

SSQ

STRATEGIC STUDIES QUARTERLY

SPRING 2014

VOL. 8, NO. 1

Commentary

China's Military Modernization and Cyber Activities:
Testimony of Dr. Larry M. Wortzel before the House
Armed Services Committee

Larry M. Wortzel

Why Cyber War Will Not and Should Not Have Its Grand Strategist

Martin C. Libicki

War on Our Doorstep: Not a Mere Crime Problem

James P. Farwell

Darby Arakelian

Toward Attaining Cyber Dominance

Martin R. Stytz

Sheila B. Banks

China: An Unlikely Economic Hegemon

Maj Heather Fox, USAF

Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework

Col Eric F. Mejia, USAF

Book Essay

Airpower Writings of John Andreas Olsen

Phillip S. Meilinger

SSQ STRATEGIC STUDIES QUARTERLY

SPRING 2014

AU Press



Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 2014		2. REPORT TYPE		3. DATES COVERED 00-00-2014 to 00-00-2014	
4. TITLE AND SUBTITLE Strategic Studies Quarterly. Volume 8, Number 1. Spring 2014				5a. CONTRACT NUMBER	
				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), Strategic Studies Quarterly (SSQ), 155 N. Twining St., Bldg 693, Maxwell AFB, AL, 36112-6026				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 Same as Report (SAR)	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Chief of Staff, US Air Force

Gen Mark A. Welsh III

Commander, Air Education and Training Command

Gen Robin Rand

Commander and President, Air University

Lt Gen David S. Fadok

Director, Air Force Research Institute

Allen G. Peck, Director and Publisher

Editorial Staff

Col W. Michael Guillot, USAF, Retired, *Editor*

CAPT Jerry L. Gantt, USNR, Retired, *Content Editor*

Nedra O. Looney, *Prepress Production Manager*

Tammi K. Dacus, *Editorial Assistant*

Daniel M. Armstrong, *Illustrator*

Advisors

Gen Michael P. C. Carns, USAF, Retired

Allen G. Peck, Director and Publisher

Christina Goulter, PhD

Colin S. Gray, DPhil

Robert P. Haffa, PhD

Charlotte Ku, PhD

Benjamin S. Lambeth, PhD

John T. LaSaine, PhD

Allan R. Millett, PhD

Rayford Vaughn, PhD

Contributing Editors

Air Force Research Institute

Anthony C. Gould, PhD

School of Advanced Air and Space Studies

Stephen D. Chiabotti, PhD

James W. Forsyth Jr., PhD

The Spaatz Center

Edwina S. Campbell, PhD

Charles E. Costanzo, PhD

Christopher M. Hemmer, PhD

Kimberly A. Hudson, PhD

Nori Katagiri, PhD

Zachary J. Zwald, PhD

Strategic Studies Quarterly (SSQ) (ISSN 1936-1815) is published quarterly by Air University Press, Maxwell AFB, AL. Articles in SSQ may be reproduced, in whole or part without permission. A standard source credit line is required for each reprint.

STRATEGIC STUDIES QUARTERLY

*An Air Force–Sponsored Strategic Forum on
National and International Security*

VOLUME 8

SPRING 2014

NUMBER 1

Commentary

- China's Military Modernization and Cyber Activities:
Testimony of Dr. Larry M. Wortzel before the House Armed
Services Committee* 3
Larry M. Wortzel

Feature Article

- Why Cyber War Will Not and Should Not Have
Its Grand Strategist* 23
Martin C. Libicki

Perspectives

- War on Our Doorstep: Not a Mere Crime Problem* 40
James P. Farwell
Darby Arakelian
- Toward Attaining Cyber Dominance* 55
Martin R. Stytz
Sheila B. Banks
- China: An Unlikely Economic Hegemon* 88
Maj Heather Fox, USAF
- Act and Actor Attribution in Cyberspace: A Proposed
Analytic Framework* 114
Col Eric F. Mejia, USAF

Book Essay

Airpower Writings of John Andreas Olsen 133
Phillip S. Meilinger

Book Reviews

*Conflict and Cooperation in the Global Commons:
A Comprehensive Approach for International Security*..... 148
Edited by: Scott Jasper
Reviewed by: Lt Col Mark Peters, USAF

*The Generals: American Military Command
from World War II to Today*..... 149
By: Thomas E. Ricks
Reviewed by: W. Michael Guillot

*International Law, International Relations, and
Global Governance* 151
By: Charlotte Ku
Reviewed by: 1st Lt Joshua D. Bower, USAF

Disclaimer
The views and opinions expressed or implied in SSQ are those of the authors and are not
officially sanctioned by any agency or department of the US government. We encourage you to
send comments to: strategicstudiesquarterly@us.af.mil.

China's Military Modernization and Cyber Activities

Testimony of Dr. Larry M. Wortzel before the House Armed Services Committee

As a member of the US-China Economic and Security Review Commission, I will present some of the commission's findings on China's military modernization, US-China security relations, and China's cyber activities from the *2013 Annual Report to Congress*.¹ The views I present today, however, are my own. I want to acknowledge the fine work of our staff in preparing the annual report and especially the excellent research of our foreign policy and security staff in helping to prepare this testimony.

China's Military Modernization

China's military, the People's Liberation Army (PLA), is undergoing an extensive modernization program that presents significant challenges to US security interests in Asia. This modernization includes creating a surveillance and strike architecture that supports operations at longer distances away from China's coast. It makes the PLA a more formidable force in all the dimensions of war: air, space, land, sea, and in the electromagnetic spectrum. The PLA has new, multimission-capable combat ships, aircraft, submarines, and new generations of missiles.

First and foremost, major elements of this program—such as the DF-21D antiship ballistic missile and increasing numbers of advanced submarines armed with antiship cruise missiles—are designed to restrict US freedom of action throughout the Western Pacific. The PLA is rapidly expanding and diversifying its ability to conduct conventional strikes against US and allied bases, ships, and aircraft throughout the region, including those that it previously could not reach with conventional weapons, such as US military facilities on Guam. As the PLA's anti-access/area-denial capabilities mature, the costs and risks to the United States for intervention in a potential regional conflict involving China will increase.² The Chinese military, of course, sensitive to nineteenth and twentieth century history, thinks of these actions as counterintervention strategies designed to prevent foreign militaries from intervening in China's sovereign affairs or territory.

Furthermore, the PLA's rapidly advancing regional power projection capabilities enhance Beijing's ability to use force against Taiwan, Japan, and rival claimants in the South China Sea. More seriously, because China's military doctrine emphasizes preemptive attacks, it raises the stakes in any crisis. Many potential security scenarios could require the US military to defend US regional allies and partners as well as maintain open and secure access to the air and maritime commons in the Western Pacific.

At the same time, rising unease over both China's expanding capabilities and increasing assertiveness is driving US allies and partners in Asia to improve their own military forces and strengthen their security relationships with each other. These trends could support US interests in Asia by lightening Washington's operational responsibilities in the region. On the other hand, if China's neighbors pursue military capabilities that could be used offensively or preemptively due to the perception that the United States will be unable to follow through on its commitment to the rebalance to Asia, this could undermine US interests in the region.

In the commission's 2013 annual report we discuss the following main developments in China's military modernization:

Navy

Aircraft Carriers. Since commissioning its first aircraft carrier, the *Liaoning*, in September 2012, China continues to develop a fixed-wing carrier aviation capability, which is necessary for the carrier to carry out air defense and offensive strike missions. The *Liaoning* is a former Russian aircraft carrier purchased from the Ukraine. It was refitted and modernized in China. The PLA Navy conducted its first successful carrier-based takeoff and landing with the Jian-15 (J-15) in November 2012, certified its first group of aircraft carrier pilots and landing signal officers on the carrier's first operational deployment from June to July 2013, and verified the flight deck operations process in September 2013.³ The *Liaoning* will continue to conduct short deployments and shipboard aviation training until 2015 to 2016, when China's first J-15 regiment is expected to become operational. The J-15 is a Chinese copy of the Russian Su-33. China likely intends to follow the *Liaoning* with at least two domestically produced hulls. The first of these appears to be under construction and could become operational before 2020.

Submarine-Launched Ballistic Missiles. China's Julang-2 (JL-2) submarine-launched ballistic missile is expected to reach initial operational capability very soon.⁴ The missile has been under development for a number of years, which shows that Chinese military industries still have some problems in developing and fielding new systems. The JL-2,

when mated with the PLA Navy's Jin-class nuclear ballistic missile submarine (SSBN), will give China its first credible sea-based nuclear deterrent. The Jin SSBN/JL-2 weapon system will have a range of approximately 4,000 nautical miles, allowing the PLA Navy to target the continental United States from China's littoral waters.⁵ China has deployed three Jin SSBNs and probably will field two additional units by 2020.⁶

Sea-Based Land Attack Capability. China currently does not have the ability to strike land targets with sea-based cruise missiles. However, the PLA Navy is developing a land attack capability, likely for its Type-095 guided-missile attack submarine and Luyang III guided-missile destroyer. Modern submarines and surface combatants armed with land attack cruise missiles (LACM) will complement the PLA's growing inventory of air- and ground-based LACMs and ballistic missiles, enhancing Beijing's flexibility for attacking land targets throughout the Western Pacific, including US facilities in Guam.⁷

Shipbuilding. The PLA Navy continues to steadily increase its inventory of modern submarines and surface combatants. China is known to be building seven classes of ships simultaneously but may be constructing additional classes.⁸ Trends in China's defense spending, research and development, and shipbuilding suggest the PLA Navy will continue to modernize. By 2020, China could have approximately 60 submarines that are able to employ submarine-launched intercontinental ballistic missiles, torpedoes, mines, or antiship cruise missiles. China's surface combat force also has modernized and expanded with approximately 75 surface combatants that are able to conduct multiple missions or that have been extensively upgraded since 1992.⁹ The combat fleets are supported by a combat logistics force that can conduct underway replenishment and limited repairs. All of these ships will be equipped to take advantage of a networked, redundant command, control, communications, computer, intelligence, surveillance, and reconnaissance system (C4ISR) fielded by the PLA.

Attack Submarines. China has a formidable force of 63 diesel-electric and nuclear attack submarines.¹⁰ They are equipped with nuclear and conventional torpedoes and mines as well as antiship cruise missiles.¹¹ In 2012, China began building four "improved variants" of its *Shang*-class nuclear attack submarine. China also continues production of the *Yuan*-class diesel-electric submarine—some of which will include an air-independent propulsion system that allows for extended duration operations—and the *Jin*-class SSBN. Furthermore, China is developing two new classes of nuclear submarines and may jointly design and build four advanced diesel-electric submarines with Russia.¹² China's growing

submarine inventory will significantly enhance China's ability to strike opposing surface ships throughout the Western Pacific and to protect future nuclear deterrent patrols and aircraft carrier task groups.¹³

Air Force

Fighter Aircraft. China also is developing two next-generation fighters, the J-20 and the J-31, which could feature low observability and active electronically scanned array radar.¹⁴ The PLA Air Force conducted the first test flights of the J-20 and J-31 in January 2011 and October 2012, respectively.¹⁵ These aircraft will strengthen China's ability to project power and gain and maintain air superiority in a regional conflict.

Cargo Transport Aircraft. In January 2013, China conducted the first test flight of its indigenously developed cargo transport aircraft, the Yun-20 (Y-20). China previously was unable to build heavy transport aircraft, so it has relied on a small number of Russian Ilyushin-76 (IL-76) aircraft for strategic airlift since the 1990s. Aircraft specifications provided by official Chinese media indicate the Y-20 can carry about twice the cargo load of the IL-76 and about three times the cargo load of the US C-130.¹⁶ The Y-20 will enhance the PLA's ability to respond to internal security crises and border contingencies, support military international peacekeeping and humanitarian assistance operations, and project power in a regional conflict.¹⁷ The larger aircraft and expanded fleet will enhance the PLA's capability to employ the 15th Airborne Army, part of the PLA Air Force.

LACM-Capable Bomber Aircraft. In June 2013, the PLA Air Force began to receive new Hongzha-6K (H-6K) bomber aircraft. The H-6K, an improved variant of the H-6 (originally adapted from a late-1950s Soviet design), has extended range of around 2,400 to 3,100 miles and can carry China's new long-range LACM, the CJ-10. The CJ-10 has a range of around 900 to 1,200 miles.¹⁸ The bomber/LACM weapon system provides the PLA Air Force with the ability to conduct conventional strikes against regional targets throughout the Western Pacific, including US facilities in Guam.¹⁹ Although the H-6K airframe could be modified to carry a nuclear-tipped air-launched LACM, and China's LACMs likely have the ability to carry a nuclear warhead, there is no evidence to confirm China is deploying nuclear warheads on any of its air-launched LACMs.²⁰ The H-6K also may be able to carry supersonic antiship cruise missiles.²¹

Space and Counterspace

In May 2013, China fired a rocket into nearly geosynchronous Earth orbit, marking the highest known suborbital launch since the US Gravity Probe A in 1976 and China's highest known suborbital launch to date. Although Beijing claims the launch was part of a high-altitude scientific experiment, available data suggest China was testing the launch vehicle component of a new high-altitude antisatellite (ASAT) capability.²² If true, such a test would signal China's intent to develop an ASAT capability to target satellites in an altitude range that includes the US global positioning system (GPS) and many US military and intelligence satellites. In a potential conflict, this capability could allow China to threaten the US military's ability to detect foreign missiles and provide secure communications, navigation, and precision missile guidance.

Furthermore, in September 2013, China launched a satellite into space from the Jiuquan Satellite Launch Center in western China. Our annual report cites commentary from Gregory Kulacki of the Union of Concerned Scientists, who believes that this launch may represent a capacity to launch new satellites in the event China suffers losses in space from space combat.²³

China also has improved its ballistic missile defense capabilities by fielding the Russian-made SA-20B surface-to-air missile (SAM) system. In some cases, China's domestically produced CSA-9 SAM system should also be capable of intercepting ballistic missiles.²⁴

On 27 December 2012, China announced its Beidou regional satellite navigation system is fully operational and available for commercial use. Using 16 satellites and a network of ground stations, Beidou provides subscribers in Asia with 24-hour precision navigation and timing services.²⁵ China plans to expand Beidou into a global satellite navigation system by 2020.²⁶ Beidou is a critical part of China's stated goal to prepare for fighting wars under "informationized conditions," which includes a heavy emphasis on developing the PLA's C4ISR and electronic warfare capabilities. The PLA is integrating Beidou into its systems to improve its command and control and long-range precision strike capabilities and reduce the PLA's reliance on foreign precision navigation and timing services such as GPS.²⁷

Strategic Intercontinental Ballistic Missiles

China is enhancing its nuclear deterrent capability by modernizing its nuclear force. It is taking measures such as developing a new road-mobile intercontinental ballistic missile (ICBM), the DF-41. This missile

could be equipped with a multiple independently targetable reentry vehicle (MIRV), allowing it to carry as many as 10 nuclear warheads.²⁸ In addition to MIRVs, China could also equip its ballistic missiles with penetration aids and may be developing the capability to transport ICBMs by train.²⁹ Furthermore, according to the DoD's 2011 report to Congress on China's military, the PLA "has developed and utilized [underground facilities] since deploying its oldest liquid-fueled missile systems and continues to utilize them to protect and conceal their newest and most modern solid-fueled mobile missiles."³⁰

Defense Spending

To support its military modernization, China continued to increase defense spending in 2013. In March, China announced its official defense budget for 2013 rose 10.7 percent in nominal terms to \$117.39 billion, signaling the new leadership's support for the PLA's ongoing modernization efforts. This figure represents 5.3 percent of total government outlays and approximately 1.3 percent of estimated gross domestic product (GDP).³¹ China's official annual defense budget now has increased for 22 consecutive years and more than doubled since 2006. Most Western analysts agree Beijing likely will retain the ability—even with slower growth rates of its GDP and government revenue—to fund its ongoing military modernization.³²

It is difficult to estimate China's actual defense spending due to the uncertainty involved in determining how China's purchasing power parity affects the cost of China's foreign military purchases and domestic goods and services, as well as Beijing's omission of major defense-related expenditures. Some purchases of advanced weapons, research and development programs, domestic security spending, and local government support to the PLA are not included in China's official figures on defense spending. The Institute of International Strategic Studies assesses China's actual defense spending is 40 to 50 percent higher than the official figure.³³ The US Department of Defense estimated China's actual defense spending in 2012 fell between \$135 and \$215 billion, or approximately 20 to 90 percent higher than its announced defense budget.³⁴

US-China Security Relations

US-China military-to-military relations deepened and expanded in 2013 after several years of setbacks. From 2012 to 2013, the number of US-China military-to-military contacts more than doubled from

approximately 20 to 40.³⁵ In particular, contact between the US Navy and the PLA Navy increased significantly during this time frame. Key military-to-military contacts in 2013 included the first port visit by a US Navy ship to China since 2009, the first port visit by a Chinese ship to the United States since 2006, and the second ever US-China counterpiracy exercise. Additionally, China in March 2013 accepted the invitation, first extended by then Secretary of Defense Leon Panetta in September 2012, to participate in the US-led multilateral Rim of the Pacific Exercise near Hawaii in 2014.³⁶

The DoD contends that a strong military-to-military relationship develops familiarity at the operational level. The department argues that this reduces the risk of conflict through accidents and miscalculations, builds lines of communication at the strategic level that could be important during a crisis, contributes to better overall bilateral relations, and creates opportunities to obtain greater contributions from China to international security. US Pacific Command commander ADM Samuel Locklear in July 2013 said, “The progress that we’re making between our two militaries is quite commendable . . . because we are able to have very good dialogue on areas where we converge, and there are a lot of places where we converge as two nations, and we’re also able to directly address in a matter-of-fact way where we diverge.”³⁷

There have been eight rounds of strategic dialogue between China and the United States, currently managed by the Pacific Forum–CSIS. This is a Track 1.5 dialogue that involves some representatives from the US government in attendance, but virtually all Chinese participants are from some part of their government. The past several rounds of the dialogue have dealt with some of the most important strategic issues facing China and the United States, including nuclear strategic stability; the relationship between cyber attacks, space warfare, and nuclear stability; ballistic missile defense; and strategic early warning. Officers from China’s strategic missile forces have been in attendance at the dialogue. I see this as one of the most productive dialogues taking place with China. The PLA is an active participant. Ideally such discussions should be direct, government-to-government talks, but it is encouraging that the PLA and the Chinese Foreign Ministry are engaged on these matters.

In another positive development, in mid-November, the US Army and the PLA ground forces conducted their first ever field exercise together. The exercise was focused on disaster relief and took place in Hawaii.³⁸

My own experience in direct military-to-military contacts with China leads me to advise caution in what we do with the PLA and what we show them. In my opinion, the wise limitations placed by Congress on

military exchanges with China in the National Defense Authorization Act (NDAA) of 2000 should not be lifted. The commission's annual report also reflects this sentiment. Military-to-military contacts with China require careful oversight to ensure that the United States does not improve China's capability against our own forces, Taiwan, or our friends and allies in the Asia-Pacific region.

Enhanced military-to-military contacts between China and the United States in 2013 took place in the context of China's efforts to rebrand the bilateral relationship as a "new type of major-country relationship." This concept, promoted heavily in 2013 by Chinese President Xi Jinping and other high-level Chinese officials, posits the United States and China should, as two major powers, seek to cooperate on a range of bilateral and global issues while avoiding the kind of harmful competition that often characterizes relationships between dominant powers and rising ones.³⁹ Cooperation is a good thing, but US military leaders cannot lose sight of the PLA's record on human rights. This dictates practical limitations on what we do with China's armed forces. The principal mission of China's military is to keep the Chinese Communist Party (CCP) in power, as we saw in the way that the PLA was used during the 4 June 1989 Tiananmen Massacre and in Tibet.

China's Cyber Activities

While China continues to develop its navy, air force, missile forces, and space and counterspace capabilities, in Chinese military writings, cyberspace is an increasingly important component of China's comprehensive national power and a critical element of its strategic competition with the United States.⁴⁰ Beijing seems to recognize that the United States' current advantages in cyberspace are allowing Washington to collect intelligence, exercise command and control of military forces, and support military operations. At the same time, China's leaders fear that the United States may use the open Internet and cyber operations to threaten the CCP's legitimacy.

Since the commission's *2012 Annual Report to Congress*, strong evidence has emerged that the Chinese government is directing and executing a large-scale cyber espionage campaign against the United States. China to date has compromised a range of US networks, including those of DoD and private enterprises. These activities are designed to achieve a number of broad security, political, and economic objectives.

There are no indications the public exposure of Chinese cyber espionage in technical detail throughout 2013 has led China to change its

attitude toward the use of cyber espionage to steal intellectual property and proprietary information. The report by Mandiant, a US private cyber-security firm, about the cyber espionage activities of PLA Unit 61398 merely led the unit to make changes to its cyber “tools and infrastructure” to make future intrusions harder to detect and attribute.⁴¹ There are about 16 technical reconnaissance (signals intelligence) units and bureaus in the PLA and at least seven electronic warfare and electronic countermeasures units.⁴² Each of China’s seven military regions is supported by an electronic countermeasures regiment, and it looks like the PLA Second Artillery Force has its own supporting unit.⁴³ These organizations focus on cyber penetrations, cyber espionage, and electronic warfare.

When confronted with public accusations from the United States about its cyber espionage, Beijing usually attempts to refute evidence by pointing to the anonymity of cyberspace and the lack of verifiable technical forensic data. It also shifts the media focus by portraying itself as the victim of Washington’s cyber activities and calling for greater international cooperation on cyber security.⁴⁴ In a press conference on the day after Mandiant released its report in February 2013, a spokesperson for China’s Ministry of Foreign Affairs said, “Groundless speculation and accusations regarding hacker attacks, for various purposes, is both unprofessional and irresponsible and it is not helpful for solving the problem.” He also emphasized cyber attacks are a serious problem for China.⁴⁵

However, a number of public US government reports, admissions by private companies that they have been the target of cyber espionage, investigations by cyber-security firms, and US press reporting contradict Beijing’s long-standing denials. While attribution is difficult and takes great skill, trend analysis is allowing cyber-security professionals to develop a more comprehensive understanding of Chinese cyber actors, tools, tactics, techniques, and procedures.

Threats to US National Security

China’s cyber espionage against the US government and defense industrial base poses a major threat to US military operations, the security and well-being of US military personnel, the effectiveness of equipment, and readiness. China apparently uses these intrusions to fill gaps in its own research programs, map future targets, gather intelligence on US strategies and plans, enable future military operations, shorten research and development (R&D) timelines for military technologies, and identify vulnerabilities in US systems and develop countermeasures.⁴⁶

Military doctrine in China also calls for attacks on the critical infrastructure of an opponent's homeland in case of conflict. In July 2013, a threat researcher at Trend Micro, a private Japanese cyber-security firm, claimed he had detected a Chinese cyber intrusion, commencing in December 2012, of a honeypot.⁴⁷ He had created the honeypot to resemble the industrial control system of a water plant in the United States. The researcher attributed the intrusion to Unit 61398, based on forensic analysis.⁴⁸ If true, this suggests Unit 61398 is collecting intelligence on critical infrastructure in addition to other targets. Such activities are consistent with PLA doctrine, which explains that one function of wartime computer network operations is to "disrupt and damage the networks of [an adversary's] infrastructure facilities, such as power systems, telecommunications systems, and educational systems."⁴⁹

A number of instances of Chinese cyber espionage targeting US national security programs have been identified in recent years. In May 2013, the *Washington Post* described a classified report by the Defense Science Board, which lists more than 24 US weapon system designs the board determined were accessed by cyber intruders. The *Washington Post* reported, "Senior military and industry officials with knowledge of the breaches said the vast majority were part of a widening Chinese campaign of espionage against U.S. defense contractors and government agencies." The list includes the Patriot missile system, Aegis ballistic missile defense system, the F/A-18 fighter, the V-22 Osprey multirole combat aircraft, and the Littoral Combat Ship.⁵⁰

Information gained from intrusions into the networks of US military contractors likely improves China's insight into US weapon systems, enables China's development of countermeasures, and shortens China's research and development timelines for military technologies.⁵¹ In addition, the same intrusions Chinese cyber actors use for espionage also could be used to prepare for offensive cyber operations. Chinese cyber actors could place latent capabilities in US software code or hardware components that might be employed in a potential conflict between the United States and China.

There has been concern in recent years about security risks to the DoD's supply chain. In a meeting in May 2013, commissioners and DoD officials discussed the department's interpretation of US law regarding procurement sources. DoD officials indicated a stricter procurement evaluation standard that includes sourcing concerns could be applied only to items on the United States Munitions List. Items outside this list are judged by a different standard, which some officials believe might preclude concerns about the origin of products. For

example, items procured for C4ISR maintenance facilities are not subject to stricter scrutiny. Commissioners raised concerns that this interpretation of the law was limiting the department's ability to address potential risks arising from certain procurement sources. Commissioners urged the DoD to expand the purview of the stricter standard to items beyond the munitions list.

The DoD is currently moving in this direction. Section 806 of the NDAA for Fiscal Year 2011 (Public Law 111-383), is intended to address the problem, but it has yet to be fully implemented. Section 806 authorizes the secretary of defense and the secretaries of the Army, Navy, and Air Force to reject procurement sources for information technology on grounds of protecting supply chain security if they receive a recommendation to do so from the DoD.⁵² The department is in the process of implementing Section 806, having conducted tabletop exercises and written the Defense Federal Acquisition Regulation Supplement Rule implementing Section 806. As of May the rule was undergoing inter-agency coordination.⁵³ These changes to DoD procurement ultimately may provide officials with the flexibility they need to protect all DoD systems. However, progress has been slow and the problem the commissioners highlighted will remain until the new policy is implemented, potentially posing a threat to national security. Therefore, in the *2013 Annual Report* the commission recommends Congress urge the administration to expedite progress in its implementation of Section 806 of the NDAA for Fiscal Year 2011.

Developments in cloud computing in China may present cyber-security risks for US users and providers of cloud computing services and may also have implications for US national security. Based on the findings of a report by Defense Group Inc. for the commission, the relationship between the Ministry of State Security (MSS) and the Chongqing Special Cloud Computing Zone represents a potential espionage threat to foreign companies that might use cloud computing services provided from the zone or base operations there.⁵⁴ In addition, the plan to link 21Vianet's data centers in China and Microsoft's data centers in other countries suggests the Chinese government one day may be able to access data centers outside China through Chinese data centers.⁵⁵ With concerns about espionage in mind, in the *2013 Annual Report*, the commission recommends Congress direct the administration to prepare an inventory of existing federal use of cloud computing platforms and services and determine where the data storage and computing services are geographically located. Such inventory should be prepared annually and reported to the appropriate committees of jurisdiction.

Cloud computing also could improve the PLA's C4ISR capabilities. DGI writes that cloud computing "could enable more effective and flexible development and deployment of military equipment, while at the same time improving the survivability of the PLA's information systems by endowing them with greater redundancy (allowing a system's capabilities to survive the disabling or destruction of any individual node)."⁵⁶

Threats to US Industry

China's cyber espionage against US commercial firms poses a significant threat to US business interests and competitiveness in key industries. This cyber espionage complements traditional human espionage. Through these efforts, the PLA and China's defense industries are able to leapfrog ahead in technologies and systems and fill in gaps in their own research and development capabilities at a considerable savings in time and money. Gen Keith Alexander, commander of US Cyber Command, assessed the cost to US companies of intellectual property theft is about \$250 billion a year, although not all the losses are due to Chinese activity.⁵⁷ Chinese entities engaging in cyber and other forms of economic espionage likely conclude that stealing intellectual property and proprietary information is much more cost-effective than investing in lengthy R&D programs.⁵⁸ These thefts support national science and technology development plans that are centrally managed and directed by the PRC government.

