systems for fusion of tactical battlefield information. In addition, several military R&D efforts in various stages of completion have used major elements of the security kernel technology: a command and control network, a cryptographic controller, a nation-wide digital communication system, a large-scale "virtual machine monitor" system, a general-purpose minicomputer operating system, and a secure militarized minicomputer (based on the commercial Honeywell Level 6). Although they confirm the utility of the security kernel, none of these R&D efforts will lead to availability and operational use on a general basis.

security policy

Although the security kernel concept is not at odds with current policy, future policy must recognize and take advantage of kernel characteristics. Policy should recognize that the mathematical model provides a way to translate paper and pencil security rules into computer terms. In addition, a meaningful policy for multilevel mode would reflect the technological realities: either the entire system must be correct (not currently feasible) or else the security kernel must be used.

As with cryptographic devices, the kernel must be protected against subversion (e.g., insertion of a trap door) during its development. But protecting the kernel certainly involves far fewer people and a much more controlled environment than trying to protect all the computer programs of the system; thus, in contrast to contemporary systems, the kernel makes it tractable to protect against subversion. Furthermore, the evaluation (for certification) of internal computer security controls is a difficult technical task. The kernel approach to design and implementation makes such certification feasible, but this evaluation still requires highly capable technical experts—just as does the evaluation of cryptographic devices.

This approach conceptually parallels modern military cryptography. (See Table II.) Yet, development must be resumed and policy adjustments made if it is to be available on a general basis at any time in the immediate future. To be sure, there are competing demands for resources. Development of directly employable weapons (such as fighters) may always have higher priority than development of computer security, but as one observer put it: "How effective would those fighters be if plans for their employment

were known in advance by an adversary who had penetrated the computer containing those plans?"[19] The security kernel is clearly the only currently available technology that can provide the security and operational capabilities we must have.

Table II. Commonality in security technology

	Cryptographic Mechanism	Security Kernel
threats negated..... rather than outlawed	wiretapping	penetration
standard commercial..... elements preserved	communications circuits	computers and programs
security sensitive..... portions limited	principally the crypto	principally the kernel
underlying basis..... precisely formulated	cryptographic algorithm	mathematical model
design evaluation..... criteria definitized	information theory	security theorems
implementation exactly..... meeting design	methodical engineering	verified programs
subversion controlled..... by physical security	manufacturing	programming
skilled experts needed..... for certification	cryptanalysts and engineers	computer scientists

Security often requires subjective judgments, and some may differ with the author on specific points. On balance it appears evident that a user who puts blind trust in the protection provided by computers for sensitive military information will seriously endanger security. In fact, most computers do not even include nom-

inal features to support a military security system. Even when they do, the essence of the computer security problem is the technical efficacy of internal controls, and the evidence is clear that most internal controls are not dependable.

On the other hand, limiting computer use in order to avoid this problem is expensive and deprives us of vital operational capability. The effectiveness versus efficiency dilemma generates pressure for underestimating the threat and overconfidence in internal security controls. Unfortunately, these pressures have led the Air Force into a disturbing and increasing dependency on weak security controls even in the absence of evidence of effectiveness.

The Air Force recently terminated the single major DOD program for providing practical and scientifically sound internal controls—controls based on the security kernel concept. Past development has clearly demonstrated the feasibility, performance, and utility of this technology. However, because of lack of both a technical understanding and a meaningful policy, there is currently little official support for development of this promising capability.

Three basic actions must be taken to control the adverse impact of our computer security weakness:

- Promulgate a clear policy that distinguishes between dependence on external controls (dedicated mode) and internal controls (multilevel mode). It should not be possible to satisfy the policy without genuinely providing security. Multilevel mode without a technically sound basis should be expressly prohibited.

- Incorporate explicit military security controls in classified processing systems. These must be based on a precise specification of the required functions (as in the kernel model for the Pentagon

Multics). This step is crucial to future introduction of multilevel security without complete system redesign. (In the interim this can also aid in the protection of privacy and valuable resources.)

• Resume security kernel development to provide technically sound multilevel security. As in the previous Air Force program, this should be oriented toward the competitive military acquisition process. Concurrently, policy must be changed to facilitate operational use of the kernel technology.

It is not easy to make a computer system secure, but neither is it impossible. The greatest error is to ignore the problem—a fatal mistake which obviously allows available solutions to remain unused. Failure in this one critical area introduces an Achilles' heel into our battlefield support systems—the cornerstone of the modern electronic Air Force.