The Chinese government, primarily through the PLA and the Ministry of State Security, supports these activities by providing state-owned enterprises information and data extracted through cyber espionage to improve their competitive edge, cut R&D timetables, and reduce costs. The strong correlation between compromised US companies and those industries designated by Beijing as "strategic" industries further indicates a degree of state sponsorship, and likely even support, direction, and execution of Chinese economic espionage.⁵⁹ Such governmental support for Chinese companies enables them to out-compete US companies, which do not have the advantage of leveraging government intelligence data for commercial gain.⁶⁰

It is difficult to quantify the benefits Chinese firms gain from cyber espionage. We do not know everything about the kinds of information that is targeted and taken, nor do we always know which Chinese actor stole the information. Some thefts may take place that are never detected. In terms of business intelligence, some targets of cyber theft likely include information related to negotiations, investments, and corporate strategies including executive e-mails, long-term business plans,

and contracts. In addition to cyber theft, Chinese companies almost certainly are acquiring information through traditional espionage activities, which limits our ability to identify the impact of cyber espionage in particular. Nevertheless, it is clear that China not only is the global leader in using cyber methods to steal intellectual property, but also accounts for the majority of global intellectual property theft.⁶¹ Chinese actors have on several occasions in recent years leveraged cyber activities to gain sensitive or proprietary information from US enterprises:

- In the report by Mandiant mentioned earlier, there is evidence that since 2006 PLA Unit 61398 has penetrated the networks of at least 141 organizations, including companies, international organizations, and foreign governments. These organizations are either located or have headquarters in 15 countries and represent 20 major sectors, from information technology to financial services. Of those organizations penetrated, 81 percent were either located in the United States or had US-based headquarters. According to Mandiant, Unit 61398, gained access to a wide variety of intellectual property and proprietary information through these intrusions.⁶² Unit 61398 is the Second Bureau of the PLA's technical reconnaissance department, based in Shanghai.⁶³
- In another high-profile example of a Chinese company allegedly targeting a US company's intellectual property through cyber espionage, the Department of Justice (DoJ) in June 2013 filed charges against Sinovel Wind Group, a Chinese energy firm, alleging Sinovel stole intellectual property from Massachusetts-based company American Superconductor (AMSC).⁶⁴ Once Sinovel was able to reproduce AMSC's technology after stealing its proprietary source code, the Chinese firm broke the partnership, cancelled existing orders, and devastated AMSC's revenue. AMSC has sought compensation from Sinovel through lawsuits in China, an effort which is ongoing and has resulted in legal fees for AMSC exceeding \$6 million.⁶⁵ While these lawsuits continue to move slowly through the Chinese legal system, adding to AMSC's legal fees, Sinovel is reaping the profits of stolen technology.⁶⁶

Deterring Chinese Cyber Theft

It is clear that attempting to name the perpetrators in China in an attempt to shame the Chinese government is not sufficient to deter Chinese entities from conducting cyber espionage against US companies. Mitigating the problem will require a well-coordinated approach across the US government and with industry. Many potential actions are being discussed by Congress, the Obama administration, and outside experts. These actions include linking economic cyber espionage to trade restrictions, prohibiting Chinese firms using stolen US intellectual property from accessing US banks, and banning US travel for Chinese organizations that are involved with cyber espionage. The US-China Economic and Security Review Commission recommends Congress take the following actions:

- Adopt legislation clarifying the actions companies are permitted to take regarding tracking intellectual property stolen through cyber intrusions.
- Amend the Economic Espionage Act (18 U.S.C. § 1831-1839) to permit a private right of action when trade secrets are stolen.
- Support the administration's efforts to achieve a high standard of protection of intellectual property rights in the Trans-Pacific Partnership and the Transatlantic Trade and Investment Partnership.
- Encourage the administration to partner with other countries to establish an international list of individuals, groups, and organizations engaged in commercial cyber espionage. The administration and partner governments should develop a process for the list's validation, adjudication, and shared access.
- Urge the administration to continue to enhance its sharing of information about cyber threats with the private sector, particularly small- and medium-sized companies.

My personal view is that the president already has the authority to place sanctions on Chinese persons, government industries, and companies through the International Emergency Economic Powers Act.⁶⁷ If the magnitude of the damage to the US economy is as great as that cited by General Alexander, the president should exercise that authority.

Sustaining the US Military's "Rebalance" to Asia

In January 2012, DoD's *Defense Strategic Guidance* declared the US military will "of necessity rebalance toward the Asia Pacific" by emphasizing existing alliances, expanding its networks of cooperation with "emerging" partners, and investing in military capabilities to ensure access to and freedom to maneuver within the region.⁶⁸ US Chief of Naval Operations ADM Jonathan Greenert explained the US Navy's role in the rebalance: "As directed by the 2012 *Defense Strategic Guidance* . . . the [US] Navy formulated and implemented a plan to rebalance our forces, their homeports, our capabilities, and our intellectual capital and partnerships toward the Asia Pacific."⁶⁹ Specifically, the US Navy aims to increase its presence in the Asia Pacific from about 50 ships in 2013 to 60 ships by 2020 and "rebalance homeports to 60 percent" in the region by 2020.⁷⁰

However, the commission's annual report notes that US Defense Secretary Chuck Hagel in July 2013 said Washington would have to choose between a smaller, modern military and a larger, older one if sequester-level funding continues.⁷¹ Admiral Greenert has warned constraints in the current budget environment could delay or prevent the US Navy from achieving its objectives in the rebalance.⁷² There is growing concern in the United States and among US allies and partners that the DoD will be unable to follow through on its commitment to the rebalance due to declining defense budgets and emerging crises elsewhere in the world. This could lead some regional countries to increasingly accommodate China or pursue military capabilities that could be used offensively or preemptively. Either scenario could undermine US interests in the region.

I urge you to keep in mind that by 2020, China could have a navy and air force in Asia that outnumbers and almost matches the technical capability of our own forces. If our military force shrinks because of our own budget problems, we may have 60 percent of our forces in the Asia-Pacific region, but 60 percent of 200 ships is far less than 60 percent of a 300-ship navy. That may not be sufficient to deter China or to reassure our friends and allies in the region.

Larry M. Wortzel, PhD
*US-China Economic and
Security Review Commission*

Dr. Wortzel was appointed a member of the US-China Economic and Security Review Commission in 2001 and served two terms as its chair. He is a retired US Army colonel who spent much of his 32-year military career in the Asia-Pacific region. Colonel Wortzel was assistant Army attaché in China from 1988 to 1990 and Army attaché in China from 1995 to 1997. He is the author of *The Dragon Extends its Reach: Chinese Military Power Goes Global* (Potomac Books, 2013). A graduate of the Armed Forces Staff College and the US Army War College, Wortzel earned his MA and PhD in political science from the University of Hawaii.

Notes

1. The complete report can be found at http://www.uscc.gov/Annual_Reports/2013-annual-report-congress.

2. “Anti-access” (A2) actions are those intended to slow deployment of an adversary’s forces into a theater or cause the forces to operate from distances farther from the conflict than they would otherwise prefer. A2 affects movement into theater. “Area denial” (AD) actions are those intended to impede an adversary’s operations within areas where friendly forces cannot or will not prevent access. AD affects movement within theater. *Air Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges* (Arlington, VA: US Air-Sea Battle Office, May 2013), 2–4.

3. “Chinese Aircraft Carrier Returns to Home Port,” *Renmin Ribao* (People’s Daily), 22 September 2013, <http://english.peopledaily.com.cn/90786/8407244.html>; “China’s Carrier-Borne Jet Pilots Receive Certification,” Xinhua, 4 July 2013, <http://english.peopledaily.com.cn/90786/8310416.html>; “China’s First Aircraft Carrier Leaves Homeport for Sea Trials,” Xinhua, 11 June 2013, http://news.xinhuanet.com/english/china/2013-06/11/c_132447284.htm; “China’s Aircraft Carrier Anchors in Military Port,” Xinhua, 7 February 2013, http://www.china.org.cn/china/NPC_CPPCC_2013/2013-02/27/content_28071340.htm; and “China Now Capable to Deploy Jets on Aircraft Carrier: Navy,” Xinhua, 25 November 2013, OSC ID: CPP20121125968098, <http://www.opensource.gov>.

4. *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2013* (Washington: DoD, 2013), 31.

5. *The People’s Liberation Army Navy: A Modern Navy with Chinese Characteristics* (Suitland, MD: Office of Naval Intelligence [ONI], 2009), 23.

6. *PLA Navy Orders of Battle 2000–2020*, written response to request for information provided to the US-China Economic and Security Review Commission (Suitland: ONI, 24 June 2013); and *Annual Report to Congress*, 10, 31.

7. *Annual Report to Congress*, 6–7; and J. Michael Cole, “China’s Growing Long-Range Strike Capability,” *Diplomat*, 13 August 2012, <http://thediplomat.com/flashpoints-blog/2012/08/13/chinas-growing-long-range-strike-capability/>.

8. Andrew Erickson and Gabe Collins, “China Carrier Demo Module Highlights Surging Navy,” *National Interest*, 6 August 2013, <http://nationalinterest.org/commentary/china-carrier-demo-module-highlights-surging-navy-8842>; *PLA Navy Orders of Battle 2000–2020*; and *Annual Report to Congress*, 5–7.

9. *PLA Navy Orders of Battle 2000–2020*.

10. *Ibid.*

11. On tactical nuclear weapons including torpedoes, mines, antiship cruise missiles, and ADMs/mines, see Robert S. Norris, Andrew S. Burrows, and Richard W. Fieldhouse, *British, French, and Chinese Nuclear Weapons, Nuclear Weapons Databook*, vol. 5 (Boulder, CO: Westview Press, 1994), 359; Gregory B. Owens, “Chinese Tactical Nuclear Weapons” (master’s thesis, Naval Postgraduate School, June 1996), 4; “Global Nuclear Stockpiles, 1945–1997,” *Bulletin of the Atomic Scientists*, November/December 1997, 67; “Estimated Nuclear Stockpiles 1945–1993,” *Bulletin of the Atomic Scientists*, December 1993, 57; and Robert S. Norris,

"Nuclear Arsenals of the United States, Russia, Great Britain, France and China: A Status Report," presentation at the 5th ISODARCO Beijing Seminar on Arms Control, Chengdu, China, November 1996. On torpedoes, see "Archive of Nuclear Data," <http://www.nrdc.org/nuclear/nudb/datab17.asp>; and Ronald O'Rourke, *China Naval Modernization* (Washington: Congressional Research Service [CRS], 5 September 2013), <http://www.fas.org/sgp/crs/row/RL33153.pdf>. According to sinodefense.com, in December 2005 China purchased Type-53-65 torpedoes from Russia and 40 Shkval torpedoes in 1998.

12. "China 'Buys Fighter Jets and Submarines from Russia,'" *BBC News*, 25 March 2013, <http://www.bbc.co.uk/news/world-asia-21930280>; and Robert Foster, "Russia to Sell, Co-Produce Lada-class Submarines to China," *Jane's Defence Weekly*, 20 December 2012, <http://www.janes.com/article/19682/russia-to-sell-co-produce-lada-class-submarines-to-china>.

13. *PLA Navy Orders of Battle 2000–2020*; and *Annual Report to Congress*, 5–7.

14. Roger Cliff, "Chinese Military Aviation Capabilities, Doctrine, and Missions," in *Chinese Aerospace Power: Evolving Maritime Roles*, eds. Andrew S. Erickson and Lyle J. Goldstein (Annapolis, MD: Naval Institute Press, 2011), 252; and Richard Fisher, "Deterring China's Fighter Buildup," *Defense News*, 19 November 2012, <http://www.defensenews.com/article/20121119/DEFFEAT05/311190005/>.

15. *Annual Report to Congress*, 8; and Fisher, "Deterring China's Fighter Buildup."

16. "Summary: PRC Expert Says Yun-20 Transport Makes Strategic Air Force Possible," OSC ID: CPP20130128787028, Open Source Center, 27 January 2013, <http://www.opensource.gov>.

17. "Summary: Guangdong Journal Views Strategic Card of 'Yun-20' Jumbo Air Freighter," OSC ID: CPP20130214695013, 31 January 2013; and Andrew Erikson and Gabe Collins, "The Y-20: China Aviation Milestone Means New Power Projection," *Wall Street Journal: China Real Time Blog*, 28 January 2013, <http://blogs.wsj.com/chinarealtime/2013/01/28/the-y-20-china-aviation-milestone-means-new-power-projection/>.

18. Zachary Keck, "Can China's New Strategic Bomber Reach Hawaii?" *Diplomat*, 13 August 2013, http://thediplomat.com/flashpoints-blog/2013/08/13/can-chinas-new-strategic-bomber-reach-hawaii/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+the-diplomat+%28The+Diplomat+RSS%29; Noam Eshel, "Chinese Air Force Gets More H-6K Strategic Bombers," *Defense Update*, 25 June 2013, http://defense-update.com/20130625_h-6k-bombers-delivered-to-pla-air-force.html; and Chen Boyuan, "H-6K Bombers Delivered to PLA Air Force," *China.org*, 22 June 2013, http://www.china.org.cn/china/2013-06/22/content_29197824.htm.

19. *Annual Report to Congress*, 33, 42, 81.

20. Ian Easton, *The Assassin under the Radar: China's DH-10 Cruise Missile Program* (Arlington, VA: Project 2049 Institute, October 2009), 1–6, http://project2049.net/documents/assassin_under_radar_china_cruise_missile.pdf.

21. Keck, "Can China's New Strategic Bomber Reach Hawaii?"

22. Andrea Shalal-Esa, "RPT-China's Space Activities Raising U.S. Satellite Security Concerns," Reuters, 14 January 2013, <http://www.reuters.com/article/2013/01/14/china-usa-satellites-idUSL2N0AJ10620130114>; "Beijing to Trigger Arms Race by Testing Anti-Satellite Missiles," Central News Agency (Taipei), 13 January 2013, OSC ID: CPP20130115968204; Gregory Kulacki, "Is January Chinese ASAT Testing Month?" *All Things Nuclear, Insights on Science and Security*, 4 January 2013, <http://allthingsnuclear.org/is-january-chinese-asat-testing-month/>; *China: PLA Activities Report 16–31 Oct 2012* (Washington: DoD, 31 October 2012), OSC ID: CPP20121120440020; "China Dismisses Report on Planned Test Launch of Anti-Satellite Missile," Xinhua, 25 October 2012, OSC ID: CPP20121025968325; and Bill Gertz, "China to Shoot at High Frontier," *Washington Free Beacon*, 16 October 2012, <http://freebeacon.com/china-to-shoot-at-high-frontier/>.

23. Gregory Kulacki, "‘Kuaizhou’ Challenges U.S. Perceptions of Chinese Military Space Strategy," *All Things Nuclear, Insights on Science and Security*, 27 September 2013, <http://allthingsnuclear.org/kuaizhou-challenges-u-s-perceptions-of-chinese-military-space-strategy/>.
24. *Annual Report to Congress*, 35–36.
25. "‘Beidou,’ China’s Pride," *Bingqi Zhishi (Ordnance Knowledge)*, 1 August 2012, OSC ID: CPP20121016680010.
26. "China Targeting Navigation System’s Global Coverage by 2020," *Xinhua*, 3 March 2012, http://news.xinhuanet.com/english/sci/2013-03/03/c_132204892.htm.
27. "Navy North Sea Fleet’s New Smart Target Ship Emits Electromagnetic Jamming against Missiles," *PLA Daily*, 4 August 2013, OSC ID: CHO2013080530196614; Yu Hu, "PLA Jinan MR Extends Military Use of the Beidou Satellite Navigation System," *Jinan Qianwei Bao (Jinan Front News)*, 17 January 2012, OSC ID: CPP20130222667020; and Sun Chao, Zhang Jun, and Wang Jun, "PLA Chengdu MR Sichuan Div Uses Satellite Navigation to Standardize Time," *Chengdu Zhanqi Bao (Chengdu Battle Standard News)*, 3 November 2011, OSC ID: CPP20130223667002.
28. Bill Gertz, "China Conducts another Mobile ICBM Test," *Washington Free Beacon*, 14 August 2013, <http://freebeacon.com/china-conducts-another-mobile-icbm-test/>.
29. *Annual Report to Congress*, 30; and Bill Gertz, "Riding the Nuclear Rails," *Washington Free Beacon*, 25 January 2013, <http://freebeacon.com/riding-the-nuclear-rails/>.
30. *Annual Report to Congress*, 36.
31. "Facts Figures: China’s 2013 Draft Budget Report," *Xinhua*, 5 March 2013, OSC ID: CPP20130305968101; "China Boosts Defense Spending as Military Modernizes Arsenal," *Bloomberg*, 5 March 2013, <http://www.bloomberg.com/news/2013-03-05/china-boosts-defense-spending-as-military-modernizes-its-arsenal.html>; Luo Zheng, "Investment in Our National Defense Expenditure Mutually Conforms with National Security and Development Interests—Interview with Sun Huangtian, Deputy Director of PLA General Logistics Department, on 2013 National Defense Budget," *PLA Daily*, 6 March 2013, OSC ID: CPP20130307088001; "China Boosts Defense Spending as Military Modernizes Arsenal," *Bloomberg*, 5 March 2013, <http://www.bloomberg.com/news/2013-03-05/china-boosts-defense-spending-as-military-modernizes-its-arsenal.html>.
32. Adam Liff and Andrew Erickson, "Demystifying China’s Defence Spending: Less Mysterious in the Aggregate," *China Quarterly*, 2013, <http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=8874207>.
33. Institute of International Strategic Studies, "China’s Defence Spending: New Questions," *Strategic Comments*, 2 August 2013, <http://www.iiss.org/en/publications/strategic%20comments/sections/2013-a8b5/china--39-s-defence-spending--new-questions-e625>.
34. *Annual Report to Congress*, 45.
35. *Ibid.*, 69–71. These contacts include high-level visits, recurrent exchanges, academic exchanges, functional exchanges, and joint exercises.
36. Shirley Kan, *U.S.–China Military Contacts: Issues for Congress* (Washington: CRS, 25 July 2013).
37. Karen Parrish, "U.S.–China Military Ties Growing, Pacom Commander Says," US Armed Forces Press Service, 11 July 2013, <http://www.defense.gov/news/newsarticle.aspx?id=120440>.
38. Michelle Tan, "Army Hosts China in First Joint Field Exercise," *Army Times*, 12 November 2013, <http://www.armytimes.com/article/20131112/NEWS/311120006/Army-hosts-China-first-joint-field-exercise>.
39. Caitlin Campbell and Craig Murray, *China Seeks a “New Type of Major-Country Relationship” with the United States* (Washington: U.S.–China Economic and Security Review Commission, 25 June 2013), http://origin.www.uscc.gov/sites/default/files/Research/China%20Seeks%20New%20Type%20of%20Major-Country%20Relationship%20with%20United%20States_Staff%20Research%20Backgrounder.pdf and Michael S. Chase,

“China’s Search for a ‘New Type of Great Power Relationship,’” *Jamestown Foundation China Brief* 12, no. 27 (7 September 2012): 14, http://www.jamestown.org/uploads/media/cb_09_04.pdf.

40. Larry M. Wortzel, *The Dragon Extends its Reach: Chinese Military Power Goes Global* (Washington: Potomac Books, 2013) 17, 40–41, 134, 145–48.

41. Dan Mcwhorter, “APT1 Three Months Later—Significantly Impacted, Though Active & Rebuilding,” *M-union*, 21 May 2013, <https://www.mandiant.com/blog/apt1-months-significantly-impacted-active-rebuilding/>; and Richard Bejtlich (chief security officer at Mandiant), telephone interview with commission staff, 21 August 2013.

42. *Directory of PRC Military Personalities* (Washington: Defense Intelligence Agency, March 2013).

43. Ibid.

44. William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, (London and New York: Routledge, 2013), 226.

45. “2013 Nian 2 Yue 19 Ri Waijiaobu Fayanren Honglei Zhuchi Lixing Jizhehui (Ministry of Foreign Affairs Spokesperson Hong Lei Presides over Regular Press Conference 19 February 2013),” Ministry of Foreign Affairs, Beijing, http://www.fmprc.gov.cn/mfa_chn/fyrbt_602243/t1014798.shtml.

46. U.S.–China Economic and Security Review Commission, *2012 Annual Report to Congress* (Washington: Government Printing Office, November 2012), 166.

47. A honeypot is part of a honeynet, which is a fake or diversionary computer network designed to draw in an adversary to identify the adversary or give the adversary false information. Honeynets can provide intelligence regarding adversaries’ “tools, tactics, and motives.” Honeynet Project, “Short Video Explaining Honeypots,” <http://old.honeynet.org/misc/files/HoneynetWeb.mov>.

48. Tom Simonite, “Chinese Hacking Team Caught Taking over Decoy Water Plant,” *MIT Technology Review*, 2 August 2013, <http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/>.

49. Wortzel, *Dragon Extends its Reach*, 142.

50. Ellen Nakashima, “Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies,” *Washington Post*, 27 May 2013, http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

51. Ibid.

52. National Defense Authorization Act for Fiscal Year 2011 (P. L. 111-383), 111th Cong., 2nd sess., 7 January 2011, <http://www.gpo.gov/fdsys/pkg/PLAW-111publ383/pdf/PLAW-111publ383.pdf>.

53. Special assistant to the DoD chief information officer, Office of the Assistant Secretary of Defense for Legislative Affairs, e-mail interview with commission staff, 28 May 2013.

54. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.–China Economic and Security Review Commission, September 2013), 32–34, http://origin.www.uscc.gov/sites/default/files/Research/Red%20Cloud%20Rising_Cloud%20Computing%20in%20China.pdf.

55. Ibid., 39.

56. Ibid., 38.

57. Josh Rogin, “NSA Chief: Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History,’” *Foreign Policy*, 9 July 2012, http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.

58. Mike McConnell, Michael Chertoff, and William Lynn, “China’s Cyber Thievery is a National Policy—And Must Be Challenged,” *Wall Street Journal*, 27 January 2012, <http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html>.

59. Commission on the Theft of Intellectual Property, *The IP Commission Report* (Washington: National Bureau of Asian Research, May 2013), 12, http://ipcommission.org/report/IP_Commission_Report_052213.pdf; and U.S.–China Economic and Security Review Commission, *2012 Annual Report to Congress*, 156.

60. In the late 1980s and early '90s a debate took place in Congress on whether the US intelligence community (IC) should share information and/or intelligence assets with US companies to provide those companies an advantage against foreign competitors. In 1991, Director of the Central Intelligence Agency Robert Gates, in a speech to the IC, stated clearly that the CIA would limit itself to helping US companies safeguard themselves from foreign intelligence operations. Robert Gates, "The Future of American Intelligence," speech to US intelligence community, Washington, DC, 4 December 1991.

61. Commission on the Theft of American Intellectual Property, *IP Commission Report*, 3, 18.

62. *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, February 2013), 2, 3, 4, 9, 21–23, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

63. *APT1*, 9.

64. "Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets," Department of Justice press release, 27 June 2013, <http://www.justice.gov/opa/pr/2013/June/13-crm-730.html>.

65. Melanie Hart, "Criminal Charges Mark New Phase in Bellwether U.S.–China Intellectual Property Dispute," Center for American Progress, Washington, DC, 27 June 2013, <http://www.americanprogress.org/issues/china/news/2013/06/27/68339/criminal-charges-mark-new-phase-in-bellwether-u-s-china-intellectual-property-dispute/>.

66. Ibid.

67. 50 U.S.C. § 1701, <http://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter35&edition=prelim>.

68. *Sustaining U.S. Global Leadership: Priorities for 21st Century Leadership* (Washington: DoD, January 2012), http://www.defense.gov/news/Defense_Strategic_Guidance.pdf.

69. Jonathan Greenert, "Foreword," in *U.S. Navy Program Guide 2013* (Washington: DoD, 2013), <http://www.navy.mil/navydata/policy/seapower/npg13/top-npg13.pdf>.

70. *U.S. Navy Program Guide 2013*.

71. "Statement on Strategic Choices and Management Review, Pentagon press briefing remarks by Secretary of Defense Chuck Hagel," Washington, DC, 31 July 2013, <http://www.defense.gov/speeches/speech.aspx?speechid=1978>.

72. House Committee on Armed Services, *Hearing on Planning for Sequestration in FY 2014 and Perspectives of the Military Services on the Strategic Choices and Management Review*, 113th Cong., 1st sess., 18 September 2013.

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.

Why Cyber War Will Not and Should Not Have Its Grand Strategist

Martin C. Libicki

Cyber war proponents often argue the domain needs its own Billy Mitchell or Giulio Douhet—strategists with great vision who will declare to the world what great power lies therein.¹ To be sure, cyber war has no shortage of advocates. But as Colin Gray recently observed, “When historians in the future seek to identify a classic book or two on cyber power written in the 1990s and 2000s, they will be hard pressed to locate even the shortest of short-listable items. . . . Certainly they are nowhere near deserving (oxymoronic) instant classic status.”²

But has the failure of cyber war to generate any such ideal necessarily been a bad thing? There is a case to be made that it is too early to expect such a classic. If the Owl of Minerva flies at dusk, in cyberspace the sun is just above the yardarm; the information revolution is hardly a done deal. But such a case is too easy. What if the fundamental features of cyber war were to remain essentially as they are into the indefinite future? Although highly unlikely, this is not so absurd a proposition. The late Roger Molander of RAND would frequently remind me that the questions we wrestled with in the mid 1990s are no less relevant and no better understood today than they were then.

Even assuming that the cyber domain has yet to stop evolving, it is not clear that a classic strategic treatment of cyber war is possible, or, even if it were, it would be particularly beneficial. In explaining why, this article makes three points. First, the salutary effects of such classics are limited. Second, the basic facts of cyberspace, and hence cyber war, do not suggest that it would be nearly as revolutionary as airpower has been, or anything close. Third, more speculatively, if there were a classic on cyber war, it would likely be pernicious.

Martin C. Libicki, PhD, is a visiting professor at the US Naval Academy and a senior management scientist at RAND focusing on the impact of information technology on domestic and national security. Previously, he worked for the National Defense University, the Navy Staff, and the GAO's Energy and Minerals Division. He holds a master's degree and a PhD from the University of California–Berkeley.

The Limited Usefulness of Classics

Clausewitz's *On War* was, is, and will continue to be perhaps *the* classic book on warfare, but it would be an exaggeration to argue that it was an "instant classic." It was published posthumously. Its influence spread slowly—within a generation in Germany and not until after 1945 in the United States. Furthermore, it really is not a book that gained its reputation by talking about land warfare as such. True, all of its chapters between the introduction and conclusion are about land *warfare*. But what made it a classic was its treatment of war itself—that is, the role and purpose of military force within the relations among states and the relationship between the goals of war and its reality in battle ("fog and friction").

In the naval domain the name Mahan is clearly front and center. Mahan lauded naval power as essential to the maintenance of a seafaring state, especially one that wanted to maintain a global empire—not an irrelevant consideration circa 1890 when he published *The Influence of Sea Power upon History, 1660–1783* (such historic dates suggest he was not overly impressed by technology fads). His book argued strenuously for large battle fleets, which by their very presence and concentration ("fleet in being") could dissuade other states from trying to assert sea control on their own behalf. He eschewed the *Jeune École* preference for commerce raiding.

Mahan's work was enormously influential inside the United States (an inspiration for Theodore Roosevelt's Great White Fleet), and perhaps even more outside it. Kaiser Wilhelm was particularly enchanted by it, as were, to only a slightly lesser extent, Jackie Fisher and the British Royal Navy. Although the expensive Anglo-German naval rivalry cannot be entirely laid at Mahan's doorstep, his influence was not trivial, and the rivalry over battleship building hardly played a calming role in that bilateral relationship.

As for naval strategy, Mahan's work was not particularly helpful for those who believed in his doctrine. The Kaiser's love for his fleet kept it in port for the two and a half years after the Battle of Jutland, even though Germany might have had a chance—admittedly, with a substantial amount of luck—to break the blockade on it and the Austro-Hungarian Empire. This blockade ultimately accelerated the Central Powers breaking under the stress of war before the Allies did. Meanwhile, the naval action that nearly broke the war the other way was the success of German

U-boat attacks on Britain's supply lines to North America. In retrospect, the more decisive use for naval power in World War I was closer (albeit with submarines, not surface ships) to the commerce-raiding that Mahan disdained 25 years earlier in favor of grand fleet actions. He had argued these fleet actions were the *sine qua non* of naval power.

All this suggests that the global enthusiasm over Mahan's writing—which *was* an instant classic—was good neither for world peace nor a productive naval strategy. Perhaps these are tough tests for any analyst to pass, but if we are to laud the writing of great strategic formulations these are not unfair evaluations.

Consider now airpower. Three individuals stand out in the development of post-World War I strategic thought: the writer Giulio Douhet and generals Billy Mitchell and Hugh Trenchard. All three argued that air forces would become an increasingly important component of modern militaries and that military strategy should, correspondingly, reflect that fact. In that insight, they were correct.

Douhet went further to emphasize the role of strategic bombardment in not only winning future wars, but also shortening them (in that respect—if World War II was any indication—he was not correct). There is an important distinction to be made between the tactical or operational use of airpower (to aid ground and naval forces) and its strategic use: to break the enemy's will to resist and destroy its ability to arm itself. In theory, air forces can do both operational and strategic missions; in practice, their resources are limited, and funds used for strategic purposes compete for resources used operationally.

This leads to the question: Was World War II's emphasis on the strategic campaign such a good idea? In the first major war in which this proposition could be truly tested, only three countries were capable of mounting a serious strategic bombing campaign—first Germany, then the United Kingdom and the United States. Germany's efforts did not seem to have accomplished much; it did not force the UK out of the war nor make much of a dent in its war production. The US and UK bombing campaigns certainly had effects, but these effects were purchased at great cost—the Eighth Air Force alone suffered more than 50,000 deaths (by comparison, the entire US Pacific campaign cost twice as many lives). The succeeding decades saw considerable controversy over whether such bombing campaigns were worthwhile, with detractors saying they *increased* Germany's will to resist and, only toward the very end,

impaired its ability to produce war materiel. A recent prominent defense of strategic bombing by Richard Overy maintains they were worthwhile,³ not for what harm they did to the Germans, but for how much Germany spent (mostly wasted) to counter them. Even if true, that is a far cry from Douhet's rationale ("air power will demoralize foes" to "air power will cause foes to overreact in self-defense"). Admittedly, a B-29 loaded with nuclear weapons can have a considerably greater effect than a B-29 loaded with conventional weapons—a victory for airpower, but only for 15 years until missiles were invented to do the job more efficiently and reliably. Furthermore, it took until NATO's campaign in Kosovo before there was a first, albeit even then arguable, validation of Douhet's thesis.