Naval Postgraduate School
Monterey, California

Notes

1. Malcolm R. Currie, "Electronics: Key Military 'Force Multiplier,' " *Air Force Magazine*, July 1976, p. 44.
2. Edgar Ulsamer, "How ESD Is Building USAF's Electronic Eyes and Ears," *Air Force Magazine*, July 1977, p. 40.
3. Importance of electronics to the Air Force is indicated in "The Electronic Air Force," *Air Force Magazine*, July 1977, p. 29, which notes that this is the magazine's seventh annual issue devoted primarily to this "fundamental Air Force concern."
4. F. W. Winterbotham, *The Ultra Secret* (New York: Harper and Row, 1974), p. 11.
5. Ibid., p. 15.
6. Ibid., p. 107.
7. Ibid., p. 191.
8. David Kahn, *The Codebreakers* (New York: Macmillan Co., 1967), p. 67.
9. Winterbotham, p. 85.
10. Kahn, p. 591.
11. Ibid., p. 392.
12. Thomas Whiteside, "Dead Souls in the Computer," *The New Yorker*, August 29, 1977, pp. 59–62.

13. Tom Alexander, "Waiting for the Great Computer Rip-off," *Fortune*, July 1974, p. 143.

14. Bonnie Ginzburg, "Military Computers Easily Penetrable, AF Study Finds," *Washington Post*, August 8, 1976, p. A6.

15. In August 1976 Air Force Systems Command directed termination of the Electronic Systems Division's ADP System Security Program. Termination was completed by September 1977, halting development (that was proceeding well) of a secure general-purpose prototype to fully demonstrate operational acceptability and the associated development of specifications, policy recommendations, and evaluation criteria for general use.

16. Lawrence Curran, "Air Force 'Kernel' Attains Computer Security Using Existing Technology," *Electronics*, September 30, 1976, pp. 59, 61.

17. The author initially hypothesized the security kernel concept and its mathematical basis. Subsequent sponsored research at the MITRE Corporation completed the detailed formulation, as described in *ESD 1976 Computer Security Developments Summary*, MCI-76—2, Electronics Systems Division, Hanscom AFB, Massachusetts, January 1977.

18. W. L. Schiller, *The Design and Specification of a Security Kernel for the PDP-11/45*, ESD—TR-75-69 (Bedford, Massachusetts: MITRE Corporation, May 1975), p. 9.

19. "Computer Security: A Case of Priorities," *Electronics*, September 30, 1976, p. 10.

Technological progress has merely provided us with more efficient means for going backwards.

Aldous Huxley

Lieutenant Colonel Roger R. Schell (Ph.D., Massachusetts Institute of Technology) is a USAF/USN Exchange Officer assigned as an Assistant Professor of Computer Science at the Naval Postgraduate School, Monterey, California. Most of his service has been in weapon systems development and acquisitions. He served as an engineer and computer software manager, and for several years he was program manager for the ADP System Security Program at Hanscom AFB, Massachusetts. He is a graduate of Air Command and Staff College and Air War College.

US Defense Politics: The Origins of Security Policy by Harvey M. Sapolsky, Eugene Gholz, and Caitlin Talmadge. Routledge (http://www.routledge.com), 270 Madison Avenue, New York, New York 10016, 2009, 191 pages, $178.00 (hardcover), ISBN 978-0-415-77265-5; 2009, 191 pages, $44.95 (softcover), ISBN 978-0-415-77266-2.

In *US Defense Politics*, Prof. Harvey Sapolsky of MIT, Prof. Eugene Gholz of the LBJ School of Public Affairs at the University of Texas–Austin, and PhD candidate Caitlin Talmadge of MIT provide a detailed look into politics affecting our national defense. The authors offer a brief history lesson on the military before addressing four questions characteristic of US policy making: "(1) What shall be the division between public and private responsibilities in each particular policy area? (2) What shall be the division between planning and the market? (3) What is to be centralized and what is to be decentralized in each policy area? (4) And what questions should be settled by experts, on technocratic grounds, and what should be settled by political means, representing the will of the people?" (p. 8).

Sapolsky, Gholz, and Talmadge express a need for blending private and public responsibilities in a manner that benefits both the government and its citizens. For example, though specifically designed for the military, the Global Positioning System has proven even more useful to civilians. The authors argue that more such mutually beneficial acquisitions would ease any political turmoil with regard to the necessary research and development.

As for planning and the market, *US Defense Politics* examines a free-market approach to US defense, pointing out, for instance, objections raised by the other military services to the Air Force's desire to control the development of remotely piloted aircraft (RPA). The authors indicate that such a stranglehold on the RPA market adversely affects the mission due to a lack of competition. Instead, "[RPA] development across multiple services would be more conducive to innovation and would create a more diverse set of capabilities for the future" (p. 160).

Addressing the question of centralization and decentralization within the defense structure, the authors note that in times of conflict, centralization is paramount, insofar as two power pyramids exist: the military, acting as an adviser, and civilians, implementing policy. Having each power in a defined role allows top leadership to effectively carry out the mission of defending our nation. Decentralization, however, "encourages the development and presentation of new ideas, but it does not encourage the implementation of any" (p. 163). Ultimately, after the military branches compete with each other, civilian leadership considers their ideas and then decides which path to choose, thus reaffirming the need for centralization: "What is unproductive is to divide the DOD up into civilian versus military camps, between an administration-dominated corps on the one hand and the permanent bureaucracy on the other" (p. 164).

Lastly, the book points out that determining whether to have experts or politicians settle certain questions actually involves a balance of power. For example, whereas defense experts argue the need for sturdier tanks, faster aircraft, or larger ships, politicians realize that other initiatives, such as providing medical service for military family members, would have a more productive effect on the overall capability of national defense. Consequently, in this instance, authorizing less expensive fifth-generation tanks, aircraft, or ships allows for a stronger all-volunteer force.

Emphasizing the importance of maintaining harmony between the civilian and military arenas as a factor in defense politics, the authors single out Robert McNamara as one of the worst secretaries of defense in history. One need only examine statements by the former secretary to discover a lack of this desired cohesiveness: "I see my position here as being that of a leader, not a judge. I am here to originate and stimulate new ideas and programs, not just to referee arguments and harmonize interests" (p. 100).

Regrettably, the book does have its flaws. Take, for example, the section on President George W. Bush, the Iraq war, and weapons of mass

destruction (WMD): "No WMD were found, not even a warehouse or two full of chemical shells, which nearly every intelligence around the world had believed existed" (p. 143). Since this book is about defense politics, the authors should have examined more carefully the background of intelligence reports. Even though intelligence agencies continuously reported the lack of evidence necessary to provide legal grounds for an invasion of Iraq, politicians in Washington pressured the analysts into producing vague reports that one could read either way. After all, in some cases, such as this one, politicians interpret intelligence reports as they see fit and then create policies.

All things considered, *US Defense Politics* is relevant and worthwhile for the Air Force community. Specifically, I recommend it to all senior noncommissioned officers and junior officers as well as to other service members who desire a fundamental understanding of how politics affects the military. The fact that each of the 12 chapters includes questions for discussion and recommendations for additional reading makes it a valuable tool for mentors who are developing the leaders of tomorrow.

SSgt Justin N. Theriot, USAF
Incirlik AB, Turkey

Structured Analytic Techniques for Intelligence Analysis by Richards J. Heuer Jr. and Randolph H. Pherson. CQ Press (http://www.cqpress.com), 2300 N Street, NW, Suite 800, Washington, DC 20037, 2010, 343 pages, $52.95 (softcover), ISBN 978-1-60871-018-8.

Richards J. Heuer Jr. and Randolph H. Pherson have produced a "how-to" guide for your brain. Having previously written about the mental pitfalls encountered during intelligence analysis, they have done the community a great service by providing a guidebook on how to mitigate such faulty intellectual thinking. (The intelligence community recognizes Heuer in particular as an expert in metacognition, or "thinking about thinking.") An essential element to any analyst's tool

kit, this study should prove valuable to people involved in the decision-making process.

Structured Analytic Techniques for Intelligence Analysis is not a textbook on intelligence, the analytical process, or obstacles to effective, unbiased thinking. Furthermore, although Heuer and Pherson do walk the reader through the eight phases of analytical thought, it is not a checklist that one must follow rigidly from start to finish. Rather, this book serves as a guide through the process, providing analysts a number of different options they can employ at their discretion to improve their end product. For each phase of the analytical process, analysts will find a number of valuable techniques that will allow them to conduct multiple approaches to each problem set, either individually or with the assistance of other analysts.

The book emphasizes analytical thought, which the authors proclaim central to good analysis. Heuer and Pherson argue that analysts should encourage the effective usage of these techniques by integrating them into daily thinking, allowing analysts to become familiar with ways of applying them. Additionally, the book examines the manner in which structured analysis can best support the distributed nature of the intelligence community, which relies on the collaboration of analysis from disparate organizations—geographically separated and dependent upon a shared understanding of the thinking process employed. Structured analysis not only overcomes an analyst's obstacles to clear thought but also offers a transparent format to explain the thought process to others.

Heuer and Pherson supply 50 different techniques for structured analysis but do not suggest using all of them in every effort. Instead, analysts should choose the most appropriate one for the given situation, taking care not to limit themselves to one or two "go-to" techniques. The authors warn that analysts should not become too comfortable with any selection of techniques, recommending that they continuously push the boundaries of their cognitive processes to avoid mental shortcuts that might lead to false assumptions and flawed

thinking. However, they do recommend a handful of "core techniques" with which analysts should become familiar due to their frequency of use and applicability to a wide range of intelligence problem sets. These procedures equip novices with a good starting point from which they can then begin to integrate other techniques. The more varied the techniques employed, the higher the thought processes attained. Although the authors organize the techniques into eight phases of analysis, a number of them overlap these categories because of their effectiveness in multiple functions.