If the strategic implications of airpower were poorly understood by virtue of their being exaggerated, the operational implications of airpower à la Billy Mitchell (and many others at the time, if not so dramatically) were on point. Airpower *would* rise in importance relative to land and sea weapons. At sea, by 1942 the carrier was universally recognized as the replacement for the battleship, although the carrier was under firm naval control. Only a half-century after World War I, success in gaining air control (the 1967 Six-Day War and Operations Desert Storm and Iraqi Freedom) predisposed and foretold success in ground combat (at least over uncluttered terrain).

The basis for Billy Mitchell's optimism was, in retrospect, clear. Every year, aircraft became faster; flew higher, farther and longer; and could carry more weight (weapons but also cargo). Antiaircraft weapons were improving but not so quickly (targeting radar and analog computing helped but only somewhat). Nor were ground or sea-based weaponry getting more impervious to bomb damage all that quickly. Technology was inexorably shifting the dominance of battle to the skies. That being so, every other decision about the conduct of battle would have to factor the shift-in-power relationships from ground and surface to air accordingly.

As noted, nothing boosted airpower as much as the development of atomic weapons, which seemed to have validated Douhet's thesis, at least *ex post facto*. The US Air Force came to absorb almost half of the nation's defense budget in the Eisenhower administration. Clearly, a single weapon capable of knocking out cities was going to have a strategic effect on both war and warfare. So, were there any classics in this new *atomic* field, and what good did they do?

The first place to look was a set of essays by Bernard Brodie for the book, *The Absolute Weapon: Atomic Power and World Order*,⁴ wherein can be found his famous quote: “Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them. It can have almost no other useful purpose.” His essays do mention deterrence, but the thrust of his writing was not about how to use atomic forces but to drive home the point that a country under serious atomic attack (that is, thousands of atomic bombs) would be effectively destroyed regardless of how well defended it was. Indeed, his essay spends more time on how to lay out cities to maximize their survivability in an atomic war than it does contemplating what a strategy of deterrence might mean for the construction and the use of forces. So, instant classic quote but no instant classic work.

More works followed in the 1950s by Albert Wohlstetter (on the importance of a second-strike capability),⁵ Tom Schelling (on strategies that “left something to chance”),⁶ and Herman Kahn (on the need for escalation dominance).⁷ It was undoubtedly brilliant stuff, but was it necessarily a wise way to fight—or, better yet, avoid—a nuclear war? The classic model of a nuclear confrontation featured ultra-cool decision makers rationally facing the prospect of mega deaths and maneuvering deftly to avoid that and worse. The actual conduct of a nuclear crisis (Cuba 1962) suggested something a little different: world leaders, having stared at the abyss, realized they had come far too close to a nuclear holocaust and never ever wanted to get that close again. Reactions to that near catastrophe included the hotline and the 1963 test ban treaty. Rather than each side making noises as if it would throw the steering wheel out the window (as Schelling’s strategy suggested), each instituted measures to ensure and assure others that it had a much better grip. Similarly, strategic thinking, deprived of direct evidence of Soviet thought, tended to assume that the Soviet Union would approach a confrontation much as Americans would—that is, by carefully delineating (if not necessarily observing) a firebreak between conventional and nuclear operations. The opening of the Soviet archives in 1989 indicated that such delineations were not particularly important to them. Fortunately, no one ever had to go to war based on these strategic theories.

Incidentally, none of this infers that such thinkers did not educate the mind by raising key questions. Even when wrong, one cannot help but profit by working through arguments and, in some cases, asking whether

their logic applies to cyberspace. Unfortunately, when such thinkers are cited as authorities—which they inevitably are—their arguments are converted into answers, at least in the minds of their adherents.

The next two domains of conflict—space and spectrum—have no comparably memorable strategic doctrines or assessments associated with them at all. This, alone, should raise the question of why cyberspace should. Once touted as the really high ground, outer space turns out to be merely a nifty place to stick information collection/processing devices—surveillance satellites, communications relays, and timing/navigation systems (e.g., GPS)—and it is not clear that space will always remain competitive vis-à-vis networked unmanned air-breathing systems for the first two roles. Space is not a particularly good place from which to fight wars. It costs a great deal to get something into orbit, and the price per pound has not appreciably fallen since the 1970s. Space-based weapons are not only expensive but, in their current incarnation, take longer to reach their targets than do simple missiles⁸—deorbiting something actually takes some time. Space systems are also quite fragile in the sense that they can be destroyed by a very small object hitting head-on at a relative speed of 36,000 miles an hour, assuming they are both in low-earth orbit. In a contest between a ground-based missile and a satellite, the odds (these days) are on the missile. So, much to the anguish of the space community, here is a domain without a strategic concept, and, at this point, not inappropriately. It is easy, incidentally, to get lost in arcane debates over which orbit in space is truly the high ground that dominates all the other orbits in space (true aficionados wax rhapsodic about controlling the L1 point, which is roughly four times as far from the earth as the moon and sits directly between the sun and the earth).

Finally, a word is needed in defense of the radio-frequency (RF) spectrum as a domain of warfare, mostly because this domain not only lacks a strategic theory but lacks a strong proponent for theory-building. Yet, it is a *physical* domain in which dominance, in the sense that those who can get their signal through and keep others from getting their signal through, thereby gives its possessor a signal advantage in warfare. No serious military power ignores electronic warfare, largely because radio communications allow militaries to coordinate their operations and radar allows detection and tracking of all manner of enemy assets. But the wizards in the business know the purpose of manipulating the use of a spectrum is to enable physical warfare; by itself, electronic warfare is

next to worthless. Similarly, no one seriously thinks that one country can wreak persuasive or dissuasive damage on another by unleashing its electronic warriors on it, although the latter may be the source of some interesting forms of annoyance, particularly if they can interfere with all GPS applications and mobile devices.

The Significance of Warfare in Cyberspace

It should be fairly clear by now that this article will not close with a ringing call for a strategic cyberspace doctrine. As oft noted, such doctrines—even, or especially, if they meet with universal approbation—are as likely to be wrong as they are right.

To start with, cyber warfare and cyber war need to be distinguished from one another. Cyber warfare, like warfare itself, is about the conduct of war, carried out inevitably to further the performance of combat in the physical domain (it can also be considered operational or instrumental cyber war). Cyber war is undertaken to affect the will of the adversary directly (it can also be considered tantamount to strategic cyber war). A similar distinction can be made between electronic warfare and electronic war—the difference being that no one talks about electronic war as something interesting.

First we can ask whether cyber warfare can so alter warfare that warfare—how it is conducted and what one can do with it—needs to be seriously rethought. Although the ultimate answer to that question is empirical and yet to be determined, it is easy to establish that such a question cannot be answered without an important intermediate step. Cyber warfare attacks systems and digital networks. Prior to the 1960s, militaries had no digital networks to attack. A cyber attack carried out against a military today can, at worst, return it to its prenetworked condition (as long as it *has* something to revert to). To argue that cyber warfare can have a revolutionary effect on the battlefield requires establishing that digital networking is itself revolutionary. This is a step many proponents of cyber warfare neglect to take.

So how much *does* digital networking improve the workings of a military? First, one does not need digital communications to have RF communications; the latter can be carried out with analog equipment as it was prior to the 1970s, and, to some extent, still is. Second, as helpful as network-centric warfare may have been for the United States, every

other military in the world is less digitized and therefore less susceptible to cyber war than the US military (notwithstanding the possibility that the digital equipment they have is more vulnerable than the equivalent in the hands of US forces).

Thus, the revolutionary impact of cyber warfare can be no greater than the revolutionary impact of digital networking, which is not, itself, a fully tested proposition. The question of how much less entails asking how effective cyber warfare can be at nullifying the advantages of digital networking. The most it can be is 100 percent, but there are many simple measures militaries can take to reduce it well below 100 percent. One is electronic isolation. If a network is disconnected from the rest of the world, it is very difficult for outsiders to penetrate it. In practice, as Buckshot Yankee and Stuxnet proved, it is not enough that a network lacks an Internet address (or a phone number). There also has to be no way for errant bytes to get into these machines via RF links that depend on the strength of the attacker's transmitter. These are challenging problems but hardly insurmountable. For the most part, systems can be immunized against much of cyber warfare if their instructions are difficult to alter without hands-on contact. This could be because the logic is hardwired into the unit, or because the logic can only be replaced by new hardware modules, or the update has to be digitally signed by a known trustworthy source (using reliable cryptographic protocols implemented correctly). This prevents malware or malicious software with rogue instructions from being placed on the machines, which then limits a machine's actions to those prespecified in its programming. Stuxnet, (and its relatives such as Flame) as well as much of cybercrime, and the advanced persistent threat all depend on the possibility of malware (arbitrarily altered instruction sets) to work.⁹

All this suggests that the effect of cyber warfare, if properly recognized, will be far less revolutionary than the putatively revolutionary effect of digitized networking.

In fairness, consider two objections to this argument. One is that militaries cannot revert to their predigitized network state. This may be empirically true, but if true, it says either that (1) such militaries have abjured that option because they *correctly* recognize that the impact of cyber warfare is something they can manage, or (2) the revolutionary impact of cyber warfare is *incorrectly* underappreciated by militaries who consequently digitize without giving sufficient thought to what would

happen if cyber warfare *were* revolutionary. If the former is true, the issue is settled. If the latter is true, then the only way cyber warfare could be revolutionary is if those victimized by it fail to see it was going to be revolutionary. This is the sort of error that is unlikely to be made more than once, if it is even made at all. Consider, by way of example, Stuxnet. If Iranians had understood what Stuxnet *could* have done to them, they would have likely taken pains to ensure that no USB device was accessible. Because it came as a surprise, Stuxnet worked. But can one assign revolutionary strategic impact to a form of warfare that requires it be systematically underestimated before it can work?

The second objection is that while cyber warfare is not much to look at now, it is only to get more important as militaries continue to digitize. This line echoes the argument that aircraft were going to get better every year; thus, what was false today may be true tomorrow. Can the same be said about cyber warfare?

At this point in the article, one distinction between cyber warfare and warfare in all other media must be made: cyber warfare (as well as cyber war) requires that the targets have made mistakes in their implementation and use of digital equipment. In theory, digital machines should only obey their given instructions in service of their owners/operators. In practice, there are variations between what a system actually does and what it is supposed to do that permits cyber warfare to work. But neither the form nor even the existence of these variations is inevitable. They are artifacts of systems programming. Such artifacts can be reduced, perhaps even effectively eradicated. As noted above, even if systems still have errors, users—especially military users—have a great number of steps they can take to reduce vulnerability to cyber warfare. Indeed, many such steps are being taken—and, doubtlessly, more would be taken if the threat from cyber attacks and the like were greater (or at least perceived to be greater) than is currently the case. This is no proof that there will be a declining threat from cyber warfare to advanced militaries (militaries that have failed to advance have little or nothing to attack in cyberspace); it may well grow. The fact that the threat from cyber warfare has to be enabled by the target's decisions weighs against the proposition that cyber warfare can be revolutionary.

Indeed, there is every indication that electronic warfare will continue to generate more consequential effects on the battlefield than cyber warfare because electronic warfare is not an artifact of the other side's poor

decisions. It is an unavoidable aspect of long-distance RF communications. And, as noted, there is no classic strategic treatment of electronic warfare; nor is there indication that such effort is missed.

That leaves the question of whether strategic cyber war can be significant enough to merit some twenty-first-century version of the Douhet proposition: a form of war that can induce countries to stop fighting (or better, avoid starting fights) without having been defeated or threatened on an actual battlefield. Arguments similar to those above can be generated to suggest that such a thesis is not terribly convincing today. Most cyber attacks, once discovered, are resolved and the effects (apart from leaked information) reversed within a period ranging from hours to days. In the long run, even in the highly unlikely event that hackers will always be able to control the systems they attack, the worst that can happen would be to convince people to abandon networking and thus set economies back to where they were in 1995 (when the Internet started to spread beyond universities and defense-related sites).¹⁰ For advanced countries, 1995 is not that much further behind than they are in 2013. Thus an economy subject to continuous, vicious, and expectedly successful attacks would not retrogress as much as a society subject to World War II-level bombing. And cyber attacks have yet to kill anyone. Granted, if societies have evolved in ways that are difficult to reverse, the effects of cyber war on such societies may be worse than if they had never adopted digitized networks in the first place. But such effects, almost by definition, can be used only once—and only if a society's leadership systematically underestimates its vulnerability to cyber war. Of course, if cyber war turns out to be weak, then perhaps they have not underestimated it at all.

Over time, the distance between 1995 and the then-current year will increase, which will, in theory, lend cyber war more leverage than it has today. Perhaps then, it will be possible to write how cyber war has changed everything we know about warfare. Or maybe not. True, just as aircraft grew monotonically more capable from their invention forward, so societies are growing increasingly digitized, with little prospect that they will move backward (unless, cyber attacks prove to be far more powerful and unavoidable than they are today). But the correlation ends there. Aircraft improvement was a contest against a fixed target (the laws of aeronautics, physics, and chemistry); cyber war is a contest against a moving target wherein offense contends with defense. It is not obvious that offense will get continually better, particularly when defense (in the

form of the target's system and software) defines what the offense can do. Granted, hackers are getting better, thanks in part to markets and market-like mechanisms for sharing information about software vulnerabilities. Furthermore, new uses for digitization (e.g., networked cars) are constantly creating new vulnerabilities or new ways for vulnerabilities to do serious damage. But defense is not catatonic. If the problem with cyber attacks gets bad enough, there are more radical steps that can be taken. One example is Apple's iOS operating system, which has successfully resisted malware because it is a fairly closed system (although some countries have been rumored to have prepared and stashed away attacks on it). Another is the consensus reached by security professionals that Java (software) should be disabled on all browsers because it is becoming very difficult for its developer to stay ahead of all the vulnerabilities hackers keep discovering in it. On purely technical grounds, every successive version of Microsoft's products is more malware-resistant than its prior versions. These days operating systems are subverted by insecure applications rather than being attacked directly. So, the technology dynamic that Billy Mitchell employed—even if aircraft cannot do it today, tomorrow's eventually will—does not necessarily translate into cyberspace, even if cyber security may get worse before it gets better.

Then there is the possibility that the strategic effects of cyber war may arise from the interaction of state actors that systematically overestimate its effects (as quasi-apocalyptic statements from both US and Chinese military officials suggest is quite possible). This could lead to unfortunate dynamics, but in the longer run, the problem with such analyses is similar to those analyses that posit leaders to *underestimate* the effects of cyber war and are therefore unprepared in ways that make it more dangerous. Either way, this is an attitude capable of being corrected by events, and, by its very nature, of temporary import (unless one can successfully argue that the *perception* of what cyber attacks *have done* is systematically in error, but that is a hard case to make).

Cyberspace, as it turns out, is ill-suited for grand strategic theories for other reasons. As mentioned earlier, cyberspace *is* changing very quickly in many important respects. Circa 1999, for instance, US cyber war capability, such as it was, housed itself within the US Space Command (disestablished in 2002). In an era in which mischief in cyberspace was most likely perpetrated by individual hackers who were adroit at getting into systems, maneuvering deftly while discovering how they worked,

doing their job, and leaving quietly, its working ethos would have made it a natural fit for something like the US Special Operations Command. Fortunately, that never happened, because within a dozen years, it was clear that hacking was less about individual rough-and-ready hackers and more like a team-based enterprise building malware tools that took commands from afar and otherwise went about their business based on their programmed-in wits. Today, the original fit between cyber war and the space business looks better—although the fit between US Cyber Command and the National Security Agency is quite good itself.

Another difficulty in proposing a grand theory of cyber warfare is that deception lies at the essence of cyber war. Systems, although meant to be under the control of their owners/operators, are tricked into obeying the commands of others. Once the precise nature of the trick is realized, it is relatively straightforward to figure out how to foil that particular attack—requiring hackers to come up with new tricks, which they often but cannot always do. Deception, by nature, introduces its own self-defeating dynamic, because its existence depends on two sides having different notions of what something can do. Success, in certain key respects, is often inherently unpredictable. Those who wrote strategic theory for, say, airpower had the advantage of understanding the interaction between the machine and its aeronautical environment and between weapons and their targets. They could use that solid base to speculate on the relationship between the effects caused by aircraft and the goals for which countries went to war. Those who would write strategic theory for cyberspace have no such foundation. Everything appears contingent, in large part, because it is.

The Possibly Pernicious Effects of Writing a Cyber War Classic

To be fair, it is not easy to counter what some yet-to-be-written cyber war classic would say. Setting forth here the brilliant insights of such a classic would create the tome this article says cannot exist. Yet, if cyber war's forthcoming classic looks like classics in past domains, they are likely to say (1) cyber war is totally important, (2) those who wield its power should fight to win wars on their own rather than helping warriors in other domains, and (3) war fighters in those other domains should take their strategic cues from what takes place in cyberspace.

To say that war in the virtual world can match the horrors of war undergone or contemplated might seem a stretch, but anyone who ventured such an opinion would not stand alone. Joining them would be the US Defense Science Board (which imagined a cyber attack so severe as to merit a nuclear response),¹¹ some Chinese generals (one of whom casually opined that a cyber attack could be as damaging as a nuclear attack),¹² and even Russian president Vladimir Putin (who said that a cyber war could be worse than conventional warfare—this from the head of a country that lost 25 million in World War II).¹³ There is nothing quite like a good nuclear analogy to rally those in favor of an independent cyber-war force. Yet, the mere argument that cyber war is going to be very important hardly says what to do with cyber-war capabilities, apart from keeping them well fed.

Emphasizing the strategic aspects of cyber war over its tactical (alternatively, operational or instrumental) aspects is not necessarily wrong. Because the operational uses of cyber war are neither ethically nor particularly strategically problematic¹⁴—in that it only substitutes nonlethal for lethal means—there is little reason *not* to use it against military targets. But military targets are generally harder targets than civilian ones. What may produce limited gains on the battlefield may produce huge payoffs off the battlefield, thereby tempting the elevation of the strategic over the operational.¹⁵ But such elevation has consequences. It affects the allocation of resources and manpower. If talented cyber warriors convince themselves that strategic warfare offers a better shot at top command slots, they will migrate accordingly. Perhaps if cyber war *is* that important, there will be enough resources and manpower to go around—although the current difficulties in finding enough cyber-security professionals suggest that their supply is not infinite and only time will tell how elastic. However, there are certain resources where serious choices must be made: that is knowledge of vulnerabilities in software that allows cyber warriors into many of their targets. To the extent military and civilian systems rely on the same software and hardware—as they increasingly do, although there are still major differences—then a vulnerability exploited for disruptive/destructive purposes (rather than espionage) is likely to be a vulnerability that can be used only during a small time window. Its availability for strategic purposes limits its availability for military purposes. Hence, choices, notably between operational and strategic cyber war, must be made. Because systems have to be penetrated

well before they are attacked, such choices may have to be made well before the character of the upcoming conflict is clear.¹⁶

Consider, too, that both forms of cyber war—the strategic and the operational—compete with cyber espionage when it comes to allocating vulnerabilities to exploit.¹⁷ Those who want to reserve the exploit for cyber espionage can make two strong points. First, since penetration, in and of itself, tends to be deliberately stealthy, the vulnerability can remain hidden longer than it can once a disruptive/destructive attack takes place.¹⁸ Second, the yield from cyber espionage can be immediate, while the yield from getting into a system that might be taken down is contingent on a war starting.

Strategic cyber war is far more problematic than its operational cousin. It raises laws-of-armed-conflict issues that operational cyber warfare does not. Similarly, it is more likely to result in escalation and in ways that make conflict resolution more difficult. By contrast, operational cyber warfare ends when kinetic warfare ends, because there is no longer any advantage in making targets more susceptible to kinetic attack when kinetic attack terminates.

If the galvanizing theory emphasizes doctrines such as preemption, further difficulties await. Although exactly how to preempt a cyber attack remains a mystery, there is very little that can be destroyed, and only a narrow class of attacks can be disrupted by actions taken outside one's network. If the doctrine is attractive enough, people will think they have found a way to do so. Unfortunately, the many ambiguities of who is doing what to whom in cyberspace suggest that understanding who is preparing to do what to whom is even harder to discern. Grave mistakes are possible—particularly if the decision to preempt attacks is delegated from the president, as many have suggested it might be.¹⁹

Finally, what might be those cues that warriors in today's domains should take from cyberspace according to some yet-to-be-written doctrine? Cyber war is sneaky stuff. It relies on deceiving computers, which, in turn, requires deceiving humans who manage these computers. It usually works a great deal better when it comes without warning. Insofar as its success depends on the discovery of impermanent elements in the target system, laid-in attacks have to be used quickly if they are to be used at all. Furthermore, because many of its effects are temporary, they must be exploited in a very short time (as quickly as within hours and days). In that sense, powerful cyber attacks can pull follow-up strategic or

operational actions behind them, whether or not the latter are, respectively, appropriate or ready. Cyber war is also an elite activity in which numbers of hackers count for little but the skills of the best of the best count for a great deal.

Cyber operations are covered in heavy layers of secrecy. In some ways, secrecy is deserved: vulnerabilities described quickly become vulnerabilities eradicated. But in other cases, it is questionable: no country admitted to having cyber-war forces until 2012. And in other ways, particularly when disclosing information about vulnerabilities that the other side found in the systems of commercial organizations, it can get in the way. All this makes it difficult to have a serious public debate about the role of cyber war in national security. To be fair, the common difficulty of understanding cyberspace also interferes with useful public debate. Hence the question: Would it be beneficial for the mores of physical war fighting to reflect the inherent mores of war fighting in cyberspace? Perhaps not.

Conclusions

So, rather than bemoan the fact that there are no instant strategic classics on cyber war, or even well-percolated ones, perhaps we should count ourselves lucky. Many of the strategic classics from earlier domains seem to have been misleading, even harmful. War fighters that deal with the more recent media, such as outer space or the radio-frequency spectrum, seem to be doing just fine without them. And cyber war appears to have even less basis for a strategic treatment than space warfare or electronic warfare. Its efficacy—much less significance—has been postulated well before it has been proven. By its very nature, cyber war has to continually morph to retain its relevance. Furthermore, there are good reasons to believe that its contribution to warfare, while real, is likely to be modest, while its contribution to strategic war is a great deal easier to imagine than to substantiate. **SSQ**

Notes

1. To those who think the argument in favor of finding a Billy Mitchell for cyberspace is a straw man, note the following requests from Frank Cilluffo, former special assistant to the president for homeland security: “We must find the cyber equivalents of Billy Mitchell, George Patton, Curtis LeMay and Bill Donovan—leaders who understand both the tactical and strategic uses of new technologies and weapons,” <http://www.gwumc.edu/hspi/policy>

/Cilluffo_Knop.pdf); Stewart Baker, former general counsel of NSA: "As Brig Gen Billy Mitchell predicted, airpower allowed a devastating and unprecedented strike on our ships in Pearl Harbor. We responded with an outpouring of new technologies, new weapons and new strategies. Today the threat of new cyber weapons is just as real, but we have responded with an outpouring—not of technology or strategy but of law review articles, legal opinions and legal restrictions," <http://www.steptoe.com/publications-8146.html>; Robert Cringely, an influential columnist in the IT trade press: "My fear is that when it comes to cyber warfare there is no Billy Mitchell today in Washington," <http://www.cringely.com/2009/06/01/remember-billy-mitchell/>; George Stein writing in *Air Power Journal* in 1995: "In some ways, 'info-warriors' are like Gen William ('Billy') Mitchell and the pioneer league of airmen. They see the potential. Mitchell's vision of the potential for airpower drove, at great cost to himself but great benefit to the nation, the development of a new form of warfare"; and Robert Lee writing in *Air and Space Power Journal* in 2013: "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."

2. Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is not Falling* (Carlisle, PA: US Army War College Press, April 2013), viii, <http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubid=1147>.

3. Richard Overy, *Why the Allies Won* (New York: Norton, 1997). Incidentally, his most recent book, *The Bombing War* (New York: Penguin, 2013), is far more critical of the entire air campaign.

4. Bernard Brodie, ed., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace, and Co., 1946).

5. Albert Wohlstetter, "The Delicate Balance of Terror," *Foreign Affairs* 37, no. 2 (January 1959): 211–34.

6. Thomas Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960).

7. Herman Kahn, *On Escalation* (Westport, CT: Praeger, 1965).

8. For a good general treatment, see Robert Preston, *Space Weapons, Earth Wars* (Santa Monica, CA: RAND, 2002).

9. This does not eliminate all sources of cyber warfare. A class of attacks known as SQL (structured query language) injection does not require malware to work, but it only works against systems that accept structured queries, which very few weapons systems do.

10. In the short run, it is possible that an errant set of codes can break equipment, as happened to Iran's nuclear centrifuges following Stuxnet. There is considerable disagreement about whether Stuxnet can be replicated. Its revelation, incidentally, by illustrating what is theoretically possible may have made a repeat performance practically much more difficult because systems managers came to understand they expose their sensitive production and control equipment to the outside at their peril.

11. "The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War." Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat* (Washington: DoD, January 2013), ES-1.

12. "The United States and China held their highest-level military talks in nearly two years on Monday, with a senior Chinese general pledging to work with the United States on cybersecurity because the consequences of a major cyberattack 'may be as serious as a nuclear bomb.'" Jane Perlez, "U.S. and China put Focus on Cybersecurity," *New York Times*, 23 April 2013, www.nytimes.com/2013/04/23/world/asia/united-states-and-china-hold-military-talks-with-cybersecurity-a-focus.html.

13. “[Putin] warned that damage from cyberattacks could be higher than that of conventional weapons.” “Putin Urges Readiness against Cyber and Outer Space Attacks,” *RIA Novosti*, 5 July 2013, www.rianovosti.com/russia/20130705/182079750/Putin-Urges-Readiness-Against-Cyber-and-Outer-Space-Attacks.html.

14. “Particularly” inserted to the extent there are not fully explored stability impacts of using cyber war as the opening shot of a kinetic engagement or using any form of warfare where attribution is less than obvious.

15. In March 2013, “The chief of the military’s newly created Cyber Command told Congress . . . that he is establishing 13 teams of programmers and computer experts who could carry out offensive cyberattacks on foreign nations if the United States were hit with a major attack on its own networks.” Mark Mazzetti and David E. Sanger, “Security Leader Says U.S. Would Retaliate against Cyberattacks,” *New York Times*, 12 March 2013, <http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html>. It would seem, from such comments, that these offensive teams would be oriented toward strategic rather than tactical missions.

16. That NATO actions against Gadhafi were unforeseen months before they took place was a key reason that cyber attacks were not used to take out Libyan air defenses. See Ellen Nakashima, “U.S. Cyberweapons Had Been Considered to Disrupt Gaddafi’s Air Defenses,” *Washington Post*, 17 October 2011, http://articles.washingtonpost.com/2011-10-17/world/35276890_1_cyberattack-air-defenses-operation-odyssey-dawn.

17. Not every exploit, however, requires a software vulnerability. Some can be penetrated and exploited by poor systems administration, notably but not exclusively, poor password management.

18. A year is roughly the time that a typical (discovered) advanced persistent threat attack lasts prior to its discovery. Mandiant, *APT 1: Exposing One of China’s Cyber Espionage Units*, <http://intelreport.mandiant.com/>. A year is also roughly the time that a discovered vulnerability sold on the vulnerability market remains undiscovered by anyone else. Nicole Perlroth and David E. Sanger, “Nations Buying as Hackers Sell Flaws in Computer Code,” *New York Times*, 14 July 2013, www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html.

19. David Sanger and Thom Shanker, “Broad Powers Seen for Obama in Cyberstrikes,” *New York Times*, 3 February 2013, <http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html>.

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.

War on Our Doorstep

Not a Mere Crime Problem

James P. Farwell
Darby Arakelian

The television show *Miami Vice* regaled viewers with stories of undercover agents as they battled to keep Colombians and their Miami cohorts from smuggling cocaine and other illegal drugs into this country. In real life, US authorities did even better. They proved so effective that the Colombia cartels decided to shift operations west and outsourced drug trafficking to Mexican gangs. Instead of cash, they paid the traffickers in-kind, offering 30–50 percent of the drugs to sell on their own, and the gangs graduated from transport to distribution. Drug trafficking through Mexico had long been a problem, but this change triggered a great rise.¹

While Western media focus heavily on the civilian deaths in Syria, they often overlook our own backyard, where Mexican drug violence has claimed 110,000 lives.² Former president Felipe Calderon pronounced that “the most lethal war is the one being fought by criminal gangs among themselves.”³ That statement reflects only one element in the story, because cartel violence greatly affects the United States.⁴ As cartels battle for turf among one another, the threat transcends borders and raises *hemispheric security* issues that embrace the United States, Canada, Mexico, and their neighbors in Central and South America. Mexican security forces have made cross-border incursions into this country, hundreds of US Customs and Border Patrol (CBP) agents have been attacked,⁵ and even US Soldiers have been suborned into acting as hitmen south of the border.⁶ The cartels are also increasingly active in US cities.