Heuer and Pherson carefully explain their methodology for choosing techniques, highlighting their criteria for selecting each one and always maintaining that no single technique is necessarily better than another. Analysts should use each one to tackle a particular problem set. The authors also include 12 questions to help analysts decide upon the most appropriate technique(s) for their project.

Recognizing that all analysis should be subject to review, Heuer and Pherson submit their own thesis—the value of structured analytic technique—for critique as well. In chapter 13, they lay out the different ways (though never promoting one technique specifically) by which one can judge the improved effectiveness produced by their recommendations. They also propose that the intelligence community as a whole establish a formal process for evaluating such techniques to ensure that the community continues to grow and refine its thinking processes rather than rely on any one source, including this book.

The study's format makes the book quite easy to use. A flowchart on the back cover walks the analyst through the eight phases of problem solving and lists likely techniques for use. The aforementioned 12 questions also help analysts seek out the best ones for employment. For each of the 50 techniques, the authors include a brief summary, an explanation of how to use it to best effect, its value, and methods for applying it, as well as examples of the technique in use and an explanation of how each one relates to the others and their original sources. In this fashion, analysts can carefully make their choice, based on the problem

at hand, or if they are already familiar with the techniques, they can simply skip to the most appropriate one and review its methodology.

Structured Analytic Techniques for Intelligence Analysis would prove most suitable as an in-class reference for a course on intelligence analysis or as an excellent resource for individuals who have completed such a class. Granted, an analyst could learn these techniques by reading the book, but they are best incorporated through hands-on training. Although intelligence analysts will benefit most from this work, anyone involved in the decision-making process—especially those who must leverage intelligence to execute their operations—will find it of incredible utility.

Lt Col Stephen C. Price, USAF
Stuttgart, Germany

Teaching Strategy: Challenge and Response edited by Gabriel Marcella. Strategic Studies Institute (http://www.strategicstudiesinstitute.army.mil/), US Army War College, 632 Wright Avenue, Carlisle, Pennsylvania 17013-5244, 2010, 354 pages, ISBN 978-1-58487-430-0. Available free at http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB976.pdf.

Teaching Strategy: Challenge and Response is itself a response to the debate about the teaching of strategy, addressing the topic from different angles, especially as it applies to professional military education. The book contains 11 chapters by authors well qualified to write about teaching strategy. In the introduction, Robert H. Dorff notes that the collection of essays continues discourse of the past five years about how to improve education in strategy at military academic institutions. He also points out that the war in Iraq, in which execution left something to be desired, reflected some shortcomings in strategy. Dorff concludes by mentioning the existence of several signs of an inability to create good strategy but does not pursue the origins of this problem.

Although the book is a product of the defense establishment, the contributors do not hesitate to air out their concerns about weaknesses in strategy education and discuss how the general population and academia misunderstand strategy. Thus, this collection would appeal not only to members of both the armed forces and the professional education system but also to politicians and the general public. Several chapters offer commentary on strategic thinking that would interest anyone involved in national security or military matters: Robert Kennedy, "The Elements of Strategic Thinking: A Practical Guide"; Thomaz Guedes da Costa, "The Teaching of Strategy: Lykke's Balance, Schelling's Exploitation, and a Community of Practice in Strategic Thinking"; Volker Franke, "Making Sense of Chaos: Teaching Strategy Using Case Studies"; and Christopher R. Paparone, "Beyond Ends-Based Rationality: A Quad-Conceptual View of Strategic Reasoning for Professional Military Education." These contributions distinguish themselves by turning their full attention to the subject at hand rather than dwelling on tangential matters such as internal issues in the professional military education system, as do some of the other contributions. All of the essays, however, raise our understanding of strategy by defining it and exemplifying how it plays a role in different political, military, and geopolitical settings. Several authors address the inability of the modern state to formulate, explain, and execute strategy.

Bradford A. Lee's chapter, "Teaching Strategy: A Scenic View from Newport" (pp. 105–48), an examination of several interesting balancing acts, deserves special mention. Lee questions whether the teaching of classical strategy, such as that associated with the Peloponnesian War and the Athenian expedition to Sicily, allows today's officers to apply this ancient wisdom to modern warfare. Do officers need more exposure to what Germans call *Bildung*, the intellectual self-cultivation of civic values and the riches of our civilization? Does this intellectual enhancement make battlefield commanders better able to save American lives, protect freedom, and end a conflict? Or is this classical education and theorizing strategy just mind noise? Like other contributors, Lee seems slightly pessimistic about the political ability to formulate a

clear and concise strategy to win a war or a conflict. In the absence of a national grand strategy, how can we expect service leaders to produce a successful military strategy? Lee also discusses practical questions such as ways of attracting and retaining suitable faculty members.