Dr. James P. Farwell is a national security expert who has advised the US Special Operations Command. He holds a JD in law from Tulane University and a DCLS in comparative law from the University of Cambridge. He is the author of *Persuasion and Power: The Art of Strategic Communication* (Georgetown University Press, 2012).

Darby Arakelian is a national security expert and former CIA officer. She holds a BA in political science, Russian, and economics from the University of Denver and an MA in security policy studies from the George Washington University. Ms. Arakelian specializes in terrorism and counterterrorism communications strategy and analysis, cyber warfare, and automated media monitoring and analysis.

Although Calderon's team boasts that it captured 25 of its 37 most wanted criminals,⁷ no one suggests the flow of drugs has been stopped. In this high-stakes struggle, while Mexico may not be a failed state, the war is eroding its credibility and ability to govern. It is also affecting security in the region. In Guatemala, cartels reportedly control 40–60 percent of the entire country.⁸ The Mexican Sinoloa cartel has formed links with Mara Salvatrucha (MS-13), a gang started in Los Angeles by Salvadoran immigrants.⁹ Mexican cartels are also linked to murders in Argentina and Peru.¹⁰

While the United States wants to stop trafficking and eliminate kingpins, Mexicans want to stop kidnapping and violence. This has left both Mexico and the United States without a cohesive strategy for combating the cartels—a totally unacceptable situation. Most observers, including the Mexican government, believe this to be a law enforcement problem. We challenge whether that approach is most effective and argue that conventional definitions for characterizing this struggle do not apply to this emerging, unprecedented conflict. The required debate over how to protect vital US security interests has barely commenced. What legal authorities govern US action? What roles should our military or law enforcement play? Do we rely upon conventional definitions of high-intensity crime, terrorism, or insurgency to dictate solutions? What are the tradeoffs for using the military or law enforcement to battle the cartels? The threat to US national security interests calls for a different approach. A combination of law enforcement, social reform, covert intelligence, military special operations, and, as appropriate, selective military action by Mexico with indirect mission assistance from the US military offers a plausible path to success.

Characterizing the Conflict to Determine Strategy

How the war is characterized matters as to what body of law governs it—the law regulating law enforcement or the law of armed conflict?¹¹ The answer affects tactics and the nature of forces employed. For example, while police can use deadly force against suspects who pose a threat of serious physical harm, the principle of military necessity authorizes a military to take all necessary measures not prohibited by international law to defeat an enemy.¹² The US and Mexican militaries have a role in low-intensity conflict, fighting an insurgency, or combating terrorism,

especially if those terrorist groups support al-Qaeda.¹³ Scholars like Paul Rexton Kan argue that while drug cartels share certain organizational and operational characteristics of terrorist organizations,¹⁴ the Mexican drug war is not an insurgency because cartels lack a political agenda. Kan's key argument rests upon the widely—and mistakenly—held view that terrorists seek political goals while criminals are motivated by greed.¹⁵ Writing in *Small Wars Journal*, Brad Freden acknowledges that elements of counterinsurgency (COIN) operations are useful in fighting the cartels but argues that “the violence, drug trafficking, and lawlessness that we see in northern Mexico does *not* constitute an insurgency. Drug cartels have no ideology beyond profit, no aspirations other than to be left alone, and no popular support beyond that which can be purchased with money or intimidation” (emphasis in original).¹⁶ University of Maryland scholar Shibley Telhami also views terrorists as linked to political goals and defines them as those who deliberately target civilians for such ends.¹⁷

Those who oppose characterizing the Mexican drug wars as an insurgency argue that cartels have not “captured” the state to implement a social or political agenda and are not seeking to overthrow the government and replace it with their own, but focus on shoving the state aside in their pursuit of profits. This thinking, ably argued by Kan, is that “no insurgent or terrorist group . . . has been dismantled by rolling up its financial networks,” a statement that would come as news to the US Treasury and other agencies engaged in counterterrorism financing.¹⁸ The pivot of the argument is that cartels do not seek to “substitute their ideology for the existing one or to achieve any other political goal that is routinely associated with armed groups who instigate social upheaval.”¹⁹

So, should fighting the drug cartels be limited to law enforcement and political measures that effect a social reform agenda or is this a form of counterinsurgency for which properly trained military geared to special missions should play a key role? Most voices strongly oppose using the military to combat drug trafficking. At its core, their argument rests most importantly on three confluent propositions.

- The Mexican drug war is not an insurgency, terrorism, or low-intensity conflict (LIC), but at most, a “mosaic cartel war” that requires social reform and law enforcement.²⁰

- The military is not well suited for waging this war. Rice University scholar Tony Payan asserts that Mexico's military strategy has produced as many as 100,000 deaths and "let loose on the civilian population the military and, increasingly, a militarized federal police."²¹
- Institutional reforms to clean up Mexico's criminal justice system could provide meaningful social reform plus a better, cohesive collaboration with the United States.

Mexico's drug war presents a different kind of warfare, with different players and political dynamics, for which success requires achieving parallel political and security goals. Characterizing the war turns on whether the drug cartels—sometimes called drug trafficking organizations (DTO) or transnational criminal organizations (TCO)—have a political ideology and seek political power. Both factors apply to the cartels. They espouse an ideology rooted in surprisingly specific stories, narratives, themes, and messages that go well beyond what other groups who are widely accepted as political, such as al-Qaeda, Italy's Red Brigades, Sendero Luminoso (Shining Path) in Peru, Colombia's FARC (Revolutionary Armed Forces of Colombia) and National Liberation Army (Ejército de Liberación Nacional, ELN), or Paraguay's Ejército del Pueblo Paraguayo (EPP) espouse. Those groups embrace the rhetoric of ideology but offer little content to define one. They all seek political power, either to overthrow the existing regime or, as in Mexico, to paralyze and remove the government as a threat to their operations. And they are all criminal.

Even then, the argument that the cartels do not present an insurgency because greed or profit, not a "political" agenda, motivates them is flawed. There is no accepted definition for what constitutes a political agenda. Yale political scientist Harold Lasswell probably came as close as anyone to how politicians view politics: "Politics is who gets what, when, and how."²² Whether parties seek money legally or illegally may affect their status as criminals or law-abiding citizens, but they may easily qualify as criminals and political actors. Most politicians would scoff at the idea that parties whose agenda in the political process is to seek money are not political. Crime and politics are not mutually exclusive.

Cartel Ideology

The notion of what constitutes an ideology lends itself to different expressions. In politics, almost any approach constitutes a belief system, although not all belief systems are ideologies.²³ Broadly, ideology consists of a collection of ideas that define goals, expectations, and actions and express a cohesive basis for thought and behavior. Ideologies exert influence over the beliefs and values that people share, how they see themselves, and how they perceive the world and their place in it. Ideology guides action and influences how people relate to one another. It defines hopes, dreams, and aspirations.

A striking quality about organizations labeled “terrorist” is their substantive lack of ideology. Harvard scholar Louise Richardson has pointed out that terrorist movements do not describe meaningfully the new world they intend to create.²⁴ All terrorist movements, she observes, “have two kinds of goals: short-term organizational objectives and long-term political objectives requiring significant political change.”²⁵ She points out that their political causes have been about changing the status quo, not offering an alternative vision for the future.

Colombian FARC leader Paul Reyes admitted he could not define a ruling program. Tamil Tigers leader Velupillai Prabhakaran’s description of the future was pabulum about a socialist state. Chechen Shamil Basayev said he stood for “power to the people,” whatever that meant. Shining Path’s Abimael Guzmán brushed off questions about his vision for the future, admitting that “we have not studied this question sufficiently.”²⁶ Colombia’s FARC and ELN and Peru’s Shining Path all morphed into criminal entities that finance themselves from drug trafficking, but all claim to fight for a political ideology. Except for regime change, it is hard to discern much content to their views. They do not discuss the exact form of government, health care, education, jobs, or items that define what real political parties or actors offer.²⁷ Al-Qaeda is no different. Richardson observes that in defining his vision, Osama bin Laden was “extremely vague.”²⁸ French scholar Olivier Roy eviscerated bin Laden for his empty rhetoric.²⁹

By contrast, the Mexican drug cartels are remarkably concrete in spinning a story, narrative, theme, and message that hold particular meaning for their targeted audiences. Greed may drive cartels, but what has made them effective is their ability to recruit and mobilize younger, alienated Mexicans through messaging what the cartels offer that the state does

not: social mobility, hope, opportunity, and prosperity. The Mexican drug cartels net a 6,000-percent profit from trafficker to user; counting from the purchase price paid to growers, the business yields an eye-popping 150,000-percent profit.³⁰ In such a lucrative market, cartels easily find a rich source of recruits among impoverished Mexicans, particularly in Juarez assembly plants established in the wake of NAFTA that pay \$200–300 a month. The cartels reportedly can pay teenagers \$5,000 for a single act of violence.³¹

Cartels articulate a story defining themselves as rooted in the romantic nineteenth-century image of a bandito preying upon the rich and a national history in which wealthy Mexicans and foreign investors have controlled much of the economy, leaving most Mexicans impoverished.³² Cartel ballads and music videos stem directly from the Mexican folk tradition of romanticizing revolutionary heroes and legend, except that today's songs glorify drug lords.³³

The songs (*narco-corridos*), videos, social media, signs, and banners (*narcomantas*) present a populist patina that celebrates the humble origins of cartel leaders and their exploits. Ricardo Ainslie points out that this strategic communication has shifted the terrain “for a political left long accustomed to an adversary defined as the nation’s elites and long accustomed to viewing itself as a movement that defended the downtrodden.”³⁴

The narratives help define a specific culture that appeals to teenagers and younger people who the cartels vigorously recruit. It is manifest in the attire: garish cowboy hats, ostrich-skin boots, flashy sneakers, brightly colored baseball hats, tight dresses, gaudy jewelry, lavish homes, fast cars, alcohol, and a glamorous life that offers the best food, beautiful women, and action. The cartels provide a way of life that offers a macho identity and pride for which recruits have no other means of access.³⁵

Writing in *Milenio*, Tijuana writer Heriberto Yépez accurately observed that the cartels have evolved from being an economy to an ideology that saturates society. The term *narco* becomes conflated in “drug trafficker” (*el narco*) and “drug life” (*lo narco*). Yépez argues that *narco* used to be an adjective that described one aspect of Mexican culture. Now it *is* culture: “narco and culture are synonyms.”³⁶ The cartels offer meaning and concrete opportunities that directly influence norms, values, beliefs, attitudes, opinion, and behavior.

The messaging is directed as well to the military. Los Zetas recruits by exploiting the fact that the minimum wage in Mexico is five dollars

a day, unfolding banners—*narcomantas*—asking, “Why be poor? Come work for us.”³⁷ One Zetas banner hanging over a major thoroughfare declared: “Operative Group ‘the Zetas’ wants you soldier or ex-soldier. We offer a good salary, food and benefits for your family. Don’t suffer any more mistreatment and don’t go hungry.” Members of at least one cartel, La Familia Michoacana, now succeeded by the Knights Templar (Caballeros Templarios), view themselves as resistance fighters against crime. They developed expertise in soft power to gain popular credibility.³⁸ They espouse an odd form of Christianity and run drug rehab clinics. The cartel offers jobs and organizes popular protests against the government.³⁹ Of course there is a darker side. The cartels employ directed violence to secure loyalty, extract revenge, send messages, claim turf, and fill power vacuums.⁴⁰ In short, the cartels *do* espouse a political philosophy that meets the hopes and aspirations, as well as playing on the fears, of their targeted audiences.

Seizing Political Power

The cartels also aggressively seek political power. They have succeeded so well that Calderon acknowledged, “This criminal behavior [by cartels] . . . has become a challenge to the state, an attempt to replace the state.”⁴¹ They have created an atmosphere of fear and intimidation that impairs the government’s ability to operate in any normal fashion in providing security or ensuring the welfare of the people. Tactics of intimidation have choked off press freedom.⁴² They have “superseded or seriously weakened” the government in a growing number of Mexican states, even in places becoming a “parallel government.”⁴³ Reportedly, the cartels spend a *billion dollars annually* to bribe police.⁴⁴ They have assassinated political candidates and high-ranking military and law enforcement officials. They engage in campaigns to subvert the Mexican government at all levels.⁴⁵ Their extortion has obstructed commerce.⁴⁶

Los Zetas stands out for why normal law enforcement will not defeat cartels, and drawing lessons, other cartels have stepped up their own capabilities. Recruiting from Mexico’s special operations forces and arming itself with AK-47s, IEDs, RPGs, and 50-caliber machine guns, Los Zetas has trained in small-squad infantry tactics, uses social media adroitly, operates with sophisticated intelligence capabilities, and could easily become an overt insurgency. It will be difficult for a regular police force to tackle this type of militia.⁴⁷ While we disagree with how Paul

Kan characterizes the drug war, we agree with a lot of his ideas on how to address it. His point that any strategy must take on the Zetas first is prescient. Among all the cartels, this one offers the greatest threat of evolving overtly into an antigovernment insurgency movement.⁴⁸ But one should never underestimate the lethality of the others.

Although concerned about the effect of labeling the Mexican drug war an insurgency, Christopher Ljungquist summed up the point that the cartels are political by stating that “the Mexican state is fighting powerful and atypical insurgencies, armed with virtually unlimited access to firearms, including anti-aircraft batteries, and funded by an expert trade in illegal narcotics worth billions of dollars.”⁴⁹ Former secretary of state Hillary Clinton is among those who concur that Mexico faces an insurgency, having declared that the cartels “are showing more and more indices of insurgencies.”⁵⁰

While not writing about Mexico per se, Bard O’Neil and David Kilcullen seem to agree that a confrontation qualifies as insurgency only where it is politically motivated and constitutes a political uprising.⁵¹ The Mexican drug war meets that definition. It is a war tailored for a *new form* of counterinsurgency defined as “an armed struggle for support of the population” that requires a holistic approach and unity of effort to achieve security, drug eradication, social reform, judicial reform, crackdowns on corruption, multinational partnerships with neighbors who the drug war affects directly and indirectly, and special-mission military efforts against heavily armed and trained cartels. It is an iterative, unique approach.⁵²

Not all criminal activity qualifies as insurgency.⁵³ But the Mexican drug war is a low-intensity conflict, and the cartels do qualify as insurgents, hostile combatants, and terrorists. The fact is the lines between crime, terrorism, and insurgency are becoming increasingly blurred. Indeed the US Drug Enforcement Administration (DEA) reports that designated foreign terrorist organizations (FTO) involved in the global drug trade have jumped from 14 groups in 2003 to 18 in 2008.⁵⁴ Therefore, it is imperative the United States, whose vital security interests are linked with Mexico as well as the rest of the hemisphere in managing and prevailing in this conflict, recognize what is happening in Mexico and deal with it realistically.

A Different Approach

We start with two realities. First, Mexico's priorities are to stop violence and kidnapping, while the United States is focused on eliminating kingpins and stopping the flow of drugs.⁵⁵ Until the early 1990s, the drug business in Mexico was relatively peaceful. US citizens suffered, but the situation worked well for Mexicans.⁵⁶ Second, neither side has a strategy for managing or prevailing in this war—a problem complicated by extreme Mexican sensitivity that the United States will intrude upon its sovereignty. Success requires resolving these challenges. While there are no quick fixes, these actions merit consideration:

- Approach the situation as a low-intensity conflict against insurgents who are both criminals and terrorists—and treat them as terrorists. Make no settlement with the cartels. They are in the business in which they want to be. The cartels are an evil, and evil cannot be defeated. It must be eradicated.
- Seize and restrict access to cartel finances. This is pivotal since their wealth gives them exceptional power that must be broken. One challenge the United States confronts is the refusal of the Treasury Department to deal with the reality of the drug war—or counterterrorism—as requiring a combination of law enforcement and special operations. The *Washington Post* reports a proposal by the White House to target cartel assets was declined by Treasury. That mistake must be rectified.⁵⁷ Mexico could deplete cartel bank accounts and seize assets. The United States could provide intelligence and technical support to help locate such assets then defer to Mexico for action. If the United States seized such assets, it should share them with Mexico as an incentive to encourage Mexican cooperation. A key element of this approach lies in disrupting the relationships cartels have with international terror networks.
- Work with the Mexican government to develop a special-mission military force that will avoid human rights violations and work well with civilian authority but that has the expertise and military capability to take on and defeat heavily armed adversaries like Los Zetas. President Nieto is backing away from his suggestion of creating a national gendarmerie. Whatever the force is called, Mexico needs an effective, well-trained special-mission force. Critics worry the cartels will try to subvert and corrupt such a force. Be assured they

will make that effort. But Mexico and the United States must work cooperatively to ensure an effective force is recruited, trained, and retained. Though not an easy task, it should not deter us.

- The United States must persuade Nieto of the value of US assistance, particularly intelligence, surveillance, and reconnaissance. The *Washington Post* reported last April that former president Calderon had granted US spy planes access to Mexican airspace to gather intelligence. US drones supported CBP patrols, and cyber technology was employed to combat trafficking. The *Post* reported the United States was also helping target and vet potential intelligence assets.⁵⁸ In Iraq, Gen Stanley McChrystal forged a task force that accounted for between 11,000 and 13,000 members of al-Qaeda. Their British counterparts accounted for another 3,500.⁵⁹ That was achieved through a fusion team that identified key terrorist leaders and middle-echelon loyalists and eliminated them. US-Mexican fusion centers were established, the *Post* reported, in Mexico City and Monterrey, as well as in regional headquarters. Apparently more limited than McChrystal's task force, this was still a step in the right direction.⁶⁰ Nieto may eschew such help, but we must persuade him to reverse course and make clear that vital US interests are at stake—and we will act accordingly.
- Except for its marines, who have proven relatively effective, Mexico's military should be employed with restraint. Those who argue that most military personnel are not trained for law enforcement have a valid point. Mexico's experience in using its military has produced mixed results, while alienating many Mexicans. The US Marines should continue and step up efforts to work with Mexico's marines through indirect mission assistance in training and equipping.
- Mexican leadership must persuade its population, especially its elites (who arguably have too often helped, not fought, the cartels),⁶¹ middle class, unions, and civil society organizations to support the fight against the cartels—stop kidnapping, extortion, robbery, human trafficking, arms smuggling, and drug trafficking. Calderon failed to lay a solid political foundation for waging the war. Success requires persuading Mexicans their own lives depend on defeating the cartels.⁶² The challenge is difficult, but Nieto must avoid repeating Calderon's mistakes.

- Work with Mexico to develop a joint strategy and support it with the necessary resources. Violence does not affect the entire country. One-third of Mexican states have violence levels similar to the United States. A strategy should focus on the most violent areas; the capital, Mexico City, and the financial center, Monterrey; and tourist areas which contribute heavily to the nation's economy, such as Acapulco, Leon, San Miguel, Cuernavaca, Guadalajara, and Toluca.
- Revamp the Merida Initiative.⁶³ Too much money went to US contractors and too little to Mexicans who could make a difference. Mexico lacks the resources needed to properly implement the institutional and social reforms needed to win this war. This is a long-term challenge, but success requires achieving social justice in Mexico. We can do more to help and we must.
- Forge border management solutions with realistic division of responsibility between the United States and Mexico.
- Abrogate the Brownsville Agreement, which former attorney general Janet Reno entered into in 1998. This agreement lacked foresight in that it compelled the United States to notify the Mexican government of undercover operations in Mexico. That agreement handicapped our law enforcement agencies on any number of fronts without Mexican compromise.
- A hemispheric approach must be reviewed by looking beyond Mexico to our regional neighbors. The drug war threatens Canada as well as Central and South America. Coordinate with Canadian SOF in providing training to Central and South American militaries for counternarcotics and to the military in Guatemala, El Salvador, Honduras, and other Latin allies through SOF assistance to help them develop special-mission capabilities for defeating drug traffickers.

The United States must move beyond defeatist rhetoric suggesting the drug war can only be managed, not won. It can and must be won. But that requires viewing it realistically and taking significant action against the cartels to help Mexico gain control of the strategic situation. While general-purpose military forces are unsuited for winning this conflict, special-mission units are essential to defeat heavily armed, often well-trained cartel forces whose capabilities can overwhelm any normal law

enforcement capability. Mexico lies on our doorstep, and much of what affects its vital interests is entwined with vital US interests. Recognizing that reality is the beginning, and it is time to get moving. **SSQ**

Notes

1. Blog del Narco, *Dying for the Truth: Undercover inside the Mexican Drug War* (Unknown site: Blog del Narco, 2012). The blog is written anonymously by Mexican journalists who conceal their identity to protect against drug cartel violence. The book documents the violence in 2010. Nobody is certain since so few homicides are reported—just 5 percent. The rest is guesswork. During Calderon's presidency, 60,000 deaths are estimated, but another 25,000 persons went missing (not all due to crime). Clare R. Seelke and Kristin Finklea, *U.S.-Mexican Security Cooperation: The Mérida Initiative and Beyond* (Washington: Congressional Research Service [CRS], 12 June 2013), 3, www.fas.org/sgp/crs/row/R41349.pdf; and "Mexican Military Takes Over Drug-Ridden Port," *AFP*, 4 November 2013, <http://www.news24.com/World/News/Mexican-military-takes-over-drug-ridden-port-20131105-3>.
2. William C. Martin, "Cartels, Corruption, Carnage and Cooperation," in *A War That Can't Be Won*, eds. Tony Payan, Kathleen Staudt, and Z. A. Kruszewski (Tucson: University of Arizona Press, 2013), Kindle Loc. 1166/7339.
3. Marcos Pablo Moloeznik, "President Felipe Calderon's Strategy to Combat Organized Crime," in *A War That Can't Be Won*, Kindle Loc. 1728/7339.
4. David A. Shirk, "The Drug War in Mexico: Confronting a Shared Threat," Council on Foreign Relations Special Report no. 60, March 2011, Kindle Loc. 74/933.
5. Paul R. Kan, *Cartels at War* (Washington: Potomac Books, 2012), 74.
6. Michael Kelly, "Mexican Cartels Are Recruiting US Soldiers as Hitmen, And the Pay Is Good," *Business Insider*, 5 August 2013, <http://www.businessinsider.com/cartels-are-recruiting-us-soldiers-as-hitmen-2013-8>.
7. "Mexico's Drug Lords: Kingpin Bowling," *Economist*, 20 October 2012.
8. "Drug Traffickers Have Stranglehold on Guatemala Says Top Prosecutor," *El País*, 23 February 2011; and Hal Brands, *Crime, Violence and the Crisis in Guatemala* (Carlisle Barracks, PA: Strategic Studies Institute, 2010), 2.
9. Adam Elkus, "Gangs, Terrorists and Trade," *Foreign Policy in Focus*, 12 April 2007. Salvadoran gangs in Los Angeles founded MS-13.
10. Strategic Forecasting, Inc. (Stratfor), *Mexico in Crisis: Lost Borders and the Struggle for Regional Status* (Austin, TX: Stratfor, 2009), 197.
11. See Gregory E. Maggs, "Assessing the Legality of Counterterrorism Measures without Characterizing Them as Law Enforcement or Military Action," 80 Temp. L. Rev., 661 (2007), 3 (online copy), http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1826&context=faculty_publications.
12. See *Tennessee v. Garner*, 471 U.S. 1, 11 (1985); US Army Field Manual (FM) 27-10, *The Law of Land Warfare*, 1956, chap. 2, sec. II, para. 29, citing annex to Hague Convention no. IV, 18 October 1907, embodying the Regulations Respecting the Laws and Customs of War on Land, art. 23(c); and Maggs, "Assessing the Legality of Counterterrorism," 4. See also Jimmy Gurule and Geoffrey S. Corn, *Principles of Counter-Terrorism Law* (St. Paul: West Group, 2010), 65; Army FM 6-20-10, *Tactics, Techniques and Procedures for the Targeting Process*, 8 May 1996, chap. 2. See generally "Protocol Additional to the Geneva Conventions of August 12, 1949 and relating to the Protections of Victims of International Armed Conflicts (1977), 1125 UNTS 3 (entered into force 7 December 1978)"; and "Protocol Additional to the Geneva Conventions of August 12, 1949 and relating to the Protection of Victims of Non-International Armed Conflicts (1977), 1125 UNTS 609 (entered into force 7 December 1978)."

13. The Authorization to Use Military Force passed by Congress on 14 September 2001, P. L. 107-40, authorizes “all necessary and appropriate force” against persons who aided organizations involved in the 9/11 attacks “to prevent any future acts of international terrorism against the United States.”

14. Kan quotes from Michael Roth and Murat Sever, “The Kurdish Workers Party (PKK) as Criminal Syndicate: Funding Terrorism through Organized Crime,” *Studies in Conflict and Terrorism* 30 (October 2007): 903, to state that cartels are “(1) involved in illegal activities and frequently need the same supplies; (2) exploit excessive violence and the threat of violence; (3) commit kidnappings, assassinations and extortion; (4) act in secrecy; (5) challenge the state and the laws (unless they are state funded); (6) have back-up leaders and foot soldiers; (7) are exceedingly adaptable, open to innovations, and are flexible and (8) enact deadly consequences for former members who have quit the group.”

15. Kan, *Cartels at War*, 6–13.

16. Brad Freden, “The COIN Approach to Cartels: Square Peg in a Round Hole,” *Small Wars Journal*, 27 December 2011, <http://smallwarsjournal.com/jrn/art/the-coin-approach-to-mexican-drug-cartels-square-peg-in-a-round-hole>. Freden concedes, however, that some COIN principles and practices can support a law enforcement strategy to weaken or destroy the cartels.

17. Shibley Telhami, *The Stakes* (Boulder, CO: Westview Press, 2002), 35. Telhami’s focus is on distinguishing between hostile or enemy forces and terrorists. For example, he points out that while the United States deems Hezbollah a terrorist organization, other parties, especially in the Middle East, do not, viewing it as a political or religious movement; and *Ibid.*, 9.

18. See Juan Zarate, *Treasury’s War: The Unleashing of a New Era of Financial Warfare* (New York: Public Affairs, 2013).

19. Kan, *Cartels at War*, 8.

20. *Ibid.*, 7; See also Payan, Staudt, and Kruszewski, eds., *A War That Can’t Be Won*.

21. Tony Payan, “The Many Labyrinths of Illegal Drug Policy,” in *A War That Can’t Be Won*, Kindle Loc. 352/7339.

22. Harold D. Lasswell, *Politics: Who Gets What, When and How* (Gloucester, MA: Peter Smith Publishing, 1990).

23. Maurice Cranston, “Ideology,” *Encyclopedia Britannica*, <http://www.compilerpress.ca/Competitiveness/Anno/Anno%20Cranston%20Ideology%20EB%2003.htm>. The French philosopher Destutt de Tracy expounded affirmative characteristics. Karl Marx saw ideology as a set of beliefs with which people deceive themselves—a theory that expressed what they are led to think as opposed to that which is true. *Ibid.*

24. Louise Richardson, *What Terrorists Want* (New York: Random House, 2006), 85.

25. *Ibid.*, 75. She discusses various motives that animate terrorist organizations, including revenge, publicity, seeking concessions, causing disorder, provoking repression, making a show of strength.

26. *Ibid.*, 86–87.

27. W. Alex Sanchez, “The End of Ideologically Motivated Violent Movements in Latin America?” *e-International Relations*, 24 September 2012, www.e-ir.info/2012/09/24/the-end-of-ideologically-motivated-violent-movements-in-latin-america/. Sanchez also falls into the trap of conventional definitions in failing to recognize that profiting from illegal activity can qualify as both a criminal and political agenda, although one does not necessarily imply the other.

28. Richardson, *What Terrorists Want*, 86.

29. Olivier Roy, trans. Carol Volk, *The Failure of Political Islam* (Cambridge: Harvard University Press, 1994). Roy argues persuasively that political Islam has failed to define a concrete vision and, to the extent that one has been, it bears a closer resemblance to radical leftwing politicians than religion.

30. Ioan Grillo, *El Narco*, (London: Bloomsbury Press, 2011), Kindle Loc. 2747/6409.

31. “Teens Lured into Mexican Drug Cartels,” *Big Country* (Nexstar Broadcasting, Inc.), 19 April 2009, www.bigcountryhomepage.com/story/teens-lured-into-mexican-drug-cartels/d/story/cSPztt2XMEW2GeUVZ-XmRQ.