In chapter eight, "The Teaching of Strategy," mentioned above, Thomaz Guedes da Costa writes about the strategist as a synthesizer instead of an analyst, a planner, and a manager. His discussion of exploiting the situation (pp. 219–22), an especially important contribution to the volume, draws on the work of B. H. Liddell Hart, Edward Luttwak, and Thomas Schelling by pointing out the value of utilizing strategic thinking as a tool set and providing guidance to exploit an opportunity as a means of ensuring the best possible outcome.

The contributors to *Teaching Strategy* not only have much to say about strategy to the Air Force community or anyone interested in the topic, but also identify a wealth of excellent sources for future reference in the endnotes to their essays. In short, the book is well worth reading.

Jan Kallberg, PhD
Richardson, Texas

Guiding Principles for Stabilization and Reconstruction by the United States Institute of Peace and the United States Army Peacekeeping and Stability Operations Institute. United States Institute of Peace Press (http://www.usip.org/publications-tools), 1200 17th Street NW, Washington, DC 20036-3011, 2009, 244 pages, $16.00 (softcover), ISBN 978-1-60127-033-7.

A particular genre of military guides related to low intensity conflict, stabilization, reconstruction, and counterinsurgency operations has become extremely popular in the media and military circles recently due to the wars in Iraq and Afghanistan. Various authors, commentators, academics, and strategists have discussed the changing, volatile nature of the world and the possibility of further and future conflict. The book *Guiding Principles for Stabilization and Reconstruction* describes the set-

ting: "As global trends indicate, instability is likely to pose greater, and perhaps more numerous, challenges in the years to come" (p. 1-2). The United States Institute of Peace, in coordination with the United States Army Peacekeeping and Stability Operations Institute, brings its extensive experience to bear in developing a manual that offers a framework for managing effective stabilization and reconstruction operations.

Beth Cole, of the United States Institute of Peace, who served as project director and one of the book's two lead writers, is dean of institutional affairs at the United States Institute of Peace Academy for International Conflict Management and Peacebuilding. Prior to her employment at the institute, she worked at the State Department and with George Mason University's Program on Peacekeeping Policy.

The manual seeks to develop strategic-level guidelines for US civilian government employees, in particular those who may deploy in support of establishing and meeting short-term objectives during stability and reconstruction operations. The principles combine best practices from government and nongovernmental organizations (NGO) and the fruits of a thorough literature review of various military, academic, and private-sector publications. Given the absence of a stability and recovery operations manual—in part because of religious, ethnic, political, and cultural factors, as well as a myriad of others—*Guiding Principles* makes a valiant effort, in a scant 244 pages, to supply the first strategic-level guidelines for complex stability and reconstruction operations. For this accomplishment alone, Beth Cole and the entire staff deserve the gratitude and attention of students, scholars, and experts in security studies and humanitarian operations.

The guide is organized into easy-to-understand sections, including scope, purpose, principles, fundamentals, and various topical areas (safe and secure environment, rule of law, stable governance, sustainable economy, and social well-being). Additionally, the volume offers several well-sourced appendices. A number of "cross-cutting principles" that can apply to all the various topical areas (called "end states" in the text) include host nation ownership and capacity, political primacy, le-

gitimacy, unity of effort, security, conflict transformation, and regional engagement (p. 2-9). As the book makes apparent, stability and reconstruction operations are not rooted solely in military operations. Rather, operations require intergovernmental coordination that, according to the text, has been lacking, causing people to ask, "What are we trying to achieve?" (p. 1-3). Overall, *Guiding Principles* blends each of the various topical areas into a central thesis in an attempt to answer the previous question as well as "How can we do it?"

Though designed as a guide for civilians who plan for and respond to stability and reconstruction operations, the book does not include a historical overview of civilian leadership and resources during such operations, which would have proved helpful. Moreover, several guidelines seem little more than commonsense anecdotal statements—for example, "act only with an understanding of the local context" (p. 6-39) and "anticipate obstructionists and understand their motivations" (p. 6-43). Additionally, the sole mention of intelligence occurs in the vague statement that "intelligence is not a formal or acknowledged part of S&R [stability and reconstruction] missions. Doctrinal guidance and cooperation on this function is sorely needed to ensure that critical information is collected and appropriately shared" (p. 6-60). In a strategic-level guide to operations, this brief mention of intelligence is disappointing and naive. Although the text seems to narrowly define intelligence only as military intelligence in a security environment, it has typically been defined more broadly because planners and specialists need to know information regarding logistics, supplies, transportation routes, locations, political leaders, and facilities.

Readers find curiously little mention of successful operations in the Balkans, Iraq, or Afghanistan and only a limited number of successful case studies that include examples of provincial reconstruction teams (PRT) or the State Department's Civilian Response Corps. However, the appendices offer guidelines and lessons learned for PRTs and other stability operations. The book remains an excellent strategic overview of resources, anecdotes, and basic guidelines, but it lacks the tactical

"on the ground" focus needed for NGOs or civilians entering conflict zones who are preparing to assist in a plethora of operations ranging from rebuilding educational institutions to developing and improving fragile economies.

Planning specialists, academics, and practitioners will find the guidelines useful. However, experienced military and diplomatic personnel may consider the work filled with too many commonsense anecdotes. *Guiding Principles* would serve as a good desk reference for civilians deploying to conflict zones or members of military planning staffs. Furthermore, professors might recommend it as an excellent handbook for a graduate-level course on security studies or peacekeeping. The book fulfills its purpose of "provid[ing] a foundation for decision makers, planners, and practitioners—both international and host nation—to construct priorities for specific missions" (p. 1-3). I intend to keep *Guiding Principles* on my shelf and will continue to read and review it during America's next ventures into stability and reconstruction operations across the globe.

Bradley Martin
McDonough, Georgia

I Could Never Be So Lucky Again: An Autobiography by General James H. "Jimmy" Doolittle with Carroll V. Glines. Schiffer Publishing (http://www.schifferbooks.com/newschiffer/search_results.php), 4880 Lower Valley Road, Atglen, Pennsylvania 19310, 1994, 622 pages, $29.99 (hardcover), ISBN 9780887407376.

In his autobiography, Gen James H. "Jimmy" Doolittle reflects on his more than 90 years of living on this earth, proposing that "I Could Never Be So Lucky Again." For a man who gained recognition as one of the early pioneers of American aviation, led the famous raid on Tokyo in 1942, received the Medal of Honor, commanded the mighty Eighth Air Force at the most critical time of the European air campaign during World War II, succeeded as a business executive, and witnessed the

twentieth century's full range of progress, his choice of a title for his book conveys the man's genuine humility, notwithstanding his tremendous accomplishments. Ultimately the formula works well, and Doolittle's account of his life is worthy of any professional's bookshelf for its history, relevance, and personal message. For someone who believes that "if a man leaves the earth a better place than he found it, then his life has been worthwhile" (p. 539), his autobiography represents a fitting coda to his life and achievements.

At more than 530 pages of narrative, Doolittle's autobiography is a bit long, but because he uses simple language to relate his accounts in a storytelling style and paces all of the vignettes effectively, the text reads quickly and easily. Even in his advanced years, Doolittle's recollection remains sharp and detailed—in some cases, perhaps too much so. Historians and aficionados of World War II airpower may appreciate the detail, but others may not. For example, the intricate, technical discussion of the development of flight instrumentation in the late 1920s is somewhat distracting, albeit historically significant. In this particular case, however, Doolittle regains the human element by interjecting aspects of his family life. In fact, he employs the common literary device of discussing family and correspondence throughout the book to reinforce the very personal nature of his undertaking.

The fact that many lessons drawn from Doolittle's experiences remain applicable today makes his story keenly relevant. Some people tend either to forget or not realize that the interwar years—and certainly World War II—witnessed some of the most rapid development of technology in history. Doolittle played a key role in these events, recognizing then, as we do now, the importance of skill, discipline, technical knowledge, and the constant drive to continuously test the limits of performance, design, and speed. His advocacy of high-octane fuel when conventional wisdom labeled it "Doolittle's Folly" (p. 191) illustrates his accurate foresight of the convergence of several technological trends. At a more strategic level, his entire experience in the European theater during the war, first as commander of Twelfth Air Force and

then of Eighth Air Force, provides an excellent examination of the pitfalls, friction, and politics of joint and coalition operations, as well as the burdens of expectation assumed by commanders. Doolittle notes difficulties with the media and prejudices emanating from regular officers (something familiar to him since he served as a reservist). Throughout the book, he also espouses the importance of the people around him, especially those under his command. For example, he characterizes decorations as "such a small payment, for such a large service" (p. 365). Today's professionals can use these and several other vignettes as touchstones relevant to current issues.

One's initial impression from the title of the book, given Doolittle's well-known raid on Tokyo in the spring of 1942, is that it refers to his success in bombing Tokyo and producing a great psychological and strategic victory for America six months after Pearl Harbor. Taken as a whole, however, the book's coverage of Doolittle's life demonstrates his penchant for preparedness, ingenuity, courage, and resolve. At nearly every turn and in nearly every vignette, the narrative resonates with a common theme of "good fortune perched on the cowl" (p. 77). In light of the sheer volume of Doolittle's extraordinary exploits, the reader could easily interpret this statement as an instance of false modesty but for the fact that his self-effacing character, humility, goodwill, and gratitude course throughout the book, in reference not only to his professional successes and calculated risk taking but also to his personal life.