32. Watt and Zepeda, *Drug War in Mexico*.

33. Sylvia Longmire, *Cartel* (New York: Palgrave MacMillan, 2011), 102.
34. Ricardo C. Ainslie, *The Fight to Save Juarez* (Austin: University of Texas Press, 2013), Kindle Loc. 4206/6219.
35. Grillo, *El Narco*.
36. Quoted in Josh Kun, "Death Rattle," *American Prospect*, 5 January 2012, <http://prospect.org/article/death-rattle>.
37. Ashley Fantz, "The Mexico Drug War: Bodies for Billions," *CNN.com*, 20 January 2012, <http://www.cnn.com/2012/01/15/world/mexico-drug-war-essay/index.html>.
38. Kan, *Cartels at War*, 43–45; and Akbar Khan, "The War on Drugs: Mexican Cartels," *Generation.net*, 29 May 2013, <http://the-generation.net/the-war-on-drugs-mexican-cartels/>. Kan quotes one observer who calls La Familia Michoacana a "faith-based, right-wing populist socialist movement" run by a criminal organization.
39. Tim Padgett and Ioan Grillo, "Mexico's Meth Warriors," *Time*, 28 June 2010, <http://content.time.com/time/magazine/article/0,9171,1997449,00.html>; and William Finnegan, "Silver or Lead," *New Yorker*, 31 May 2010, www.newyorker.com/reporting/2010/05/31/100531fa_fact_finnegan?currentPage=all.
40. Kan, *Cartels at War*, chap. 2, well describes the business plan that cartels employ.
41. Payan, "Many Labyrinths of Illegal Drug Policy."
42. Blog del Narco, *Dying for the Truth*; Oscar Villalon, ed., *Blood Calls to Blood: Mexican Writers on the Drug War* (San Francisco: By Liner, 2012); Alfredo Corchado, *Midnight in Mexico: A Reporter's Journey Through a Country's Descent into Darkness* (New York: Penguin Press, 2013); Ainslie, *Fight to Save Juarez*; and Guadalupe Correa-Cabrera and Jose Nava, "Drug Wars, Social Networks and the Right to Information," in *A War That Can't Be Won*.
43. Payan, "Many Labyrinths of Illegal Drug Policy." See also Ed Vulliamy, *Amexica: War along the Borderline* (Farrar, Strauss & Giroux, 2010), 246. Shawn Teresa Flanigan has drawn interesting parallels between the Mexican drug cartels and Hamas and Hezbollah. All are tied to relatively defined geographic locations. All seek to control specific territory to maintain access to drug trade routes. All have deep, sophisticated relationships with the states within which they operate. See Flanigan, "Terrorists Next Door? A Comparison of Mexican Drug Cartels and Middle Eastern Terrorist Organizations," *Terrorism and Political Violence* 24, no. 2 (2012): 279–94.
44. Payan, "Many Labyrinths of Illegal Drug Policy."
45. Ainslie's *Fight to Save Juarez* offers a riveting account of the bloodbath that cartel violence has inflicted on that city. It is an excellent study of how Mexico's government has failed to cope. See also George W. Grayson, *Mexico: Narco-Violence and a Failed State?* (New Brunswick, NJ: Transaction Publishers, 2009). There is wide reporting on the corruption problem.
46. See Vulliamy, *Amexica*, 247. He goes into great detail about the extortion practiced among even small businesspeople.
47. George W. Grayson and Samuel Logan, *The Executioner's Men* (New Brunswick: Transaction Publishers, 2012); and Longmire, *Cartel*.
48. Kan, *Cartels at War*, 150–51.
49. Christopher S. Ljungquist, "Mexican Cartel War: Profiling an Unorthodox Insurgency," *Geopolitical Monitor*, 4 February 2013, <http://www.geopoliticalmonitor.com/mexican-cartel-war-profiling-an-unorthodox-insurgency-4777>.
50. "Clinton Says Mexico Drug Crime like an Insurgency," *BBC News*, 9 September 2010, <http://www.bbc.co.uk/news/world-us-canada-11234058>.
51. Bard O'Neil, *Insurgency and Terrorism: From Revolution to Apocalypse*, 2nd ed. (Washington: Potomac Books, 2005); and David J. Kilcullen, "Three Pillars of Counterinsurgency," remarks delivered to the US Government Counterinsurgency Conference in Washington, DC, 28 September 2006, both cited in Freden, "COIN Approach to Mexican Drug Cartels."
52. Army FM 3-24.2, *Tactics in Counterinsurgency*, April 2009, <https://www.fas.org/irp/doddir/army/fm3-24-2.pdf>.

53. Terrorist organizations and criminal groups may have peripheral connections (arguably, al-Qaeda). Terrorist organizations may have criminal sympathizers (arguably, Hezbollah). Criminal entrepreneurs may act as specialists or shadow facilitators for terrorist groups (arguably, Viktor Bout, Abu Ghadiyah, Monzer al-Kassar). Terrorists groups and criminals organizations may collude (arguably, the Taliban and drug traffickers). See <http://fpc.state.gov/documents/organization/141615.pdf>.

54. Statements by Stephen W. Casteel (DEA) and Raphael Perl (CRS), "Narco-Terrorism: International Drug Trafficking and Terrorism—A Dangerous Mix," prepared for a hearing conducted by the Senate Judiciary Committee, 20 May 2003; and Michael Braun, "Drug Trafficking and Middle Eastern Terrorist Groups: A Growing Nexus?" speech at the Washington Institute for Near East Policy, 18 July 2008. The CRS observes that the US government lacks a strategy or policy to address comprehensively the confluence of terrorism and transnational crime. John Rollins and Liana S. Wyler, *International Terrorism and Transnational Crime: Security Threats, U.S. Policy and Considerations for Congress* (Washington: CRS, 18 March 2010), 4.

55. Dana Priest, "U.S. Role at a Crossroads in Mexico's Intelligence War on the Cartels," *Washington Post*, 27 April 2013, http://www.washingtonpost.com/investigations/us-role-at-a-crossroads-in-mexicos-intelligence-war-on-the-cartels/2013/04/27/b578b3ba-a3b3-11e2-be47-b44febada3a8_story.html.

56. See Pamela F. Izaguirre, "Narco-Politics: How Mexico Got There and How It Can Get Out," *Council on Hemispheric Affairs*, 22 August 2013, www.coha.org/narco-politics-how-mexico-got-there-and-how-it-can-get-out/.

57. Priest, "U.S. Role at a Crossroads."

58. Ibid.

59. Mark Urban, *Task Force Black* (Little, Brown, & Co., 2011).

60. Priest, "U.S. Role at a Crossroads."

61. Watt and Zepeda, *Drug War in Mexico*.

62. See James P. Farwell, *Persuasion and Power: The Art of Strategic Communication* (Washington: Georgetown University Press, 2012); and Longmire, *Cartel*. Longmire presents an excellent description of those challenges and how Calderon perceived and addressed them.

63. Seelke and Finklea, *U.S.-Mexican Security Cooperation*, 3. See also Craig A. Deare, "U.S.-Mexico Defense Relations: An Incompatible Interface," Strategic Forum, Institute for National Strategic Studies, National Defense University, July 2009; and Statement of Assistant Secretary of State for International Narcotics and Law Enforcement Affairs William Brownfield, US House Committee on Foreign Affairs, Subcommittee on the Western Hemisphere, "U.S.-Mexico Security Cooperation: An Overview of the Merida Initiative 2008–Present," 113th Cong., 1st sess., *CQ Congressional Transcripts*, 23 May 2013.

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.

Toward Attaining Cyber Dominance

Martin R. Stytz

Sheila B. Banks

It's not what you don't know that kills you; it's what you know for sure that ain't true.

—Mark Twain

Achieving global cyber superiority or global cyber control by any organization is no longer technically possible. Instead, the proper overarching objective should be dominance of one or more of the elements of cyberspace of most importance to the organization at any given time.¹ The successful nation is the one that achieves and maintains strategic and tactical dominance in its critical elements of cyberspace when required.² Two important questions related to the strategic aspects of cyber conflict are: what should be the basic technological building block(s) for strategic cyber defense to assure dominance of one's own critical elements of cyberspace, and what are the classes of strategic data target(s) strategic cyber defense must protect?

Strategic cyber conflict enables surprise, shock, and confusion to be inflicted upon an adversary at the time of the attacker's choosing, in a manner of the attacker's choosing, and in a manner that exploits the adversaries' decision-making biases. *Strategic offensive cyber dominance* exploits adversary biases by a combination of data exfiltration and manipulation to lead adversaries to make decisions that we want them to make. It undercuts the opponents' effective decision making and mission command. Strategic cyber offensive targeting should be based upon the desired effects on the data and decision processes of the opponent and not

Retired lieutenant colonel Martin R. Stytz is the Collegiate Professor for Cybersecurity at the University of Maryland and associate research professor at Georgetown University. He received a BS degree from the Air Force Academy in 1975, an MA from the University of Central Missouri, an MS from the University of Michigan, and a PhD in computer science and engineering from the University of Michigan in 1989. His research interests include distributed simulation, software protection, and cyber security.

Dr. Sheila B. Banks is president of Calculated Insight. She received her BS from the University of Miami in 1984, a BSEE and MS in electrical and computer engineering in 1987 from North Carolina State, and her PhD in computer engineering (artificial intelligence) from Clemson University in 1995. Her research interests include artificial intelligence, human behavior and cognitive modeling, and cyber security.

upon the material damage that may, or may not, be inflicted. Conversely, *strategic defensive cyber dominance* enables effective decision making for one's own side. It ensures accurate, trustworthy, relevant data is provided to friendly decision makers. The vast amount of open-source cyber-attack literature demonstrates that no combination of tactical cyber defense technologies is impervious. Therefore, one's own systems and decision makers must be prepared technologically and psychologically to function despite strategic cyber attacks designed to undermine situational awareness (SA), decision-making ability, and mission command by attacking their data and other elements of cyberspace.

Strategic cyber defense dominance arises from a combination of tactical cyber defense technologies, a resilient cyber defense system architecture, and decision-maker preparation for psychological effects of a strategic cyber attack. Technologically, a resilient strategic cyber defense should be based on an active, dynamic layered cyber defense (DLCD). Strategic cyber defense preparation requires training decision makers via exposure to the effects of cyber attacks so they can surmount the challenges posed by a strategic cyber attack. Because of the obvious dangers posed by training using cyber attacks in the real world, the decision-maker training venue must be a simulation environment. The DLCD, situational awareness, and decision-support approach we describe complements the joint information environment (JIE) or similar dataflow architectures and their cyber defenses.

This article addresses strategic cyber dominance, with a focus on strategic cyber defense. It contains a background discussion on strategic cyberspace and situational awareness while examining the active DLCD concept.³ The article also presents an approach to strategic cyber defense training and simulation to prepare decision makers for the data uncertainties and confusion that will occur in a cyber conflict.

Strategic Versus Tactical Cyberspace

Strategic cyber warfare is a contest for access, control, use, and manipulation of the opponents' data coupled with protection and confident use of your own data. In contrast, the offensive tactical level of cyber warfare comprises the technologies used to penetrate opponents' cyber defenses and technologies to exfiltrate, alter, or manipulate their data. Examples of tactical offensive cyber warfare technologies are

worms, viruses, botnets, port scanners, Trojans, backdoors, and social engineering attacks (like phishing). We use the term *malware* to denote all offensive tactical cyber warfare technologies. The defensive tactical level of cyber warfare concerns the technologies used to protect one's systems and data. Examples of technologies used for defensive tactical cyber warfare purposes are encryption, firewalls, onion routing, air-gapped networks, biometric logon, and address space randomization. We differentiate between tactical and strategic cyber operations to highlight the difference between the tactical struggle to control access to systems and their data and the struggle to access and control cyberspace elements to achieve strategic objectives. Tactical cyber conflict is dominated by technological considerations; strategic cyber conflict is dominated by data, SA, and decision-making considerations. We contend that any physical effects of tactical-level cyber activities, while important, are also irrelevant at the strategic cyber warfare level.

Cyber conflict is different from information operations. Information operations can be executed by a number of technologies, even humans, whereas the data alterations achievable in a cyber conflict are unique, of greater scope, adaptable, and more rapid than in information operations. Therefore, we consider cyberspace technology as a capability that is distinct from information operations. As noted above, the challenges faced by the strategic cyber defender are increasing, and there is little prospect for achieving complete trustworthiness for any portion of a defender's cyberspace short of complete isolation from the Internet (which obviously negates the utility of that set of the defender's cyber systems).⁴ There are several clear causes for the severity and scope of the tactical cyber defense challenge. First, blended tactical cyber attacks are becoming more commonplace and should be expected. Tactical cyber attacks commonly employ cross-channel, cross-domain, and cross-functional components, thereby both significantly increasing the complexity of the tactical cyber attack and the difficulty of detecting or defending against it. Second, while defenses against known tactical cyber attacks are necessary, they are not sufficient to ensure a successful tactical cyber defense because new attack technologies are always under development. As a result, tactical cyber defenses cannot expect to repel or mitigate every attack. Complicating the problem is the existence of an unknown number of zero-day attacks. Third, cyber adversary resources are increasing due to nation-state involvement and criminal involvement, which accelerate the

rate of advance in cyber-attack technologies. Fourth, computer and network technology advancements have traditionally favored tactical cyber attack, which undermines the ability of cyber defenses to repel or mitigate such an attack. Finally, tactical cyber standards compliance does not guarantee cyber security or even effective tactical cyber defense but does increase its costs. For these reasons, cyber defenders should expect their tactical defenses to be breached, they should expect breaches to be increasingly difficult to detect, and they should be prepared to operate successfully despite a successful breach while also recovering from and sealing the breach.

Despite the challenges posed by the adversary's strategic cyber-attack objectives and tactical cyber attacks, strategic cyber defense must endeavor to secure the cyberspace elements vital to the current decision-making context. The approach used to secure these elements is the cyber defense strategy; typically a cyber defense strategy is static or changes slowly on a human time scale. A decrease in trust or a delay in delivery of a crucial cyberspace element or component of an element is a strategic cyber defense "loss." Specifically, the strategic cyber defense loses if the attacker can (1) retard the delivery of cyberspace elements or components needed for critical decisions, (2) reduce the velocity of dataflow in the defender's cyber systems, (3) force the use of outdated/outmoded equipment or systems to secure cyberspace elements or components, (4) impede the exchange of cyberspace elements or components among the defenders, or (5) retard improvements or adoption of cyberspace technologies. Clearly, cyber attackers will attempt to increase their capabilities in all five areas. Of critical importance during a cyber attack is that not all elements of cyberspace or components of each element are of equal value *and* the value of each element or component varies over time due to changes in the decision context. Decision context alone determines element importance. Because element value varies, the key question for the strategic cyber defender is which of the five areas are crucial to the strategic attacker's success and which are crucial to strategic cyber defense. Cyberspace element priorities, and therefore cyber defense resource allocation, must change as circumstances and decision context change. We contend that the cyber defense strategy should also change as rapidly.

To respond rapidly to changes in cyberspace element priorities, strategic cyber defenses must be able to dynamically, seamlessly, and stealthily

change to improve the defenses for the cyber elements and components that have the greatest value and importance at any given time. However, changes in the defense strategy or tactics undertaken to increase protection for crucial elements or components must not sacrifice lower-value elements or components (obviously, an element's value may increase in the next decision context.) Instead, the higher-value elements and components must be provided with additional protection(s) while preserving the value of components and elements not under attack or of less importance in the current decision context. The foundation for these capabilities rests upon DLCD and its ability to support rapid changes in cyber-defense strategy and tactics.

Executing an effective strategic cyber attack upon an important strategic and tactical target is not a technologically simple undertaking. A successful strategic or tactical cyber attack requires a high degree of technical sophistication, patience, and a deep, thorough understanding of computing technologies, human cognition, decision making, and individual and group situational awareness development. Perversely, cyber attackers need not possess these technological abilities; they can be purchased from people who do have them. However acquired, technological advances are enabling attacks not previously possible as well as increasing the likelihood of success of known types of tactical cyber attacks, which has resulted in an increased ability to target specific elements of cyberspace.⁵ The challenges posed by increasingly capable malware are both compounded and offset by the widespread use of virtual machine (VM) and cloud computing technologies.⁶ Cyber attackers have, and likely will retain, the tactical technical advantage and the initiative requiring that we assume that all cyberspace elements are at risk. Recent technological developments demonstrated by the Stuxnet, Bluepill, Flame, and Conficker tactical cyber attacks indicate the likely character of future attacks as well as their likely consequences upon decision makers.

Stuxnet highlighted the challenges faced by strategic cyber defense. It apparently only activated if the infiltrated system was one of its targets. In a targeted system, it proceeded to alter the software at the target and to search for new targets from within the system. Humans or computer systems did not direct or manage the Stuxnet campaign. Instead, the Stuxnet software autonomously conducted the cyber attack. The same degree of autonomy must be expected to occur in the future. Of greater concern is the primacy of cyber elements, especially data, over physical

systems as illustrated by the Stuxnet attack. Tactically, Stuxnet altered the performance of the targeted centrifuges; however, its success was critically dependent upon its capability to alter data. Stuxnet altered the centrifuge performance data available to human decision makers; the human operators believed that centrifuge performance was correct. Without this key cyber-element tampering capability, the Stuxnet cyber attack would have been easily detected and would have failed.

Clearly, future cyber attacks will target systems in a more sophisticated manner than Stuxnet or Flame. They will transmit data from the targets and/or subtly modify the data to corrupt it in a malicious but not immediately apparent manner. We expect that future cyber attacks will be structured to introduce false information, to target specific individuals as well as systems for information degradation, and to precisely corrupt information that reaches decision makers within ongoing cyber campaigns of tactical and strategic significance. Cyber attacks will be coordinated and mounted in campaigns designed to maximize confusion and maximally, automatically exploit tactical and strategic successes.

As Conficker demonstrated, the technology exists to create a cyber weapon consisting of millions of computer systems and maintain command and control of that weapon despite changes to tactical cyber defenses during the tactical cyber attack. Stuxnet demonstrated the technology for a cyber weapon that behaves like a “smart munition” due to its capability to alter, damage, or destroy specific data on specific physical systems. Eventually, nations will possess cyber arsenals containing a variety of these and other classes of controlled, precision cyber weapons as well as broad cyber-attack weapons. We should expect that cyber campaigns will employ a wide variety of malware that operates cooperatively and strategically to disorient and confuse decision makers, delay decisions, and lead decision makers to incorrect conclusions and poor decisions without being aware the information they are using is corrupted. Despite the clear and increasing cyber threat, scant attention has been devoted to either decision making or strategic cyber defense training during a cyber attack when decision-critical portions of cyberspace have been compromised. We can prepare for and to some degree prevent the disruption caused by a strategic cyber attack by exposing decision makers to simulated strategic cyber attacks as well as by pursuing new strategic defense technologies with the intent of improving decision maker situational awareness during cyber attacks.

Situational Awareness

The unique peril posed by cyber attacks arises from the use of information technologies, including computers, software, networks, and sensors in the network-centric warfare (NCW)/data-centric warfare (DCW) paradigm.⁷ NCW/DCW leverages data and the other elements of cyberspace to improve operational performance and outcomes. The improvements in shared situational awareness and group decision making provided by NCW/DCW capabilities reduce information uncertainty between and among decision makers.⁸ These two significant advantages provide a detailed, shared, composite insight into the state of the conflict. The cyberspace elements that support NCW/DCW are the only way to achieve the timely, accurate decisions needed in current and future cyber conflicts. A strategic cyber attack undermines the data and other cyberspace elements used for decision making and impairs development of individual and group situational awareness. The vulnerabilities exploited by a tactical cyber attack in support of a strategic cyber attack are inherent to the technologies used to achieve the advantages provided by modern cyberspace technologies. The advantages offered by cyberspace technologies make them profitable targets. A strategic cyber attack can prevent valuable data from reaching decision makers, corrupt decision-relevant data, corrupt decision-support systems, and corrupt the other elements of cyberspace. However, it is not the corruption of the cyberspace elements that is a concern; it is the corruption of decision making. The rise of modern computing and networking technologies has given rise to the expectation that correct individual and shared situational awareness will develop and facilitate decision making. The rapid acquisition of individual and group situational awareness can enable a faster, coherent response to evolving circumstances. A strategic cyber attack adversely affects group and individual situational awareness.

Situational awareness is the result of a dynamic process of perceiving and comprehending events in an environment.⁹ It enables reasonable projections of how the environment may change and permits predictions concerning future circumstances and outcomes. The process (see fig.1) bears some similarity to Col John Boyd's observe-orient-decide-act (OODA) loop formulation for situational awareness.¹⁰ The components of the process are not stages, but instead are interlocking cycles that progress in relation to each other using an action progression schema. The factors promoting individual SA are both structural and situational.

Structural factors include background, training, experience, personality, interests, and skill. Situational factors include the mission that is being performed and the circumstances at the time of the mission. Structure and situational factors affect situational awareness as illustrated in figure 2.

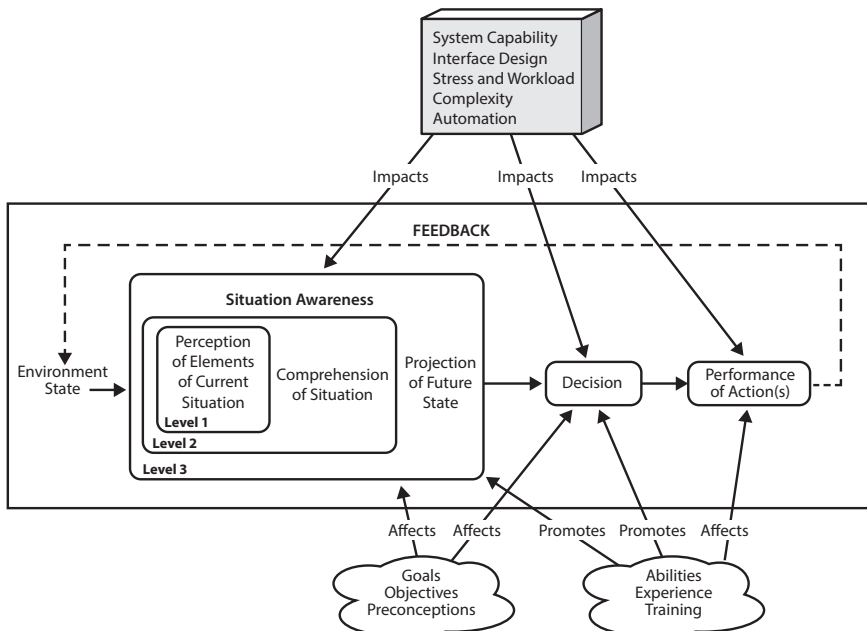


Figure 1. The situation awareness cycle

(Adapted from Mica Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors* 37, no. 1 [1995])

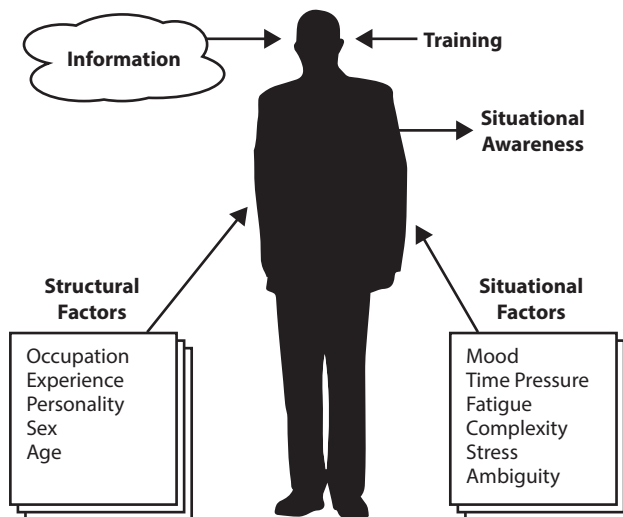


Figure 2. Situation awareness formation

Shared (or group) SA can be defined as a common relevant mental model of an environment or as the degree to which an individual's perception of the environment mirrors the same situation as perceived by others in the group. Achieving shared SA benefits from cyberspace dominance and an interoperable information representation, both of which demand an effective strategic and tactical cyber defense. Group SA ensures that a clear and accurate, common, relevant picture of the situation is possessed by leaders at all levels. Shared situational awareness requires a common comprehension of relevant policy and strategy as well as the state of operations, technology, logistics, tactics, plans, command structure, personalities, and readiness posture.

There are many factors that are known to degrade shared SA across a group: (1) false group mind-set, (2) the "press on regardless" mind-set (allowing mission accomplishment to affect objective assessment), (3) insufficient training/variable skill levels, (4) poor personal communications skills, (5) perception conflicts, (6) frequent changes in personnel, (7) degraded operating conditions, (8) lack of a common set of information across a group, and (9) the absence of nonverbal cues. In general, physically distributed workers have poorer shared SA than do collocated workers, a problem that is exacerbated by the tendency to rarely discuss contextual information among distributed workers.¹¹ A modern, well-planned strategic cyber attack will assuredly target and undercut both individual and shared SA by magnifying the impact of one or more factors that degrade both. In light of these and other foreseeable developments in tactical cyber-attack capabilities, we suggest that the current *static defense-in-depth* best practice for tactical cyber defense is becoming outmoded and unviable in the face of foreseeable tactical cyber-attack capabilities. To enable an effective, flexible strategic cyber defense, a transition to a tactical cyber defense based upon an *active, dynamic layered cyber defense-in-depth* is necessary.

Diminishing Cyber-Attack Effectiveness through DLCD

Dynamic layered cyber defense-in-depth requires active tactical cyber defense of data and other cyberspace elements in a manner that provides rapid and robust response to a cyber attack by isolating the infected systems as they are detected and augmenting the tactical cyber defense of

uninfected systems to prevent the spread of the malware infestation and to preserve cyberspace elements' value. The key to deploying effective, mutually supportive, and coherent dynamic, active defense-in-depth lies in continuous, rapid analysis of the status and quality of the protection for cyberspace elements and systems and using the resulting evaluation to immediately alter and improve tactical cyber defenses for the targeted data and systems. However, since there can and will undoubtedly be multiple infestations and multiple cyber-attack campaigns mounted at the same time, the ability to successfully wall off multiple infestations and deploy multiple, independent defensive rings around uninfested cyberspace elements (and their components) are needed. Data valuation and cyber-attack categorization are essential to the success of this approach because the value of the threatened data should determine the resources dynamically devoted to cyber element's defense.

Fundamentally, every cyber attack has as its primary objective control of the defender's cyberspace elements (typically data) by either the execution of the attacker's computer instructions upon the defender's computational resource(s) or the execution of the defender's high-privileged instructions upon the defender's computational resource(s) using parameters chosen by the cyber attacker. We can restate these objectives as either executing attacker's instructions upon the defender's computer's "bare metal" or executing privileged defender system commands using the attacker's input values. Logically, the primary objective of the tactical cyber defense must be to prevent achievement of both objectives. In practice this has been difficult for the tactical cyber defense due to the traditional emphasis placed upon computational throughput and efficiency and the resulting reliance upon perimeter tactical cyber defenses. The emphasis has become self-defeating, because it enables tactical cyber-attack success, promotes strategic cyber-attack success, and leaves the defender vulnerable to poor situational awareness and the inevitable surprises that are a consequence of poor SA.

Strategic cyber defense should have as its objectives preventing penetration of the tactical cyber defenses, and in the event of penetration, preventing the attacker from determining the cyber terrain, preventing the attacker's malware from executing, and if the malware executes, preventing it from accessing its target and/or communicating. While these objectives are pursued somewhat in current tactical cyber-defense technologies, the first objective listed receives the greatest emphasis, and

a successful penetration usually results in a successful cyber attack. The strategic cyber defensive need is to dramatically increase the ability to achieve these objectives while maintaining flexibility and robustness in response to a cyber attack.

Because any static layered tactical cyber defense can be defeated, a DLCD must be able to change any aspect of its configuration at any time. By doing so, a DLCD (1) makes defeating a tactical cyber defense configuration as difficult as possible, (2) provides cyber defenders with a tactical cyber defense environment whose defenses can be dynamically altered, (3) provides the cyber defenders with tools for rapid detection of tactical cyber attacks, (4) enables cyber defenders to successfully operate despite a breach in tactical cyber defenses, (5) provides an environment that enables rapid recovery from tactical cyber penetration and compromise, and (6) eliminates any advantage a tactical cyber attacker may have due to transitory knowledge of some aspect of the tactical cyber defenses.¹² To complement these objectives, we rely on principles of cyber security,¹³ employ state-of-the-art tactical cyber security technologies, and require a means for identifying, modeling, and prioritizing the key components of each element of cyberspace in any decision context.

Current strategic and tactical cyber-defense technologies give the defender control of the cyber terrain, allowing the cyber defense to determine the conditions of engagement in a cyber attack. Some current tactical cyber-defense technologies, like application control and address space randomization, can be effective in preventing some unauthorized applications from executing and in preventing access to some dangerous URLs, but current tactical cyber defense technologies are static and not completely effective. DLCD appears to be more promising and effective. Using DLCD, the cyber defender can erect an ever-varying maze of tactical cyber defenses based on virtual machines, each with a different combination of properties and operational characteristics that serve to complicate the tactical cyber-attackers' challenge. Examples of the tactical cyber defenders' control include but are not limited to halting computing processes, migrating computational processes from a compromised computational environment to a secure one, changing network communications ports and addresses, changing M2M authentication codes and encryption keys, changing virtual machine configuration and nesting, purging software, engaging additional firewalls, altering firewall properties, altering applications, altering authentication protocols, and/

or disconnecting portions of the defended system from the Internet. The challenge posed to the tactical cyber attacker can be further complicated if the cyber defender feeds false information concerning the state of the tactical cyber attack back to the cyber attacker, which can be very effective because the cyber attacker almost always lacks a noncyber information channel to ascertain the accuracy of the information.