Appropriately, one has the sense that this story is in fact a very personal work. Doolittle shares his recollection of successes, blunders, and (what he considered at the time) abject failures. His reflection on how he felt after his crash landing in China following the Tokyo raid—his sincere belief that he had utterly failed and that his aviation career was over—is strikingly telling in this regard, given the historical significance and success of the raid. His candor and humility are a refreshing shift from much of the biographical material available on famous personages—warriors, especially—which tends to parlay no shortage of bravado and self-aggrandizement. By contrast, in August 1945 when

Doolittle commanded Eighth Air Force, he learns of the imminent Japanese surrender and receives word from higher command authorities that "if [he] wanted the 8th Air Force bombers to be in combat with the Japanese, [he] had better get an operation going" (p. 454). Doolittle declined, not willing to risk his crews or cause additional casualties and damage just so the Eighth could boast that it had bombed both Berlin and Tokyo. Additionally, some of his first and final thoughts express his devotion to Joe, his beloved wife and friend for over 70 years. Their affection for each other and their family through all of the tremendous upheavals of the interwar years and the war itself would inspire any military couple or family. Indeed, in this regard one might even interpret the subtext of the narrative as a love story.

In sum, Doolittle's autobiography is very enjoyable and a highly recommended candidate for one's personal or professional library. It strikes the reader as a very high horsepower, candid, and detailed historical account of the origins of American airpower and the life of one of America's greatest Airmen. We come to know this Airman, engineer, daredevil pilot, business leader, Medal of Honor recipient, general, and (most importantly, as the subtext reveals) loving husband and father. The main thread of the narrative, of course, recounts Doolittle's experiences as a military aviator. However, taken in total, his life remains relevant to issues facing twenty-first-century professionals. Regardless of the reader's profession, *I Could Never Be So Lucky Again* offers valuable insights from a man who actively participated in the birth of airpower, served as a critical leader in the conflagration of World War II, lived through the beginning and end of the Cold War, and witnessed the advent of modern air and space power in Operation Desert Storm. Doolittle led a unique, exciting, and successful life, owing to his tremendous inquisitiveness, humility, ingenuity, confidence, courage, and resolve. One could argue it was not he, but we, who were lucky.

Col Darren Buck, USAFR
Tyndall AFB, Florida

India, Pakistan, and the Bomb: Debating Nuclear Stability in South Asia by Šumit Ganguly and S. Paul Kapur. Columbia University Press (http://cup.columbia.edu/), 61 West 62nd Street, New York, New York 10023, 2010, 152 pages, $21.50 (hardcover), ISBN 978-0-231-14374-5; $14.50 (softcover), ISBN 978-0-231-14375-2.

Part of a 10-volume series entitled Contemporary Asia in the World published by Columbia University Press, *India, Pakistan, and the Bomb: Debating Nuclear Stability in South Asia* provides a comprehensive look at the nuclear programs of India and Pakistan and examines whether these programs stabilize or destabilize the region. The book's most interesting feature is that the authors actively debate this particular effect of nuclear weapons, especially with regard to the relationship between India and Pakistan. Both Ganguly and Kapur have published other works on these two countries and have knowledge of and experience in writing about the politics of South Asia. Although most other such studies present only one perspective of nuclear stability, these authors take opposite sides of the argument and debate each other throughout the work, thus giving the reader a complete picture and understanding of the possible outcomes of a nuclear South Asia. Whereas Ganguly takes the position that nuclear weapons have had a stabilizing effect on the relationship between India and Pakistan, Kapur maintains that they have destabilized the South Asia security environment writ large and will continue to do so. Both attempt to lay out their positions succinctly and logically. They supply a historical framework for the countries' relationship before nuclear weapons entered the picture, showing how the two nations evolved following British colonialism. Ganguly and Kapur then introduce their competing frameworks, each of which addresses how nuclear weapons have altered India's and Pakistan's dealings with each other. The time periods analyzed by the authors include 1980 to 2002, 2002 to 2007, and 2008 to the present.

On the one hand, Ganguly optimistically asserts that nuclear weapons have produced a stabilizing effect, especially in the sense that

each nation's nuclear deterrence has limited military responses during conflicts. Kapur, on the other hand, argues for strategic pessimism, pointing out that aggressive behavior by a new nuclear power leads to regional destabilization. For him, nuclear weapons in India and Pakistan have had this effect in South Asia because of their potential to escalate any conflict between the two countries.

A short case study on the Kashmir conflict of 1990 helps illustrate each man's position. Ganguly argues that during this incident, even though India and Pakistan increased their military presence around Kashmir, the situation did not escalate because each understood the other's nuclear capabilities and did not wish to risk possible nuclear war. Kapur declares that Pakistan's incursion into Kashmir occurred because nuclear weapons gave it the confidence to challenge the status quo in Kashmir more aggressively, thereby destabilizing the region. Such instability was inevitable because Pakistan believed that its nuclear deterrence would keep India from elevating the Kashmir incursions to an all-out military conflict, allowing Pakistan to assume a more aggressive military posture vis-à-vis India. This case study is just one of the many examples offered by the authors to illustrate their position on how nuclear weapons have affected the relationship between India and Pakistan.

Anyone interested in the politics and nuclear stability of India and Pakistan will find this short work easy to understand and read. Its inclusion of a brief historical background helps the authors clarify their arguments and supplies a context for understanding the complex relationship between the two nations. Because *India, Pakistan, and the Bomb* has far-reaching applications, any military member deploying to US Central Command would benefit from the larger lessons that accrue from an understanding of the India/Pakistan relationship—such as the implications of an Iranian nuclear program. As someone who followed Ganguly's line of thinking prior to reading this book, I must

say that it led me to reconsider my beliefs about the effect of nuclear weapons on South Asia.

Maj Joseph M. Ladymon, USAF
Nellis AFB, Nevada

Such Men As These: The Story of the Navy Pilots Who Flew the Deadly Skies over Korea by David Sears. Da Capo Press (Perseus Books Group) (http://www.perseusbooksgroup.com/dacapo/home.jsp), 387 Park Avenue South, 12th Floor, New York, New York 10016, 2010, 432 pages, $25.00 (hardcover), ISBN 9780306818516; 2011, $18.00 (softcover), ISBN 9780306820106.

Carrier aviation played an important role in the Korean air war, adding more weight to the American air effort as well as offering a number of other advantages. It filled in for range-limited Air Force aircraft, especially early in the war when South Korean airfields were unsuitable for Air Force jets. Moreover, throughout the conflict, carrier aviation furnished support against targets in northeastern Korea. Navy and Marine Airmen provided close air support superior to that of the Air Force in terms of accuracy, rapidity of response, loiter time, and proximity to friendly forces—and with fewer incidents of friendly fire. However, the Air Force flew 2.5 times as many combat sorties as did the carrier aviators, fighting and winning the most celebrated and best remembered aspect of the Korean air war—the battle for air superiority. These factors, coupled with the newly formed Air Force's push for its place in the military establishment, have resulted in the junior service's dominating the literature of the Korean air war.

David Sears's *Such Men As These* will help correct this imbalance. He has quite a story to tell. The aviators flew off World War II carriers and employed mainly propeller-powered aircraft of that same vintage in the fight. The jets flew one-third, the stalwart World War II–era F4U two-fifths, and the World War II–designed AD one-quarter of the carrier combat sorties. They operated in a tough climate, over rugged terrain,

and against considerable ground fire. Further, the pilots reaped little glory, for unlike the situation in World War II, Korea offered no ships of size to engage and few aerial victories. (Navy aviators claimed 13 enemy aircraft destroyed for five Navy and Marine aircraft lost in air-to-air combat.) Carrier aviators logged about the same number of sorties as in World War II although they dropped three-quarters more bombs.

The book tells the story of life on the carriers and the air battle as seen by Navy aviators. (Marine carrier Airmen are not included.) The author uses an anecdotal approach, writing of the Airmen's background, exploits, and postwar experiences. He seeks "to tell human stories against the backdrop of history" (p. 349), and he does so quite well. The narrative includes not only the constant struggle but also the exciting moments—combat, death and damage, and accidents (some fatal, some not). Sears makes clear that the carrier air war in Korea was a factory-like process, day in and day out, unlike the peak-and-valley tempo of World War II operations. He is candid and not always complimentary. Along the way, he describes James Michener's service as a war correspondent and the genesis of his classic book *The Bridges at Toko-ri*, the semifictional account of this action, including the models for Michener's fictional characters in the novel. (The title of Sears's book is a paraphrase from Michener's.) Sears includes fighter pilots as well as attack and helicopter crews (those who made it back safely as well as those who did not) in all elements of the story—on shore; preflight; during launch, attack, recovery, and rescue; and postwar. The author does an excellent job of showing the flavor of the carrier air war from the individual's viewpoint.

Readers seeking more will be disappointed. Although Sears covers the entire war in adequate (perhaps too much) detail, he devotes little attention to the aircraft or tactics employed and includes no analysis or general wrap-up. Written for a popular audience, the book in general is an easy read, but it provides few footnotes (and lacks citations even for direct quotations.) Some readers may find some of the vignettes drawn out, such as the Medal of Honor story regarding Tom Hudner

(who attempts to rescue Jesse Brown, the first African-American naval aviator) and another aviator's extended experience as a prisoner of war.

I highly recommend *Such Men As These* for readers interested in the human side of the carrier air war in Korea. (For balance, I suggest that they also read *The Naval Air War in Korea*, Richard Hallion's more traditional and analytical version of the subject.) David Sears has produced an impressive book that adds to our knowledge of the air war in Korea. It shows American Airmen at their best in the neglected story of naval aviation during that frustrating and difficult conflict.

Kenneth P. Werrell
Christiansburg, Virginia