Nevertheless, as of this writing, tactical cyber defensive changes must be implemented before, not during, the cyber engagement, thereby forfeiting a tremendous advantage possessed by the tactical cyber defense. Altering the tactical cyber defense during the attack as well as controlling the tactical cyber-attack information received by the attacker would amplify the tactical cyber defense's advantages and diminish the effectiveness of the tactical cyber attack, which is the reason for the use of DLCD. The layers in DLCD do not correspond to layers of security but rather to layers of independent virtual machines that an attacker must navigate to penetrate a system and to exploit a successful tactical cyber attack. Diminishing the effectiveness and ease of tactical cyber attacks minimizes the opportunity for surprise, minimizes the exploitation of surprise, and improves protection and employment of the four elements of cyberspace by the cyber defense. Altering the cyber terrain by using DLCD complicates the tactical cyber attackers' ability to assess the progress of the attack and decreases their ability to achieve attack objective(s). By increasing the rate at which the cyber terrain changes using DLCD, the tactical cyber defense could force the attacker to adapt so frequently and to be so uncertain of the information coming back that the tactical cyber attack's chances for success significantly diminish. In the next section we further discuss DLCD operation.

Active Cyber Defense

Traditionally, the principles for securing cyber systems include (1) the system must be substantially undecipherable, (2) the system must not require secrecy and can be stolen by the enemy without causing trouble, (3) the system must be easy to change or modify at the discretion of the correspondents, and (4) the system must be easy to use and must neither stress the mind nor require the knowledge of a long series of rules. These principles have been employed to a degree since the earliest research in computer security.¹⁴ In the cyber-security systems context,

these principles demand (1) the tactical cyber attacker cannot determine the tactical cyber defenses before or during the cyber attack, (2) possession of a system that implements the tactical cyber defenses provides no insight into the tactical cyber defense configurations of similar systems, (3) the tactical cyber defenses must be easy to change at any time by the cyber defenders, and (4) the tactical cyber defenses are essentially invisible to people that have no cyber-security responsibilities. The need for dramatic improvement in tactical cyber defense points to the need for DLCD. DLCD implements the principles by being architected and designed to isolate malware infestations, complicate the tactical cyber attacker's perspective of the cyber terrain, and maintain sufficient, accurate, and trustworthy cyberspace elements despite attack. This approach differs from current tactical cyber-defense attempts in its extreme emphasis on the four principles as the foremost property and requirement for the cyber system without regard for their impact on system performance.

DLCD also emphasizes the importance of three additional desirable properties of a cyber system: maximizing information velocity within the system when it is under attack, maximizing the objective reasons for user trust of the system and its data, and maximizing the ability of the cyber system to modify tactical cyber defenses by either increasing or decreasing their complexity and security properties. The change in properties is based upon the importance of the information being processed by the system in relation to the current decision-making context. By prioritizing the security of the cyber system, we enable the attainment of these three additional properties.

In DLCD, the outermost layer of the tactical cyber defense has access to the computing hardware; each additional nested layer further isolates the hardware from the cyberspace component, and vice-versa. The innermost layer of the DLCD defense encloses the component. Because software probes are used to instrument the operation and performance of each layer, DLCD can give decision makers sufficient time and information to recognize and counteract a cyber attack. DLCD also allows the cyber defenders to alter tactical cyber-defense complexity and configuration at any time, which further complicates the challenges posed to an attacker. We contend that human oversight and judgment is crucial to the operation of DLCD and for insuring that a cyber attacker does not trigger tactical cyber-defense responses that squander resources. As a result, while some responses in the tactical cyber defense

must be automatic, the human decision makers provide overall guidance and management of the defense. Figure 3 illustrates the essence of the DLCD approach for a single element of cyberspace. Figure 4 illustrates its use for application protection.

The key to DLCD is the protection of each element of cyberspace by one or more nested Type 1 virtual machines, each operated by its own virtual machine monitor (VMM) using different configurations.¹⁵ Each virtual machine provides a layer of cyber-defense protection, having its own set of virtual machine (VM) properties and traditional tactical cyber defenses, as illustrated in figure 3. Additional virtual machines are added to the layered protection as warranted by the threat and importance of the component in the current decision context. End-to-end security within the DLCD environment is accomplished along the lines described by Cricket Liu and Paul Abilitz in *DNS and BIND*.¹⁶ For example, communication between virtual machines must be secure and reliable. Therefore, data is encrypted before transmission between virtual machines or between applications. Secure communication is enhanced using virtual private network (VPN) technology to secure interprocess communication within the computer system. Issuing virtual machines and authorized applications a digital certificate for authentication provides additional security. Defensive tactical cyber security is further improved by using DNSSEC and IPSEC for communication within and between layers and IPv6 addresses to identify individual applications and virtual machines (IPv6 addresses are not shared or inherited).¹⁷ The combination of VM with other tactical cyber-defense technologies enables secure, dynamic alteration of the defensive cyber terrain that the attacker must overcome to achieve cyber-attack objectives.

By using multiple nested virtual machines and other cyber-defense technologies to protect the elements of cyberspace, DLCD supports dynamic allocation of tactical cyber-defense resources by enabling the addition of virtual machines to the layers of protection of an element or component, by altering the mix of VM types and configurations, or by changing tactical cyber-attack detection systems within each VM without altering or influencing the other VMs or cyberspace elements within a system. Using DLCD, the defensive cyber terrain can be altered in a significant, useful, unpredictable manner that cannot be detected or prevented by the cyber attacker or by malware that has breached the system's defenses. DLCD presents tactical cyber attackers with a

reconfigurable maze that they must continuously solve to penetrate defensive cyberspace and exploit a penetration. Note that for each VM layer added to protect a component or an element, the poorer the performance of the enclosed element or component, which inevitably degrades the utility of the cyberspace element or component for broader mission accomplishment. It is therefore vital that decision makers alter protection only in response to actual threats against cyberspace resources; otherwise the performance of the elements and components can be degraded to such a degree that they lose utility for a decision maker. The complexity of the tradeoffs between element security and timeliness is the basis for our contention that humans must manage tactical cyber defenses even though rapid responses must be executed by intelligent systems.

By using a multilayered, nested virtual machine approach (figs. 3 and 4) as the basis for DLCDD, the tactical cyber defense can respond to a tactical cyber attack while the attack is in progress. A dynamic layered tactical cyber defense based upon nested VM technologies can effectively protect the four cyberspace elements.

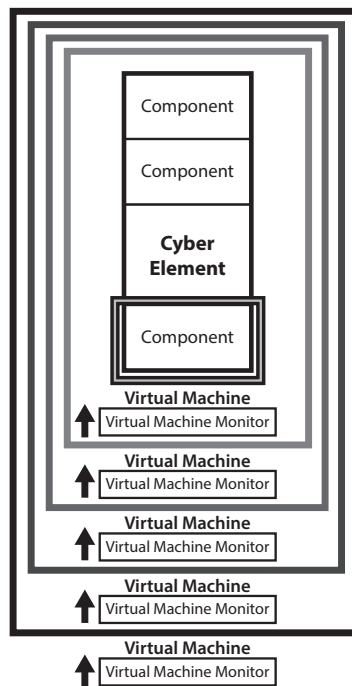


Figure 3. Nominal dynamic layered cyber defense architecture for an element showing VMM placement

The importance of timely and accurate delivery of cyberspace elements to decision-making success is hard to overstate.¹⁸ Delay leads to failure to gain or maintain situational awareness, to failure to make decisions, and to incorrect decisions. The need to share some portions of each cyberspace element to develop and maintain group SA further compounds the challenge of timely and accurate delivery, because in modern conflict there are generally many decision makers involved in the assessment and decision process for each decision, as envisioned in the JIE. While cyberspace elements increase in value when shared, the sharing process also increases the vulnerability of the element and of the decision-making process. As a result, when decision makers are assessing tactical cyber-defense approaches, they must not only consider how best to protect the elements that are crucial to the current decision context, but also how to protect the elements and components delivered to all others involved in the same decision. The tactical cyber defense challenge is increased by the variability in the elements and components of cyberspace across different decisions, by the variability in the ability of a cyberspace element or component to decrease uncertainty, by the differences in the tolerances of elements, components, and decision makers to risk, and by varying perceptions of the importance of each decision within the evolving situation.

The well-known difficulty of cyberspace element value assessment, especially data, is increased when the number of decision makers using the same elements increases. The clear solution to the problem is to assess cyberspace element and component value in a variety of situations and use these valuations as guides to cyber-defense action during attacks. We can conduct cyberspace element and component value assessments by monitoring the protection choices and cyberspace element usage choices made during decision making in a simulation environment. To make the assessment, we assume that the relevant cyberspace elements and components employed for the decision are important and that the other cyberspace elements and components that are not considered are not as important in that particular circumstance. Nevertheless, the cyberspace elements and components not employed in a decision must be protected to a degree. Human participation is crucial in making and revising element and component priorities for tactical cyber defense because of the complexities involved when making priority assessments. The simulation-derived priorities can be used to guide decision-maker cyberspace

element and component tactical cyber defense choices during real-world cyber attacks.

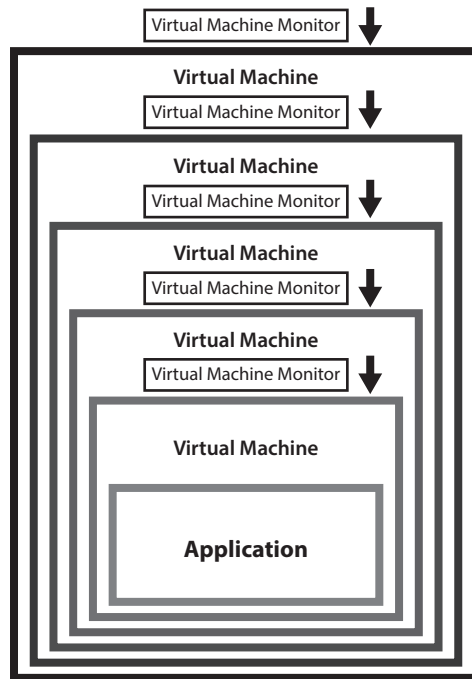


Figure 4: Using nested virtual machines to protect an application in DLCD

Training Cyber Defense

As cyber attacks increase in technical sophistication they can increase their ability to target specific information, data, and physical resources, which can be disorienting. Even an attack that does not disorient users can still produce confusion, which in turn decreases group SA, individual SA, and decision-making quality. The inevitable result of increased technical sophistication by cyber attackers is improvement in their ability to cloud situation awareness, disrupt decision dissemination, and prevent accurate feedback. Preparation for decision making during a cyber attack requires training to prepare for a cyber attack's psychological, SA, and decision-making challenges coupled with the tools for information analysis and management needed to help decision makers evaluate the information available to them, assess the trustworthiness of the information, and develop situational awareness. The pursuit of cyberspace

SA is crucial to securing cyberspace and to attaining SA in the other parts of the conflict—air, ground, sea, or space. Because cyberspace SA for both individuals and groups of decision makers is vital, developing training environments for decision makers and strategic cyber defenders to provide experience and expertise in addressing cyber attacks and their attempts to undercut SA is imperative. The needs of the strategic cyber defender are clear: strategies that protect elements and their components when under cyber attack while ensuring decision makers have the components of the cyberspace elements they need.

In light of these complementary requirements, strategic cyber defender and decision-maker training must address two needs. *First*, to prepare defenders and decision makers for the confusing, contradictory, and misleading cyberspace elements present during a cyber attack. Training can prepare them to cope with the psychological stresses caused by variations in cyberspace element availability and quality. A key aspect of this training must be learning to assess cyberspace element value, both as it relates to the value (importance) of available elements in relation to current decisions as well as relative to the value of the elements compromised. Decision makers must learn that cyberspace element value is not correlated with security classification. The defenders also need to evaluate effectiveness of various strategies to counter cyber attacks and campaigns. The *second* need is to prepare decision makers to exploit cyberspace dominance via effective employment of trustworthy data analysis/comprehension (such as analysis based upon big data) and data interaction/management technologies. Analysis, comprehension, and interaction must be performed, in part, automatically due to the volume of data available. Nevertheless, decision makers must learn how to navigate cyberspace, how to use visualizations as viewports into critical portions of cyberspace, how to compare and compose visualizations to provide needed insights, how to identify and exploit key data, and how to coordinate their navigation, analysis, and comprehension efforts despite cyber attacks designed to undermine these efforts.

The challenges posed to strategic cyber defense in addressing these two needs are significant, because achieving and maintaining broad-spectrum defensive cyberspace dominance is increasingly difficult and unreliable due to improvements in tactical cyber-attack technologies. The crucial challenge in strategic cyber defense lies in determining which defense to employ in light of which elements require improvement in

tactical cyber defense and which elements are adequately defended in the current decision-making context. Because of the volume of data that must be considered and the rapid pace of activity, the strategic cyber defender as well as the decision maker must be prepared for the confusing and novel information circumstances they will encounter. Exposure to simulated cyber attacks can prepare the strategic cyber defender to accomplish proper assessment of cyber circumstances and to select the most advantageous strategic and tactical cyber defense responses to cyber attacks.

Preparation of strategic cyber defenders is critical because instinctive behaviors exhibited in the face of uncertainty are invariably incorrect and counterproductive. Under stress, instinctive behaviors are adopted. Stress-induced behaviors lead to the use of emotional bias to make decisions (making the decision that enables the person *feel* that a more positive outcome is likely), to expectation bias (the expectation that the things the person *wants* to happen will happen), to loss/risk aversion (the tendency to value choices that *seem* to minimize risk and loss in spite of any evidence or data to the contrary), and to the adoption of the sunk-cost fallacy (wherein the tendency is to *continue* an action because the decision maker believes the situation will not get worse or because the decision maker has a vested emotional and ego interest in continuing the same course of action). Finally, instinctive behaviors may also lead to past-fixation (the tendency to make decisions based on the expectation that conditions that existed in the past *will recur* despite the fact that they can never recur). Countering instinctive, counterproductive behaviors is difficult and should be one of the main concerns of strategic cyber defense training via simulation.

The tools and training required by strategic cyber defenders and decision makers to prepare them for the challenges of cyber conflict must address three classes of cyber situations: operations during normal conditions, operations during a cyber attack, and operations after a cyber attack.¹⁹ The training, techniques, and tools that are vital in these three circumstances can be developed using simulation environments designed to provide the following capabilities: (1) improve understanding of the challenges posed during a cyber attack, (2) test and evaluate cyber defense tools, techniques, and training, (3) practice using cyber defense tools and techniques to acquire expertise, and (4) assess cyber element value during a wide array of circumstances to determine how best to

deploy cyber defenses. The tools, techniques, and training must be extensive and flexible so they can be readily altered to address new cyber threats and tactical cyber attacks as they arise or become possible.²⁰

Training Cyber Defense through Simulation

Cyber-attack simulation is the only means to prepare decision makers for the complexity of the inevitable attacks upon cyberspace elements. It is the best means available to determine the strategies to be used to secure the critical elements of cyberspace in support of the decision makers' needs.

Simulation provides a safe and flexible way to prepare strategic cyber defenders and decision makers for the challenges faced in a cyber attack as well as for assessing cyberspace element protection techniques and defense strategies. Cyber-attack simulation can provide an environment that allows decision makers and strategic cyber defenders to practice so that their decisions and activities in the real world will produce an effective strategic cyber defense, adequate SA, and effective decisions. To scale as technologies evolve, cyber-attack simulation must portray attack and defense actions in a manner that corresponds to how these actions are perceived by humans, even as the attack proceeds and defenses succeed or fail in the simulation environment. To achieve these goals, the cyber simulation environment must capture and represent the activities of the decision makers and strategic cyber defenders, the attacker and defender goals, the sequence of operations the attacker will execute, the activities of the tactical cyber defense, logical and physical data location(s), and the potential responses of the attackers and defenders to each others' actions. In previous works, we described cyber-attack simulation techniques that can be used to model cyber operations, their components, and possible responses to defensive actions.²¹

The simulation of cyber attacks presents a number of analysis and assessment challenges, all of which concern determining the status and importance of the cyberspace elements available to decision makers. Previous studies of the importance of data to decision making as well as the challenges posed by contradictory or confusing data can be used as a basis for determining how to alter cyberspace elements and their components in response to a simulated cyber attack. To simulate a cyber attack, we need only affect the cyberspace elements available to users;

we do not need to infect or corrupt computers or their software. For realistic simulation, the stimuli and cyberspace elements provided to decision makers must contain the noise, discontinuities, and errors of the type that would be caused by the actual cyber activity so the decision maker and cyber defenders are accustomed to cyber attacks as they might unfold in the real world. The same simulation environment can be used to assess cyberspace element value and to develop procedures for continuing operations in the face of cyber attacks.

Four simulation goals are necessary to prepare decision makers and cyber defenders for cyber attacks. *First*, teaching them how to determine the targets of cyber attacks. *Second*, teaching them the techniques and tactics likely to be used against targets. *Third*, teaching the decision makers and cyber defenders the effects of each type of attack and the techniques and tools that should be used to counteract each type of cyber attack. *Fourth*, teaching them the means for explicitly assessing cyberspace element value and deploying cyber defenses to protect the highest value information. An additional consideration for defenders is exploring strategies and tactics to assess their usefulness. Cyber simulation can achieve these goals. To minimize the development cost of simulation environments, current simulation systems can be coupled with cyber simulation systems, as illustrated in figure 5. The scenarios to be executed in the cyber simulation are described using the Unified Modeling Language (UML).²² To create realistic cyber simulation environments, the components of the cyber simulation environment must exchange information about the cyber attack and cyber defense, the status of the cyber event, and portray the results of the cyber attack and defensive responses.

The key to this approach is recognizing that simulating a cyber attack only requires affecting the information presented to the users in the simulation environment. Therefore, to prepare for the SA and decision-making challenges faced during a cyber attack, only the presentation of the cyberspace elements must be altered; the “true” elements and their values need not be altered. Three approaches are available to affect element presentation: increase the amount of information presented via an element, block information needed by a user that is provided by an element, and substitute false information for the actual information presented via an element. For example, a user can be given an overwhelming amount of data, denied data, or given a mixture of accurate and false

data. Other techniques that can be used to simulate a cyber attack are: instructing every simulation host to replicate every message received at the host but with the number of messages received changed by a random but small amount, instructing every simulation host to duplicate the same information in numerous windows, or instructing every simulation host to remove random words from each message. The effects of these simple measures can be compounded if false messages are repeated at random time intervals after the first receipt of the message.

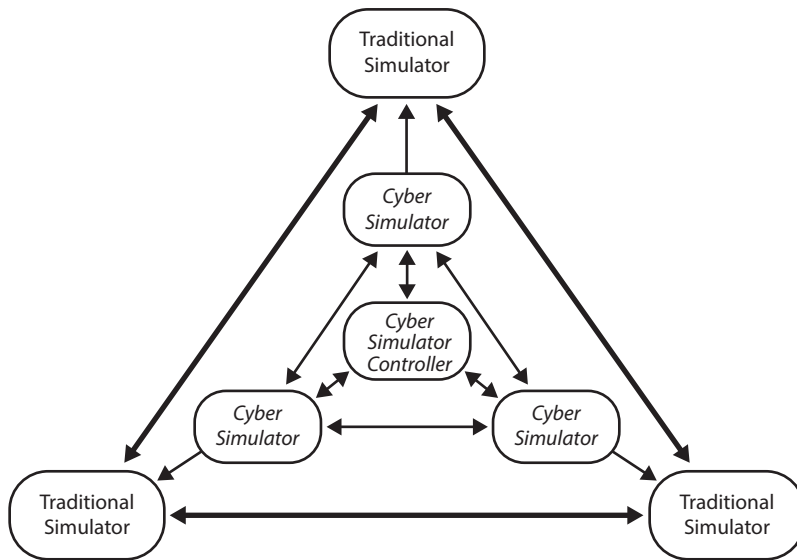


Figure 5. Conceptual cyber simulation environment

A cyber training simulation environment (see fig. 5) must accomplish three tasks to achieve its training goals: determine if a simulated cyber attack is successful, determine the effect of the simulated cyber attack upon each host and its data, and portray simulated cyber defensive responses to the simulated attack. In the illustrated approach, each host has a cyber simulator that services the host and provides these three capabilities. The cyber simulator provides each host with inputs needed to portray the effects of simulated attacks and defense responses. The simulation systems communicate with each other using a logically separate cyber simulation network to achieve a consistent cyber state across the simulation environment.

At each step of the cyber attack and cyber-defensive response, the simulation environment must provide appropriate, realistic indications

of the status of the attack and cyberspace elements status/values so they reflect the delays and alterations that would occur in the corresponding real-world cyber attack. For example, changes in the tactical cyber defense that increase or decrease the depth of defense would be reflected in increased or decreased delays in data transport. The simulation architecture allows cyber defenders to alter the types and configurations of the tactical cyber defense at any time. As a result of exposure to a realistic cyber defense and attack environment, the defender and decision maker can experience the effects of their defensive choices and experiment with dynamic techniques.

An example scenario illustrates how the cyber simulation environment can be used to prepare decision makers and strategic cyber defenders for attacks. The cyber simulation environment could be tasked to provide experience in using information analysis and navigation technologies to detect the presence of a botnet. The botnet detection methods introduced could include analysis of specific network and/or cloud traffic flows, analysis of aggregate network and/or cloud traffic data, variations in data volume, variations in network traffic sources and destinations, and other atypical behavior. The training environment would prepare the decision makers and defenders for the real world where one indicator of infection is not enough. In practice, confirmation of a botnet infection requires multiple indicators to achieve robustness of confirmation by providing both the ability to corroborate data of dubious or variable dependability and minimize the false alarm rate.

In figure 6, “protection” or “value” rings are used to prioritize the four cyberspace element components. The rings correspond to the value and priorities assigned to each cyberspace element’s protection. For the strategic cyber defender, the ring model can be used to guide resource allocation as well as decisions to isolate systems or subsystems that are compromised. In the ring-modeling approach, the closer the rings are to the center, the greater value, importance, and usefulness (of that cyber element) is in the decision context. The number of rings and the content of each ring are determined by the decision-making context. As a result, the number and content of rings for each element vary dynamically. We use one set of rings for each of the four elements. Each cyberspace element ring contains components of approximately the same importance for that element in a decision-making context. The ring model also serves to simplify the cyber-attack simulation challenge. To simulate

an attack within a decision-making context, we affect the elements and components needed in the decision context by simulating the modification of the content of the specific rings for those elements of defensive cyberspace that are compromised. The decision, type of cyber attack, the tactical cyber defenses, the expertise of the decision maker, and the learning outcome(s) for the simulation exercise determine the number of rings affected for each element and the element's components that are altered.

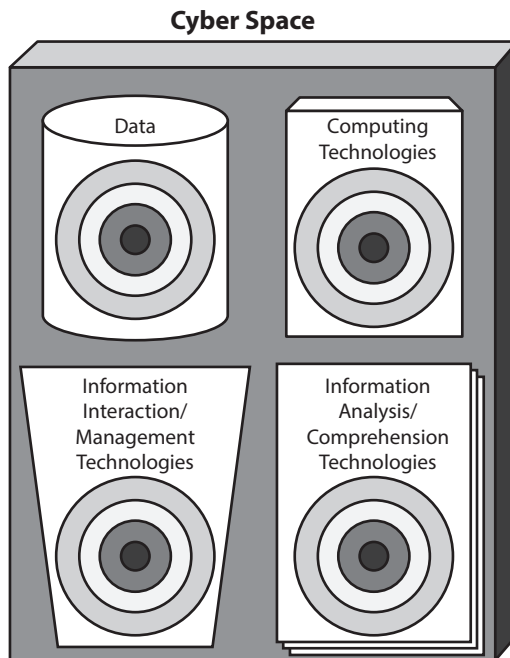


Figure 6. Framework for modeling relative importance of the components of cyberspace elements

A cyber simulation training environment can prepare decision makers to proactively alter tactical cyber defenses, prioritize data, prioritize the elements of cyberspace, and operate during a strategic cyber attack wherein some cyberspace elements and components are compromised to an uncertain degree.

The simulation approach described above allows us to address the four decision-maker and cyber defender training considerations with minimal risk to real-world cyberspace coupled with high fidelity in the cyberspace simulation environment. The simulation problem that remains is determining cyberspace metrics for assessing both simulated

and real-world cyberspace status and for developing situational awareness. Cyberspace metrics must provide insight into cyberspace state, cyber-attack attempts, cyber-attack targets, the degree of a cyber attack's success, and the effectiveness of deployed cyber defenses at the element and component levels.²³

Summary and Open Issues

Cyber dominance has one goal, the command of cyberspace elements. While decision makers implicitly expect cyberspace dominance, it is not assured in light of current tactical cyber-attack technologies and tactical cyber defense technologies. Achieving cyber dominance will not guarantee victory for a data centric force; however, the lack of cyber dominance will almost certainly ensure its defeat. Any approach to cyber dominance must possess two crucial traits: the approach must enhance defensive cyber security and maintain system reliability during cyber attack. The approach described above for achieving defensive cyber dominance calls for DLCD coupled with simulation training to assist decision makers and strategic cyber defenders. It can provide experience needed to allow decision makers to operate within a compromised defensive cyber environment and to identify, analyze, and predict the objectives and presence of cyber attacks. The same approach also permits the development and evaluation of strategic cyber defense options to employ against various cyber attacks and campaigns. The approach complements the JIE or similar dataflow architectures and their tactical cyber defense technologies.

As cyber technologies improve, the challenges to achieving cyber dominance will increase. Additionally, the intricacy of future cyber systems and cyberspace will increase, as witnessed by the development of inter-cloud technologies, "smart grid" technologies for remote control and management of real-world infrastructure (SCADA systems),²⁴ IPv6 deployment, and the "Internet of Things."²⁵ We expect that the increasing power of computing technologies and the increasing complexity of tactical and strategic cyber attacks will compound the difficulties posed to the cyber defender and create new pathways for executing cyber attacks.

Preparation for future cyber attacks requires the development of training systems that impart the experience and expertise needed to make effective strategic and tactical cyber defense possible. While the requisite training systems can now be deployed, before an all-inclusive cyber

simulation environment can be fielded for training purposes, further research and development to advance cyber battle understanding, human behavior modeling, intent inferencing, information display, data mining, and decision making during cyber conflict and strategic cyber defense must be conducted. An additional important area of investigation is gaining a better understanding of decision making and situational awareness within large-scale and high-volume data environments that have noise and uncertainty inherent to the data as well as due to cyber attacks. The required research in high-data-volume environments lies at the intersection of machine learning, data mining, game theory, large-scale data analysis, and SA development technologies. A final area of further research is assessment of the effectiveness of tactical cyber defense options best suited to achieve each desired cyber-defense strategy.

While deception and information denial operations are as ancient as warfare itself, technically sophisticated cyber attacks permit, for the first time, a wide-scale, persistent, and virtually undetectable attack upon the data, tools, and other elements of cyberspace that a decision maker routinely employs. The technically sophisticated cyber attack of the future will destroy or corrupt data, surprise decision makers, generate confusion, delay response, and greatly increase what Clausewitz calls the “fog and friction” in war. Because cyberspace will be contested, decision makers must be prepared for strategic cyber attacks designed to undermine their decision-making ability. To be unprepared for the effects of a strategic cyber attack is to remain in needless peril. In the future, addressing the strategic cyber-attack challenge will become more, not less, critical to success.²⁶

Glossary

cloud computing—a model for enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

component-level metrics—measure the performance of specific characteristics of a cyberspace component. Example components include (1) the number of page swaps per time interval in each virtual machine, (2) the average elapsed time before a page is swapped in a virtual machine,

(3) average elapsed time to migrate a virtual machine from one host to another, and (4) the average time to execute RC4 encryption a set number of times on a specified clear text input among different virtual machines and others.²⁷

cyber attack—an application of cyber security technologies within cyberspace with the intent of degrading an adversary's data, computing technologies, information analysis/comprehension and/or information interaction/management capability to one's advantage.

cyber defense—the application of cyber security technologies to protect one's portion of cyberspace to secure data and computing technologies as well as protect information analysis/comprehension and information interaction/management capabilities.

cyber security technologies—the subset of computing technologies used either to protect one's own data, information analysis/comprehension technologies, computing technologies, and information interaction/management technologies or to undermine those of an adversary.

cyberspace—composed of four elements: (1) data, (2) computing technologies (such as computer hardware, computer software, computer networks/infrastructure, network protocols, virtualization, and cloud computing), (3) information analysis/comprehension technologies (including information visualization, artificial intelligence, collaboration, data mining technologies, and big data technologies), and (4) information interaction/management technologies (including human-computer interaction, intelligent agents, human intent inferencing, and database technologies).

digital certificate—a signed public key. A trusted authority signs the digital certificate before it is issued.

DNSSEC (Domain Name System Security Extensions Convention)—a set of Internet engineering task force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) on Internet protocol (IP) networks. A domain name server manages the domain names repository and provides name resolution for an internet zone. The DNSSEC specifications are covered by Request for Comments (RFC) 4033, 4034, 4035, and 3833 at <http://www.ietf.org/rfc.html>.

exploit—software that attacks a cyber security vulnerability.

(human) intent inferencing—an artificial intelligence-based technique used to provide an intelligent user interface in which the goals of

the user are deduced based upon a history of user actions and a computable representation of the current mission.²⁸

information stream—a logical path through the architecture from an information source to a designated information sink.

IPSEC (Internet Protocol Security) is a set of protocols for securing IP communications at the network layer, layer 3 of the OSI model, by authenticating and/or encrypting each IP packet in a data stream. IPSEC includes protocols for cryptographic key establishment.

intercloud—a model for computing based on a cloud composed of computing clouds.

malware—software used to disrupt computer operation, gather sensitive information, or gain access to private computer system. It includes computer viruses, ransomware, backdoors, worms, Trojan horses, rootkits, spyware, rogue security software, and other malicious software. The type of malware is classified based on how it is executed, how it spreads, and what it does. A **virus** is malware that can execute itself by placing its own code in the execution path of another program and can replicate itself by replacing existing computer files with copies of itself. A **Trojan** is a hidden program that masquerades as a benign application. A **worm** does not require a host program to propagate but enters a computer through a weakness in the computer system defenses and propagates using network traffic security flaws. A **backdoor** is software that allows access to the computer system by bypassing normal authentication procedures.

rootkit—malware that hides traces of an attack, installs Trojans and backdoors, provides the attacker with root control of the system, and enables further malicious activity.


situational awareness (SA)—“the perception of the elements in the environment within a volume of space and time, the comprehension of their meaning, the projection of their status into the near future, and the prediction of how various actions will affect the fulfillment of one’s goals.”²⁹ Endsley identifies four components of situational awareness: **perception** (what are the facts), **comprehension** (understanding the facts), **projection** (anticipation based upon understanding), and **prediction** (evaluation of how outside forces may act upon the situation to affect your projections). These stages are similar to but not identical with Boyd’s observe-orient-decide-act (OODA) loop construct.³⁰

smart grid—employs computer-based remote control and automation on all elements of electrical power delivery to optimize electrical power generation and distribution.

software gauge—software that converts data collected by a software probe into a measure that is meaningful for a particular system for the purpose of performance tuning, information assurance, functional validation, compatibility, or assessment of operational correctness.

software probe—software that interacts with an operating system, operational application, or subset of an application to collect data for a gauge(s).

virtualization—a technique for emulating a computing resource and for hiding the physical characteristics of computing resources from the systems, applications, or end-users that interact with those resources. Virtualization exploits virtual machine technologies. Virtualization technologies provide six key benefits: (1) efficient use of computing resources, which reduces information technology infrastructure and environmental (power, cooling, and real estate) requirements; (2) fault isolation in which an application error, operating system crash, or user error in one virtual machine will not affect the use of other virtual machines on the same system; (3) increased security where vulnerabilities or exploits can be contained and quarantined in a single virtual machine without affecting the entire system; (4) rapid provisioning through file copy or volume cloning used to rapidly create new virtual machines; (5) flexibility in managing change to include the ability to scale according to the demand for services, unique operating systems, and service provisioning; and (6) portability through the abstraction of devices combined with the encapsulation of virtual data in virtual disks. Virtualization is a key technology for cloud computing.

Additional definitions are available at <http://www.sans.org/security-resources/glossary-of-terms/> and <http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf>. 

Notes

1. For our purposes, the four elements (or aspects) of cyberspace are (1) data, (2) computing technologies, (3) information interaction and management technologies, and (4) information analysis and comprehension technologies.

2. Chris Buckley, “China PLA Officers Call Internet Key Battleground,” Reuters, 3 June 2011. Senior Col Ye Zheng and his colleague Zhao Baoxian, stress in *China Youth Daily* the importance of China’s cyber warfare capabilities, concluding that “just as nuclear warfare was the strategic war of the industrial era, cyber-warfare has become the strategic war of the information era, and this has become a form of battle that is massively destructive and concerns the life and death of nations.” See also R. A. Clarke

and R. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010); A. F. Krepinevich, *Cyber Warfare: A Nuclear Option?* (Washington: Center for Strategic and Budgetary Assessments, 2012); Gen Keith Alexander, *Testimony before the House Armed Services Committee*, 23 September 2010; D. E. Geer and J. Archer, "Stand Your Ground," *IEEE Security and Privacy* 10, no. 4 (2012): 96; "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, 11 October 2012; and B. H. Liddell Hart, *The Revolution in Warfare* (New Haven, CT: Yale University Press, 1932), 121.

3. This and other terms are discussed in a glossary at the end of the article.

4. Val Smith and Chris, "Why Black Hats Always Win," *Blackhat.com*, January 2010; Joanna Rutkowska, "Subverting Vista Kernel for Fun and Profit," Black Hat USA, July 2006; J. Levine, J. Grizzard, and H. Owen, "Detecting and Categorizing Kernel-Level Rootkits to aid Future Detection," *IEEE Security and Privacy* 4, no. 1 (January/February 2006): 24–32; Rutkowska, "Rootkit Hunting vs. Compromise Detection," Black Hat Federal 2006, Washington, DC, 25 January 2006; A. Lakhotia, "Analysis of Adversarial Code: Problems, Challenges, and Results," Black Hat Federal 2006; William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010); A. Acquisti and J. Grossklags, "Privacy and Rationality in Individual Decision Making," *IEEE Security and Privacy* 3, no. 1 (2005): 26–33; I. P. Cook and Pfleeger, "Security Decision Support: Challenges in Data Collection and Use," *IEEE Security and Privacy* 8, no. 3 (2010): 28–35; J. Giffin, "The Next Malware Battleground: Recovery after Unknown Infection," *ibid.*, 77–82; K. J. Hole and L. Netland, "Toward Risk Assessment of Large-Impact and Rare Events," *ibid.*, 21–27; J. R. Kenney and C. Robinson, "Embedded Software Assurance for Configuring Secure Hardware," *IEEE Security and Privacy* 8, no. 5 (2010): 20–26; M. E. Johnson and Pfleeger, "Addressing Information Risk in Turbulent Times," *IEEE Security and Privacy* 9, no. 1 (2011): 49–58; J. Schiffman et al., "Network-Based Root of Trust for Installation," *ibid.*, 40–48; B. Stone-Grosset et al., "Analysis of a Botnet Takeover," *ibid.*, 64–72; P. Ning, Y. Cui, and D. S. Reeves, "Intrusion Detection: Constructing Attack Scenarios through Correlation of Intrusion Alerts," *Proceedings of the 9th ACM Conference on Computer and Communications Security*, November 2002; M. M. Pillai, J. H. P. Eloff, and H. S. Venter, "An Approach to Implement a Network Intrusion Detection System Using Genetic Algorithms," *Proceedings of the 2004 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries*, October 2004; E. Skoudis and L. Zeltser, *Malware: Fighting Malicious Code* (Upper Saddle River, NJ: Prentice Hall, 2003); C. C. Zou, W. Gong, and D. Towsley, "Formation and Simulation: Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense," *Proceedings of the 2003 ACM Workshop on Rapid Malcode*, October 2003; R. Graham and D. Maynor, "SCADA Security and Terrorism: We're Not Crying Wolf," Black Hat Federal 2006; M. Jakobson and Z. Tamzan, *Crimeware: Understanding New Attacks and Defenses* (Upper Saddle River: Addison-Wesley, 2008); J. V. Antrosio and E. W. Flup, "Malware Defense Using Network Security Authentication," *Proceedings of the Third IEEE International Workshop on Information Assurance (IWIA'05)*, March 2005; J. Aycock and K. Barker, "Viruses 101," *ACM SIGCSE Bulletin: Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education* 37, no. 1 (February 2005); D. Ellis, "Formation and Simulation: Worm Anatomy and Model," *Proceedings of the 2003 ACM Workshop on Rapid Malcode*, October 2003; D. M. Kienzie and M. C. Elder, "Internet WORMS: Past, Present, and Future: Recent Worms: A Survey And Trends," *ibid.*; J. Nazaro, *Defense and Detection Strategies against Internet Worms* (Boston: Artech House, 2004); S. T. King and P. M. Chen, "Backtracking Intrusions," *ACM Transactions on Computer Systems (TOCS)* 23, no. 1, January 2005; C. Kruegel, W. Robertson, and G. Vigna, "Detecting Kernel-Level Rootkits through Binary Analysis," *Proceedings of the 20th Annual Computer Security Applications Conference*, December 2004; C. P. Pfleeger and S. L. Pfleeger, *Analyzing Computer Security: A Threat, Vulnerability, Countermeasure Approach* (Upper Saddle River: Prentice Hall, 2012); Pfleeger and Pfleeger, *Security in Computing*, 4th ed. (Upper Saddle River: Prentice Hall, 2007); R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. (Indianapolis: Wiley, 2008); and M. Maras, *Computer Forensics: Cybercriminals, Laws, and Evidence* (Burlington, MA: Jones & Bartlett, 2012).

5. *Ibid.*

6. J. M. Graaido, R. Schlesinger, and K. Hoganson, *Principles of Modern Operating Systems*, 2nd ed. (Burlington, MA: Jones & Bartlett, 2013); P. A. Karger and D. R. Safford, "I/O for Virtual Machine Monitors: Security and Performance Issues," *IEEE Security & Privacy* 6, no. 5, (2008): 16–23; H. Takabi, J. B. D. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Security & Privacy* 8, no. 6, (2010): 24–31; Qian Liu et al., "An In-VM Measuring Framework for

Increasing Virtual Machine Security in Clouds,” *IEEE Security & Privacy* 8, no. 6, (2010): 56–62; R. L. Krutz and R. D. Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing* (Indianapolis: Wiley, 2010); A. Belapurkar et al., *Distributed Systems Security: Issues, Processes, and Solutions* (Indianapolis: Wiley, 2009); C. Cachin and M. Schunter, “A Cloud You Can Trust,” *IEEE Spectrum* 48, no. 12 (2011): 28–51; and K. Jamsa, *Cloud Computing* (Burlington, MA: Jones & Bartlett, 2013).

7. D. S. Alberts et al., *Understanding Information Age Warfare* (Washington: CCRP Press, 2001); and Alberts and R. E. Hayes, *Power to the Edge* (Washington: CCRP Press, 2003)

8. Ibid.

9. Mica Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems,” *Human Factors* 37, no. 1 (1995): 35–64.

10. Frans Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Abingdon, UK: Routledge, 2005).

11. L. Ying, L. Bingyang, and W. Huiqiang, “Dynamic Awareness of Network Security Situation Based on Stochastic Game Theory,” 2nd International Conference on Software Engineering and Data Mining (2010), 101–5; K. Smith and P. A. Hancock, “Situation Awareness is Adaptive, Externally Directed Consciousness,” *Human Factors* 37, no. 1 (1995): 137; VADM A. K. Cebrowski, “Network-Centric Warfare: An Emerging Military Response to the Information Age,” 1999 Command and Control Research and Technology Symposium, 29 June 1999, <http://www.nwc.navy.mil/press/speeches/ccrp2htm>; and P. Hinds, *Perspective Taking among Distributed Workers: The Effect of Distance on Shared Mental Models of Work*, World Trade Organization Working Paper # 7 (Stanford, CA: Center for Work, Technology, and Organization, 1999).

12. Lynn, “Defending a New Domain.”

13. J. H. Saltzer and M. D. Schroeder, “The Protection of Information in Computer Systems,” *Proceedings of the IEEE* 63, no. 9, (1975): 1278–1308; Saltzer and M. F. Kaashoek, *Principles of Computer System Design* (Indianapolis: Wiley, 2009); R. E. Smith, *Elementary Information Security* (Burlington, MA: Jones & Bartlett, 2013); A. Kerckhoffs, “La Cryptographie Militaire,” *Journal Sciences Militaires* 9 (February 1883): 161–91; B. Schneier, “Secrecy, Security, and Obscurity,” *Cryptogram Newsletter*, 15 May 2002, <http://www.schneier.com/crypto-gram-0205.html>; C. E. Shannon, “Communication Theory of Secrecy Systems,” *Bell System Technical Journal*, October 1949, 656–715; D. E. Denning, “A Lattice Model of Secure Information Flow,” *Communications of the ACM* 19, no. 5 (1976): 236–43; DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, 26 December 1985; P. A. Karger and R. R. Schell, *Multics Security Evaluation: Vulnerability Analysis*, ESD-TR-74-193, vol. II, HQ Electronic System Division, June 1974; K. Thompson, “Reflections on Trusting Trust,” *Communications of the ACM* 27, no. 8 (1984): 761–63; R. E. Smith, “A Contemporary Look at Saltzer and Schroeder’s 1975 Design Principles,” *IEEE Security and Privacy* 10, no. 6, (2012): 20–25; R. Smith, *Elementary System Security* (Burlington, MA: Jones & Bartlett, 2013); S. Smith and J. Marchesini, *The Craft of System Security* (Upper Saddle River: Addison-Wesley, 2008); S. Lipner, T. Jaeger, and M. E. Zurko, “Lessons from VAX/SVS for High-Assurance VM Systems,” *IEEE Security and Privacy* 10, no. 6 (2012): 26–35; J. C. Wray, “An Analysis of Covert Timing Channels,” *Proceedings of the IEEE Symposium on Security and Privacy*, (1991): 52–61; L. J. Fraim, “SCOMP: A Solution to the Multilevel Security Problem,” *IEEE Computer* 16, no. 7 (1983): 26–34; C. Larman, *Agile and Iterative Development: A Manager’s Guide* (Boston: Pearson Education, 2004); H. Shrobe and D. Adams, “Suppose We Got a Do-Over: A Revolution for Secure Computing,” *IEEE Security and Privacy* 10, no. 6 (2012): 36–39; R. J. Feiertag and P. G. Neumann, “The Foundations of a Provably Secure Operating System,” *Proceedings of the National Computer Conference*, 1979, 329–34; and W. H. Ware, *Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security* (Santa Monica, CA: RAND, 1970).

14. Ibid.

15. R. J. Adair et al., “A Virtual Machine System for the 360/40,” Cambridge Scientific Center Report 320, IBM, May 1966; G. M. Amdahl, G. A. Blaauw, and F. P. Brooks, “Architecture of the IBM System/360,” *IBM Journal of Research and Development* 8, no. 2 (1964): 87–101; Paul Barham et al., “Xen and the Art of Virtualization,” *Proceedings of the 19th ACM Symposium on Operating System Principles (SOSP)*, Bolton Landing, NY, October 2003, 164–77; A. Bieniusa, J. Eickhold, and T. Fuhrman, “The Architecture of the Decent VM: Towards a Decentralized Virtual Machine for Many-Core Computing,” *Virtual Machines and Intermediate Languages (Systems Programming Languages and Applications: Software for Humanity)*, Reno, NV, 17–21 October 2010; Sean Campbell and Michael Jeronimo, *Applied Virtualization Technology: Usage Models for IT Professionals and Software Developers* (Santa Clara, CA: Intel Press, 2006), chap. 9; R. P. Case and A. Padegs, “Architecture of the IBM System/370,” *Com-*

munications of the ACM 21, no. 1 (January 1978): 73–96; R. J. Creasy, “The Origin of the VM/370 Time Sharing System,” *IBM Journal of R&D* 25, no. 5 (September 1981): 483–90; R. W. Doran, “Amdahl Multiple-Domain Architecture,” *Computer*, October 1988, 20–28; R. C. Daley and J. B. Dennis, “Virtual Memory, Processes, and Sharing in MULTICS,” *Communications of the ACM* 11, no. 5 (May 1968): 306–12; T. Egawa, N. Nishimura, and K. Kourai, “Dependable and Secure Remote Management in IaaS Clouds,” 2012 IEEE 4th International Conference on Cloud Computing Technology and Science, 3–6 December 2012, Taipei, Taiwan, 411–18; D. Gifford and A. Spector, “Case Study: IBM’s System 360-370 Architecture,” *Communications of the ACM* 30, no. 4 (April 1987): 291–307; P. H. Gum, “System/370 Extended Architecture: Facilities for Virtual Machines,” *IBM Journal of Research and Development* 27, no. 6 (1983): 530; K. Hwang and D. Li, “Trusted Cloud Computing with Secure Resources and Data Coloring,” *IEEE Internet Computing* 14, no. 5 (September/October 2010): 14–22; A. S. Lett and W. L. Konigsford, “TSS/360: A Time-Shared Operating System,” *Proceedings of the Fall Joint Computer Conference*, AFIPS, vol. 33, part 1 (1968): 15–28; A. Mann, “The Pros and Cons of Virtualization,” *Business Trends Quarterly*, First Quarter 2007; R. A. Meyer and L. H. Seawright, “A Virtual Machine Time-Sharing System,” *IBM Systems Journal* 9, no. 3 (1970): 199–218; Seawright, and R. A. McKinnon, “VM/370—A Study of Multiplicity and Usefulness,” *IBM Systems Journal* 18, no. 1 (1979): 4–17; A. V. Anderson et al., “Intel Virtualization Technology,” *IEEE Computer* 38, no. 5, (2005): 48–56; B. Yee et al., “Native Client: A Sandbox for Portable, Untrusted x86 Native Code,” 2009 30th IEEE Symposium on Security and Privacy, Oakland, CA, 17–20 May 2009, 79–93; and Y. Wen and K. Du, “Pollux VMM: A Virtual Machine Monitor for Executing Untrusted Code,” 1st International Conference on Information Science and Engineering (ICISE2009), Nanjing, China, 28–29 December 2009, 1785–1788.

16. Cricket Liu and Paul Abitiz, *DNS and BIND*, 5th ed. (Sebastopol, CA: O’Reilly & Associates, 2006).

17. A. Karasidis, *DNS Security* (New York: Springer, 2012); and N. Doraswamy and D. Harkins, *IPSEC: The New Security Standard for the Internet, Intranets, and Virtual Private Networks* (Upper Saddle River: Prentice Hall, 2003).

18. D. L. Rulke and J. Galaskiewicz, “Distributed Knowledge, Group Network Structure, and Group Performance,” *Management Science* 46, no. 5 (May 2000): 612–22; M. R. Stytz and S. B. Banks, “Metrics for Assessing Command, Control, and Communications Capabilities,” 11th International Command and Control Research and Technology Symposium, San Diego, CA, 20–26 June 2006; P. Barton, “What Happens to Value of Information Measures as the Number of Decision Options Increases?” *Health Economics* 20 (2011): 853–63; D. Bellin, “The Economic Value of Information,” *Science Communication* 15, no. 2 (1993): 233–40; A. Cleveland, “Harvesting the Value of Information,” *Journal of Management and Engineering* 15, no. 4 (1999): 37–42; P. Delquié, “The Value of Information and Intensity of Preference,” *Decision Analysis* 5, no. 3 (2008): 129–39, 169; R. Glazer, “Measuring the Value of Information: The Information-Intensive Organization,” *IBM Systems Journal* 32, no. 1 (1993): 99; T. Hulme, “Unlocking the Business Value of Information: Information on Demand,” *Business Information Review* 26, no. 3 (2009): 170–81; M. E. Johnson and S. L. Pfleger, “Addressing Information Risk in Turbulent Times,” *IEEE Security and Privacy* 9, no. 1 (2011): 49–58; A. Kangas, “Measuring the Value of Information in Multicriteria Decision Making,” *Forest Science* 26, no. 6 (2010): 558–66; C. Oppenheim et al., “Studies on Information as an Asset I: Definitions,” *Journal of Information Science*, vol. 29, no. 3, (2003): 159–66; Oppenheim et al., “Studies on Information as an Asset II: Repertory Grid,” *Journal of Information Science* 29, no. 5 (2003): 419–32; Oppenheim et al., “Studies on Information as an Asset III: Views of Information Professionals,” *Journal of Information Science* 30, no. 2 (2003): 181–90; Oppenheim et al., “The Attributes of Information as an Asset,” *New Library World* 102, no. 11/12 (2001): 458–63; R. Fattahi and E. Afshar, “Added Value of Information and Information Systems: A Conceptual Approach,” *Library Review* 55, no. 1–2 (2006): 132–47; A. Repo, “The Dual Approach to the Value of Information: An Appraisal of Use and Exchange Values,” *Information Processing & Management* 22, no. 5 (1986): 373–83; A. Shepanski, “The Value of Information in Decision Making,” *Journal of Economic Psychology* 5, no. 2 (1984): 177–94; and J. Sillince, “A Stochastic Approach of Information Value,” *Information Processing & Management* 31, no. 4 (1995): 543–54.

19. M. R. Stytz, and S. B. Banks, “Toward Improved Software Security Training Using a Cyber Warfare Opposing Force (CW OPFOR): The Knowledge Base Design,” *Proceedings of the SPIE Conference on Data Mining, Intrusion Detection, Information Assurance, and Data Networks 2005*, 5812, no. 28–29 (March 2005): 130–41; Stytz and Banks, “Metrics to Assess Command, Control, and Communications (C3) Performance within a Network-Centric Warfare Simulation,” *Proceedings of the SPIE*

Conference on Enabling Technologies for Simulation Science X, vol. 6227 (April 2006): 17–21; Stytz and Banks, “Requirements and Issues in Cyberwarfare Simulation,” *Proceedings of the 2000 Fall Simulation Interoperability Workshop*, Orlando, FL, 17–22 September 2000, 1–10; Stytz and Banks, “Toward Computer Generated Actors As Cyberspace Opposing Forces Used In Network Centric Warfare Simulations,” *Proceedings of the 2004 Spring Simulation Interoperability Workshop*, Washington, DC, 18–23 April 2004, 84–95.

20. An approach that does not use simulation for user preparation for cyber attacks is discussed by S. L. Garfinkel and G. Dinout, “Operations and Degraded Security,” *IEEE Security and Privacy* 9, no. 6 (2011): 43–48.

21. Ibid.; and Stytz and Banks, “Metrics for Assessing Command, Control, and Communications Capabilities,” 11th International Command and Control Research and Technology Symposium, 20–26 June 2006, San Diego, CA.

22. G. Booch, J. Rumbaugh, and I. Jacobson, *The Unified Modeling Language User Guide* (Reading, MA: Addison-Wesley, 1999).

23. Our first efforts toward development of tools for cyberspace performance metrics are discussed in previously cited references. The metrics are similar to the online, one-pass algorithms used in high frequency trading and derive from digital signal processing.

24. *Communications of the ACM* 55, no. 4: special issue on smart grid technology.

25. *IEEE Computer* 46, no. 2: special issue on the “Internet of Things.”

26. J. Carr et al., Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats (McLean, VA: Grey Logic, 2010), 12.

27. A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt* (Upper Saddle River: Addison-Wesley, 2007).

28. S. Banks and C. Lizza, “Pilot’s Associate: A Cooperative, Knowledge-Based System Application,” *IEEE Expert* 6, no. 3 (1991): 18–29.

29. Mica Endsley, “Situation Awareness Global Assessment Technique (SAGAT),” *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference*, 789–95.

30. Osinga, *Science Strategy and War*.

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.

China: An Unlikely Economic Hegemon

Heather Fox, Major, USAF

Before any nation can achieve hegemon status, it must have economic strength. Numerous authors note that a strong economic base is the seed from which all other sources of national power emerge and hence can be considered a type of national foundation. Martin Jaques, for example, states that “military and political power rest on economic strength.”¹ Economics forms the support base for national power, and major international power shifts typically emerge as a result of economic developments, not military power or political influence, as Paul Kennedy’s research into several centuries of global power politics highlights:

There is detectable a causal relationship between the shifts which have occurred over time in the general economic and productive balances and the position occupied by individual powers in the international system . . . economic shifts heralded the rise of new Great Powers which would one day have a decisive impact upon the military/territorial order. This is why the move in global productive balances toward the “Pacific rim” which has taken place over the past few decades cannot be of interest merely to economists alone.²

China continues to grow economically at what some consider an alarming rate.³ Meanwhile, the United States, struggling with budget woes and sequestration, remains the world’s preeminent economic and military leader but in decline relative to China. The relationship between these two nations and the comparative power they possess may well lay the foundation for future global power shifts impacting not just China and the United States, but indeed the entire international community.⁴ However, while China is still expected to become extremely powerful, it may not rise to the level many expect due to three limiting factors: currency, exports, and demographics. These factors, along with mutual dependency between the two nations, have implications for US policy

Maj Heather Fox is a graduate of the US Air Force Academy and holds MA degrees in strategic intelligence and defense studies from the American Public University and King’s College London, respectively. She attended the UK’s Advanced Command and Staff Course and is currently serving with the RAF at Air Command. She has flown as an instructor and combat pilot in the United States, Europe, Southwest Asia, and the Republic of Korea.

toward China. Thus, it is in the best interest of the United States to form a coherent long-term plan to best engage China in a way that avoids friction and promotes prosperity for both states.

Certainly, other factors may significantly shape China's future, including domestic unrest, politics, resource consumption, and military capability. But it is the concept of economics as the base of power that makes China's rise significantly important to the United States. While the intent here is not to predict China's economic future—indeed doing so with any certainty would be difficult—formulating long-term US policies toward China would be better informed by considering the major factors which might impact its economy rather than simply extending current economic growth trends without considering dynamics that may change its trajectory.⁵ This root of Chinese power must be understood for the United States to successfully relate to China, influence it when necessary, and, if extreme circumstances require, counter it.

China's Rising Economy

Experience: that most brutal of teachers. But you learn, my God do you learn.

—Generally attributed to C. S. Lewis

China began economic reforms in 1978 allowing more private ownership, property rights, and international free trade while still imposing significant central government influence. Even with a recent slowdown, its economy has increased under these changes at a stunning annual rate of around 8–10 percent.⁶ Since overtaking Japan in 2010, China now boasts the second largest gross domestic product (GDP) behind the United States and is expected to surpass the US economy in about a decade if it continues to grow at the present rate.⁷ This rising economy, in conjunction with the world's largest foreign exchange reserve holdings of \$3 trillion, bestows significant financial power.⁸ Arvin Subramanian notes that China is also emerging as a global creditor and is in fact the largest supplier of funds to the United States, creating the potential for escalating impact. He points out that “being a leading financier confers extraordinary influence over other countries that need funds, especially in times of crisis.”⁹

Many believe China's economic rise and gathering power will continue, hence the predictions of surpassing the United States in the coming decades. Institutions such as Goldman Sachs and the Carnegie Endowment predict China will surpass the US economy by 2027 or 2035, respectively.¹⁰ Economist Robert Fogel expects that "by 2040 China not only will have long since surpassed the United States, but also its economy will be nearly three times as large and will account for fully 40 percent of total world output."¹¹ In a *Foreign Policy* article, Fogel contends, "According to my forecasts, China's share of global GDP—40 percent—will dwarf that of the United States (14 percent) and the European Union (5 percent) 30 years from now."¹²

Viewing Fogel's *Foreign Policy* article alongside his National Bureau of Economic Research working paper reveals his 2040 model is based on China maintaining an 8 percent GDP growth rate with essentially only positive influences on its economy, such as growth in education and rural production.¹³ A 2010 *Economist* article predicts China overtaking the United States sometime in the 2019–22 range. Factors cited for this conclusion include GDP growth, inflation, and the increasing value of the yuan. Importantly, this article implies the increasing value of the yuan will *enable* China to fiscally overtake the United States, but it gives no mention to the dynamic of that increasing value having a detrimental impact on exports.¹⁴ In fact, these predictions do not give much, if any, consideration to China's major economic limitations. Fogel's only nod to potential problems is his reference to skeptics pointing out issues such as "rising income inequality, potential social unrest, territorial disputes, fuel scarcity, water shortages, environmental pollution, and a still-rickety banking system," to which he replies, "Although the critics have a point, these concerns are no secret to China's leaders; in recent years, Beijing has proven quite adept in tackling problems it has set out to address."¹⁵

In the event these predictions are correct and China's GDP surpasses that of the United States between 2020 and 2040, having a larger GDP does not necessarily bestow the title "hegemon" to China. One can argue the legitimacy of referring to China as an economic hegemon if the US dollar and European Union euro are still the leading international currencies and China has only risen to this status by playing outside the rules by which other trading nations abide. China will certainly be powerful, but without control of the dominant international currency

and faced with potentially constant global pressure to change practices, its leadership and influence will be significantly limited. China's massive reserves and rising GDP may provide economic power, but the practices it will have to use to get to this predicted position certainly are not those of a leader.

Even if China's GDP does lead the world, so long as the yuan is not completely free nor the leading global reserve currency and China uses unfair practices to gain an advantage, it will not be the global economic hegemon. For these and other reasons, such as high raw material consumption and lack of soft power, David Shambaugh refers to China as a "partial power" having broad but not necessarily deep global power to influence. "China is a global actor without (yet) being a true global power—the distinction being that true global powers influence other nations and events. Merely having a global presence does not equal having global power unless a nation influences events in a particular region or realm."¹⁶

Despite this partial power concept, it is difficult for US leaders to ignore forecasts of China's economy expanding by 8 percent annually through 2040 as predicted by Fogel or 5.6 percent through 2050 per the Carnegie Endowment model.¹⁷ No matter the actual growth rate, so long as it is greater than that of the United States, it is cause for concern within Washington given the power this cedes to China.¹⁸ For example, some Western corporations are unwilling to criticize China over a range of issues due to the financial power China wields over them.¹⁹ Asian nations may also be in the uncomfortable position of having to "choose between the two giants," based on China's growing strength.²⁰

The paradoxical state of the Chinese economy, however, is such that some of the major driving forces fueling its financial boom cannot remain in place once a certain level of power is reached. Based on this conflict, Samuel Huntington's observation that "economic growth and other increases in a country's capabilities often proceed along an S curve: a slow start and then rapid acceleration followed by reduced rates of expansion and leveling off" seems far more realistic when explaining China's rise.²¹

All of these trends could make China's rise alarming to the United States, but it may not be as powerful as initially seem on the surface. Significant limitations could slow growth. Although there are a multitude of factors contributing to China's economic rise and resulting US trade deficit, those most likely to challenge China's long-term economic

growth include the value of its currency, an uneven economy based on exports and state investment, and changing demographics that will reduce its workforce.

China's Devalued Currency

China has engaged in a deliberate policy of devaluing the yuan through currency pegging and currency restrictions to encourage significant foreign investment and manufacturing.²² While such policies have created an economic boom for China in recent years, its growing economic power will make it increasingly difficult to keep its currency value so low, potentially driving out foreign investment and manufacturing to other developing nations able to offer cheaper services.

Although it is easy to say Beijing simply devalues its national currency, the complexities of this are far more intricate. The devaluation of the yuan has been largely facilitated through fixing its value to the US dollar and avoiding its internationalization. Economists estimate that the yuan is devalued by 15 to 40 percent.²³ China accomplishes this through significant purchases of US Treasury bonds to ensure the value of the dollar remains higher than the yuan.²⁴

Salman Khan, a US economist and educator, uses a hypothetical example to clarify this interaction. He explains that if China exports \$50 million worth of goods to the United States, while it only imports \$20 million of US goods, a \$30 million trade deficit ensues. Chinese traders will exchange their 50 million US dollars for their own currency, while US traders will want \$20 million worth of that sum to convert the yuan to US currency. While the \$20 million worth is exchanged, there is a surplus of \$30 million flooding the market, and per supply and demand, the value of the dollar should fall accordingly. China, however, does not want the value of the US dollar to fall, as this would increase the relative value of the yuan and make Chinese manufacturing more expensive. Therefore, China uses its vast reserve holdings to buy the surplus US dollars, \$30 million in this example, to ensure the value of the dollar does not fall.²⁵ Unlike Khan's example, the actual 2012 US trade deficit with China was approximately \$315 billion.²⁶ While this illustration explains pegging and Chinese currency accumulation concepts, it is not the cause of the trade deficit itself. This involves multiple factors driving lower costs, thus higher consumer demand, for Chinese products. These are discussed in following sections.

This Chinese tactic of devaluing its currency by pegging it to the US dollar occurred from 1995 to 2005 and again from 2008 to essentially current times.²⁷ In 2005, the rate was approximately 8.1 yuan to the dollar and rose roughly 25 percent when it unpegged from the dollar in 2005.²⁸ When China reestablished the fixing policy in 2008, the rate was about 6.8 yuan to the dollar, but under global pressure, China announced in 2010 it would very gradually start to untie the yuan's fixed value from the dollar.²⁹ Some loosening has occurred, with the yuan currently valued at approximately 6.14 to the dollar; however, it still remains largely pegged to US currency.³⁰

In a similar vein, China has managed to keep the value of the yuan artificially low by currency restrictions and, until very recently, essentially avoided trading it in international markets. China's motivation for this policy has been the same as pegging the yuan to the dollar. Because of expanding Chinese industry and economics, the demand for a freely traded yuan would be high, driving up its value. The rise would subsequently mean more expensive Chinese goods and assembly, potentially pushing significant business to lower-cost nations. Banking executive Ken Miller states, "Beijing does not dare make its capital account convertible;" its export industry simply would not be the competitive giant it is now if the yuan were freely traded.³¹

Recent developments, however, indicate China may be taking Miller's dare. In 2009 China started to allow some nations to import and export using the yuan,³² and it has slowly allowed that list to increase to 19 countries and regions as of March 2013. Brazil and Australia are some of the most notable new additions to the list, and France, Great Britain, and Switzerland are also vying for similar arrangements. New and potential currency deals certainly indicate a significant appetite for internationalization of the yuan, and a recent report from international bank HSBC predicts further loosening of the yuan will make it one of the major globally traded currencies by 2015.³³ Despite these developments, the yuan still has substantial government controls and is not a free-market commodity allowed to reach its equilibrium value,³⁴ leading China to a substantial crossroads regarding its desire to become a global reserve currency versus the need to keep the value of the yuan low.

The global financial crisis created anxiety over US dollar holdings and with increasing fiscal confidence, China is starting to push for use of the yuan rather than the dollar or euro as a major international reserve

currency.³⁵ The dollar and euro made up about 90 percent of all foreign exchange reserves in early 2012 and account for approximately 74 percent of current international payments as the only currencies large and powerful enough to sustain the volume of international trading.³⁶ But confidence in these two currencies is waning, and some are looking to diversify with alternatives. Specifically, China no longer trusts the dollar, and many leaders in Beijing are making moves to promote replacing the dollar and euro with the yuan as a global reserve currency. To do this, though, China must unpeg the yuan and allow full international access for it to become a trusted international form of currency and reserves.³⁷ This means the value of the yuan is very likely to rise and the massive exports China relies on to fuel its economy will no longer be as attractive to foreign investors.

China cannot attain the economic influence needed to be considered a fiscal hegemon unless its currency is at least one of the major internationally traded and saved currencies. Thus, it cannot become the next global economic hegemon without the value of the yuan increasing, creating a major incongruity: can it become the leading global economic power without the artificial measures Beijing has put in place to fuel the economy? While China's economy can continue to grow, it will have difficulty becoming a global financial authority unless the yuan is freely traded, but China's economy is very likely to suffer if the yuan's value significantly increases. This dynamic will serve as a major growth restraint. While China is undoubtedly becoming a financial power, straight-line economic predictions on its imminent dominance must be adjusted.

Exports and the State-Fueled Economy

The International Monetary Fund (IMF) reported that "by 2003, China's export growth rate was seven times higher than the export growth rate recorded by the world as a whole,"³⁸ and exports only continue to thrive.³⁹ While this strategy has certainly succeeded in propelling China's international economy, that growth has come at significant expense to its domestic economy—that is, consumption within China and the average individual's buying power—creating what some have referred to as, "a lopsided giant."⁴⁰ Beijing's financial policies require strict government control to manipulate the value of the yuan, influence internal economics through interest rates and state investment, and protect Chinese banks from open competition which could have a significantly

upsetting effect on the Chinese economy.⁴¹ To achieve these three effects, China's government must possess considerable reserve holdings to buy US bonds, influence and invest domestically, and have enough assets to keep its domestic banking system isolated. Not only are reserves needed for these functions, but that need continues to grow as China's buying off currency surpluses to keep the yuan devalued forces it to continue reserve accumulation.⁴²

In 2010, Chen Zhiwu of MIT assessed that the Chinese government controlled approximately 70 percent of domestic assets,⁴³ and in February 2012 economist Adam Hersh testified before the US-China Economic and Security Review Commission that "government control over China's economy remains pervasive, including through direct ownership of virtually all of the formal financial system and much of the economy's productive assets."⁴⁴ The tactic of government control through reserve holdings may work for China in the short term, but without domestic stimulation, this unbalanced financial system will become a significant liability if foreign investments and exports continue to decline.

China's domestic consumption is the lowest among major global economies, at about 50 percent of US rates.⁴⁵ Claude Meyer describes this state versus household spending discrepancy by noting, "China's financial might demonstrates the power of the State, financial institutions and businesses, but does not in any way reflect the situation of its households, whose income lies between that of El Salvador and Egypt."⁴⁶ In addition to insufficient cash flow failing to stimulate domestic spending, government interest rate controls are leading to minimal investment, saving, and wealth accumulation.

The government in Beijing, through a closed banking system with no competition, has kept interest rates it pays savers low, while the interest rates it charges borrowers are significantly higher than normal market forces would dictate. According to the Wharton School of Business, in 2010 China's tightly governed interest rate spread between what borrowers are charged and savers are paid was 1.5 to 2.5 percentage points larger than other banks around the world which allow free-market forces to determine rates.⁴⁷ This controlling practice leads to wealth accumulation for Chinese banks, and hence the Chinese government,⁴⁸ which is needed to buy off foreign surpluses to devalue the yuan. It also creates yet another dynamic where the Chinese population has little ability to generate wealth. Artificially low interest rates may not keep up with

inflation, creating an actual *negative* net return for savers.⁴⁹ Chinese investors have few options for better returns due to significant restrictions on domestic savers investing anywhere except Chinese banks.⁵⁰ Additionally, these abysmal saving options force many domestic consumers to put aside additional income to cover necessities such as health care or education, further stagnating the domestic consumption engine.⁵¹

Vice Premier Li Keqiang's 2010 comments on an "irrational economic structure . . . [and] uncoordinated and unsustainable development" indicate China's awareness of the problem.⁵² Yet in June 2012, both lending and deposit interest rates were cut equally by 25 percent,⁵³ and in July 2012, rates were lowered again but this time slightly unequally, narrowing the rate spread by 0.06 percent.⁵⁴ While a slightly smaller rate spread is a step in the right direction, it is questionable how much lowering rates in a way that benefits borrowers, but not individual savers, might stimulate Chinese domestic growth.

The summer of 2012 also witnessed slightly relaxed rate restrictions, with Chinese banks allowed to set rates as low as 70 percent of the benchmark for loans and up to 110 percent of par for deposits.⁵⁵ While these changes lend hope for further loosening of restrictions, Chinese banks are still highly controlled by a government which needs profits to fuel its export-driven yuan pegging. The lower lending rate may stimulate some domestic improvements, but China's overall interest rate picture can be viewed as supporting its export rather than domestic economy. Unfortunately for those who would initiate reform, a devalued yuan and low interest rates fuelling exports at the expense of domestic spending are profitable for the most powerful. Sebastian Mallaby and Olin Wethington explain in their 2012 article:

State-owned banks do not want to pay depositors market interest rates. Politically connected borrowers, such as state-owned construction companies that build China's impressive infrastructure, do not want to give up access to cheap capital. Politically connected exporters, on whom provincial governors count to create jobs in their regions, do not want to give up the advantage created by the favorable exchange rate. Groups that have an interest in reform—savers who receive artificially low returns and consumers who pay a high price for imports—are no match for powerful producers.⁵⁶

A final aspect to this lopsided picture, but perhaps one of the most important dynamics to the current economic boom, is massive state investment in Chinese industry.⁵⁷ According to Asian economic theorists Michael Pettis and Claude Meyer, China is following a model that others,

including Japan, have used to jumpstart a national economy. In very basic terms, the model prescribes that nations with little industry or infrastructure inject significant government investment to establish a subsidized and, therefore, very competitive industrial and production base. This, in turn, starts measurable foreign trade and the accumulation of reserves, which a nation can further inject into its industrial capacity and enter the global financial stage.⁵⁸ In China's case this model has thus far been highly successful, with its "abundant savings deposits and vast resources of labour" proving a powerful engine to support its industrial might.⁵⁹ As Pettis and Meyer point out, however, the model is not sustainable. At a certain point every new industrial enterprise is no longer necessary, some of the significant government investments fund unprofitable enterprises, and debt begins to accumulate. Pettis describes more specifically China's use of this model:

China has the highest investment rate ever recorded, and the highest growth rate of investment probably ever recorded, [such] that we start to run out of economically viable projects. But because the system was so geared toward continuous increases in investments, we keep on investing, and when that happens, investments become allocated into projects that do not generate sufficient real returns.⁶⁰

Similar to the devaluation of the yuan, this tactic of government-supported industry may have sparked a near-term boom but set the stage for longer-term fiscal problems. The global economic crisis of 2008 succinctly demonstrates China's long-term problem with its state investment strategy. When the global crisis impacted exports and its domestic economy was not able to absorb the downturn, the Chinese government introduced a two-year stimulus plan in 2008 worth \$600 billion. While this indeed sparked some short-term growth, it has created the potential for even more debt while doing nothing toward fixing a more fundamental problem of a poor domestic economy and low household incomes.⁶¹ Meyer explains the recent stimulus, though the issue he raises also illustrates the larger problem with the industrial investment model China started decades ago:

The surge in [2008] bank lending has exacerbated industrial overcapacity and may fuel a property and stock market bubble, the bursting of which would leave a massive overhang of bad debt. Even more worrying, the stimulus plan has worsened rather than improved the quality of growth. Investment has taken over from faltering external demand and was responsible for over 90 percent of growth in 2009. Continuing in 2010, the stimulus plan did little to redirect the Chinese economy toward stronger domestic demand.⁶²

While reserve holdings, artificial interest rates, and government investment in industry have helped fuel the Chinese economic boom, it could be at the expense of long-term financial health. For China to remain on a relatively stable economic growth trajectory, its domestic consumption must be able to absorb downturns in exports which could result from factors such as the global financial crisis and the yuan's increasing value. Despite China's apparent awareness, as evidenced in Vice Premier Li's comments, its ability to grow a domestic spending engine simply may not compensate quickly enough for the downturn in exports caused by an increasingly powerful yuan.⁶³

Therefore, experts contend the tools China will need to effect actual domestic financial reform will be at the expense of those it uses to artificially stimulate its economy. Higher interest rates and actual returns on savings will give the average Chinese consumer more confidence to spend rather than set aside earnings. Similarly, a looser market and rising yuan will also increase Chinese spending by giving consumers more international purchasing power and increasing imports. Yet, exports and state profits gained through exports and low deposit rates will suffer, as well as the degree of Chinese government control over the economy. Hence, whether due to exports lagging and domestic consumption unable to fill the gap or balancing the export giant by generating a sound domestic market at the expense of "comparative advantages" such as substantial government investment or a devalued yuan,⁶⁴ there may be a significant slowing effect on Chinese economic growth.

Chinese Demographics

The Chinese workforce is approximately 900 million to 1.34 billion strong,⁶⁵ fueling a significant production base for China's export boom with its cheap labor the "driving force behind their industrial competitiveness."⁶⁶ Two critical factors, China's one-child policy and its lack of health care, however, may cut away at these numbers and greatly reduce the masses available to work in assembly lines, factories, and production facilities. It is this future impact to the available workforce that will serve as the final influence to plateau Chinese economic expansion.

Different sources cite slightly different fertility rates in China today, but the child-to-mother ratio ranges from 1.1 to 1.56 thanks to the one-child policy.⁶⁷ At the same time, a dynamic called replacement rate, which is the fertility rate a population requires to remain at relatively

constant numbers, is currently 2.1 children per mother for China.⁶⁸ This discrepancy indicates a population decline at some future point. The UN estimates China's population will peak in 2015, followed by a rapid drop-off as a direct result of the one-child policy.⁶⁹ A ripple effect of the one-child policy will lead to further decreases in coming generations due to significantly more boys than girls being born, as Chinese culture favors male offspring, leading to some female infanticide, or more commonly, sex-selective abortions. Therefore, "In about 20 or 25 years' time, there will not be enough brides for almost a fifth of today's [Chinese] baby boys—with the potentially vast destabilizing consequences that could have."⁷⁰

A final effect of the policy is an aging population. Because Chinese children are not replacing their elders in equivalent numbers, the percentage of the population over the age of 60 is expanding, while the percentage of those below 14 is falling.⁷¹ An older population will significantly reduce the work force, with China's 2010 ratio of nine laborers per retiree falling to just four per retiree by 2030.⁷² The aging population also means an increased health care burden. A World Health Organization study predicts China's "burden of diseased population" as a percentage of overall population will rise dramatically from 44 percent in 2004 to 65 percent in 2030 due to its elderly increase.⁷³ Thus, the coming decades will see the one-child policy significantly eat away at China's overall population and masses of cheap labor, and the increasing portion of elderly Chinese will add an additional burden to that decreasing workforce.

While demographic impacts of the one-child policy will impact China's approximately billion-strong workforce as early as 2015, the growing health crisis will also factor into its economic future. Yanzhong Huang, a senior fellow for global health at Seton Hall University, has termed China, "the sick man of Asia," based on the alarming rates of disease and sickness there today. China leads the world in diabetes and noncommunicable diseases such as cancer; has a significant and increasing HIV/AIDS threat; accounts for one-third of worldwide hepatitis B virus carriers; and faces a burgeoning mental health crisis with data suggesting an approximate 50 percent rate of mental illness.⁷⁴ Many of these problems stem from an aging population but also from China focusing on manufacturing and GDP growth rather than any type of

effective health care system. While officials are starting to reform health care, it still has a long way to go.⁷⁵

Government investment in health spending has increased since 2002, and the Chinese government now reports 94 percent of its population has some sort of health care coverage. Despite this seemingly positive trend, the system is government-run with an inefficient structure, suffers from rampant corruption, and emphasizes care in urban areas at the expense of rural ones. Therefore, the reality is closer to the coverage provided by a 2010 rural cooperative program that technically covers individuals, but only at the rate of “8.6 percent of total health-care expenditures per capita.”⁷⁶ This means many average citizens have to set aside savings to cover potentially significant out-of-pocket expenses for health care at the cost of domestic spending. As Huang explains, “When people have to worry about expensive medical bills, they are less likely to spend money on other things. Between the mid-1990s and 2006, more than 50 percent of total health care spending was out-of-pocket payments.”⁷⁷ Unfortunately, the situation may be difficult to resolve. The Yale-China association highlights that China may struggle to find an easy solution with significant obstacles to providing quality care, including “a hybrid market-socialist society,” no established health insurance industry, and low per-capita income.⁷⁸

While this is a dismal state of affairs in human terms, it will also hit China on an economic level. Widespread health issues mean a loss of productivity; a 2011 report by economists and health care experts concluded that in 2005 China lost a sum equivalent to 13 percent of its GDP due to disease and lost labor.⁷⁹ An aging population with little health care will also push workers to spend less time on the production line and more time taking care of elderly parents and grandparents.⁸⁰ And finally, as with low interest rates, significant out-of-pocket health expenses for not only an individual worker, but an aging family as well, means less money going into the domestic Chinese economy.⁸¹

China is beginning to add more health reforms, and prudent measures to improve the quality of health care and insurance coverage may solve some of these issues. Although true, it will be at the expense of production, as expressed by Salvatore Babones: “Today’s little emperors will spend their most productive years taking care of their parents. And as they do, China’s economic activity will have to move away from high-productivity manufacturing and toward low-productivity health

services.”⁸² Jack Chow of Carnegie Mellon University paints a slightly more promising picture with Beijing further increasing health reforms in 2009 and government programs leading to a 3 percent drop in child mortality and incidents of tuberculosis decreasing 45 percent from 2000 to 2010.⁸³ While these trends are good news for Chinese citizens and one hopes they persist, continued health care improvements will divert funds from practices allowing continued GDP expansion. According to Meyer, “The financial cost of such a [health] system is likely to become increasingly onerous, and perhaps even crushing, as the population ages and the labour force shrinks as it will from 2015–20.”⁸⁴ Whether lost workdays and household health care costs limit domestic spending or Beijing decides to spend resources to overhaul its health system, either path will cost China and impact its economy.

Thus, the combined effect of the one-child policy and an impending health-care-related slowdown is likely to influence China’s ability to produce at current rates. Its leaders clearly understand this exports-based, state-capital-infused, and cheap-labor-driven economy is not sustainable, and the Chinese government has emphasized increasing productivity to fill the gap. A 2011–15 “Five Year Plan” has been put in place which will, among other things, put a premium on productivity, with rewards/repercussion for companies based on efficiency performance.⁸⁵ Since China is currently in the lower ranks on the global productivity-per-worker scale, there is room for substantial improvement.⁸⁶ It is possible then, that it may offset the decline in workforce with increased productivity. Despite the potential for increased production technology reducing the number of workers needed,⁸⁷ it is still conceivable a significant reduction in the workforce will hamper China’s cheap exports machine. Whether this is through less capacity to produce or higher wages to a smaller but more skilled workforce, it will be further impacted by the possible effects of a “crushing” health care crisis. Although challenging to accurately predict, it is quite feasible all these factors will have an overall negative influence on China’s capacity to produce through 2015–30 as both population decline and the health crisis begin to fully bear their weight.

Implications for US Policy

The preservation of commercial and financial interests constitutes now a political consideration of the first importance, making for peace and deterring from war.

—Alfred Thayer Mahan, July 1902

Forecasting China's economic and, therefore, military and political power in the coming decades with any precision is difficult due to a vast range of changing dynamics. These include some important issues not discussed here, such as its vast consumption of raw materials, the global oil market, and ecological factors. What does seem clear, however, is that an undervalued yuan, large state investment, and masses of cheap labor are not sustainable, leading to an eventual economic slowdown. Given this likelihood of China *not* surpassing the United States economically in the coming decades and settling into a position of "partial power," as David Shambaugh suggests, what are the implications for US policy toward China?

Economics as a Policy Tool

Foremost, one must understand the potential for misunderstandings is high. Headlines proclaiming China's economy will overtake that of the United States in 20–30 years or that China holds 22 percent of US foreign debt may strike fear in the hearts of US officials and the American public, leading to shortsighted policies and unhelpful rhetoric. A Pew Research Center poll found that at the end of 2009, 53 percent of Americans viewed China as a major threat, while 44 percent thought China was the world's leading economic power compared to the 37 percent who thought the United States had the foremost financial strength.⁸⁸ Such factors may be easy targets for political candidates to exploit, which only strengthens the escalation potential of such rhetoric.

US leaders need to understand that China's economy is not as threatening as a cursory analysis might indicate. This does not mean China's monetary rise should not demand significant attention. On the contrary, US policymakers must dig deeper to see China is an emerging power with significant growing pains yet to overcome and with considerable dependence upon the United States. Rather than viewing China's growing economy as a threat, it must be continually analyzed and understood

to find ways to work toward mutual benefit rather than allowing misunderstanding and fear to drive inappropriate headlines or policies.

Claude Meyer asserts, “The United States is a key [Chinese] economic partner at the moment, but it is American hegemony that will ultimately be challenged. The quest for supremacy in Asia is just a step on the way. . . . There can be no doubt that considerable tension will remain.”⁸⁹ This tension, along with press reports and slightly frenetic attitudes of China overtaking US hegemony, has potential to lead to US missteps which must be avoided. Shambaugh supports this concept in his comments on overestimating China’s dominance:

China is certainly not about to “rule the world,” [as] in the estimate of Martin Jacques’s recent popular book. To the contrary, as Joseph Nye has observed: “The greatest danger we have is overestimating China and China overestimating itself. China is nowhere near close to the United States. So this magnification of China, which creates fear in the U.S. and hubris in China, is the biggest danger we face.”⁹⁰

Understanding not only China’s long-term economic sustainability challenges, but also the interrelationship between the economies of China and the United States is important for developing policy and successfully navigating these tensions. One of the more significant concerns is China’s massing of US securities, which could confer substantial power over the US economy. Due to China’s need to buy US trade-deficit funds, primarily US Treasury bonds, its holdings of US assets was an impressive \$1.16 trillion in September 2012—approximately 22 percent of US foreign debt.⁹¹ While this has been a source of anxiety in terms of China’s potential impact and power over the US economy, it also leverages significant US influence over the Chinese economy. Estimates put China’s foreign exchange reserve, arguably the bedrock of its economy, at approximately 70 percent in US dollars.⁹² China has just as much cause to feel uncomfortable about the economic relationship as the United States.

Some contend that China selling off US securities or significantly lowering its US investment rate represent their two largest economic concerns.⁹³ Both would flood the market with US assets and lower the value of the dollar, not to mention introducing significant flux into the US economy. The potential for these actions also calls into question the extent of influence such involvement in the US dollar confers to China.

Although these three concerns are legitimate, China's economic threat may not be as one-sided and powerful as it initially seems.

While any large-scale selloff of US Treasury bonds would lead to the US dollar falling, this would also diminish the value of China's sizable savings in US dollars. Further, the United States constitutes China's largest export market.⁹⁴ If the value of the US dollar falls and the US economy declines, Chinese export profits will suffer. China could deliver an economic blow to the United States by rapidly selling US Treasuries; however, any lessening of the dollar's value or the purchasing power of the US consumer will subsequently impact China by reducing the value of its vast savings in US dollars and its ability to export to US consumers.

There is also concern that China will stop investing so heavily in US Treasuries for any number of reasons, including diversifying its financial holdings or investing in domestic Chinese programs instead. While a slow and deliberate reduction of Chinese investment could even be positive for the United States if it means unpegging the yuan, an abrupt and significant decrease from current levels could be considerably detrimental to the US economy if it does not allow for other markets to fill the void. As noted in a recent report to Congress, "Given [a] relatively low savings rate, the US economy depends heavily on foreign capital inflows from countries with a high savings rate (such as China) to meet its domestic investment needs and to fund the federal budget deficit."⁹⁵ A rapid reduction of Chinese purchases will have a similar effect on large-scale sales of US Treasuries, in that a surplus of assets will inundate markets, and the value of the US dollar will fall. While the US economy will no doubt suffer in the event of a rapid reduction of Chinese investment, so will China's. Once again, the Chinese action impacting the dollar will produce a counteraction to lessen the value of China's vast US holdings and reduce its exports to the United States so long as the current state of dependency exists. China cannot fiscally wound the United States without also hurting itself.

As long as US leaders understand these interactions, China has little influence to bend US markets and policies to its will through economic intimidation or otherwise, as it has much to lose if US markets fail. As viewed from the Chinese perspective, the United States has significant influence over China's economic future as the controller of that asset. Further, and in the most extreme and abysmal of circumstances, should the two nations come to outright hostilities, those US Treasury bonds

representing most of China's national wealth are unlikely to be honored and may well turn the vast Chinese savings into a worthless pile of IOU notes. US economic reliance on China is unquestionable and understandably uncomfortable; nevertheless, China is just as much a hostage of US economic policies. This marriage somewhat negates the question of untoward Chinese influence over US policy, and the threat of hostile Chinese economic actions wanes with an understanding of the second-order effects US finances have on China. The US economy's reliance on China may not be comfortable, but China is also dependent, with that dependency conferring still significant US leverage over China if required.

In determining US policy toward China then, the bottom line is the use of economics as a policy tool can and should be employed if necessary to forestall physical conflict. There are global precedents for the use of economics as a weapon in warfare. Nicholas Lambert's *Planning Armageddon* outlines Great Britain's plan to destroy Germany fiscally at the outset of World War One as an alternative to continental warfare. The economic plan was executed in August 1914 to such effect that after just three weeks, neutral nations and powerful bankers successfully pressured the British government to stop, based on fears of the impact on global markets. Assuming the war would be quickly won anyway, Britain succumbed to pressure and quickly ended the economic warfare plan and, in its place, carried out a drastically reduced fiscal attack in the form of a naval blockade on Germany.⁹⁶ One must wonder how much might have been saved had Britain carried through on its economic plan instead?

Another example is that of the United States pressuring the United Kingdom to withdraw from Egypt in the Suez Crisis of 1956. The pound sterling's stability and value was key to British economics, and the UK's outflow of financial reserves at the time was seriously threatening the pound in comparison to the dollar. To save the pound sterling, the UK needed a massive inflow of currency through, at the time, the essentially US-controlled IMF. The United States successfully used this leverage to force Britain out of Egypt with the incentive of an IMF bailout; "The United Kingdom's need for financial assistance gave the Americans the perfect lever to force an immediate withdrawal."⁹⁷

Aside from historic examples, economist Robert Ross cites more recent instances of this working for the United States with respect to China: "In bilateral economic relations, the United States has negotiated

with China to resolve conflicts arising from Chinese protectionism and from Beijing's inadequate protection of intellectual property rights. In each case, Washington has used coercive tactics to elicit near one-sided Chinese compliance."⁹⁸

More specifically, in 1992 the United States threatened significant economic sanctions if China did not make considerable trade reforms allowing increased external access to Chinese markets, and by 1995 most requested reforms were in place. Perhaps most important was China's 2001 accession into the World Trade Organization (WTO), which occurred only after it completed a number of trade reforms requiring years of negotiation and coming primarily at the behest of the United States and the European Union.⁹⁹

Despite an apparent working relationship on the economic front, the same cannot be said for US military and diplomatic relations with China. Chinese aggression in the South China Sea, its military buildup with opaque strategic intent, and cyber intrusions are just some concerns where the United States has recently tried to exert diplomatic and military power to clarify or change Chinese actions. Despite considerable effort and increased US military presence in Southeast Asia, the United States has had little to no success in altering these Chinese activities.¹⁰⁰ On the other hand, the instances of fiscal pressure account for just a few examples of US economic power, and many more fiscal issues have been resolved through US pressure and threats of economic sanctions.¹⁰¹ Although these illustrations have far deeper complexities than presented here, they demonstrate the general trend of China bending to US pressure when that pressure is in the form of an economic rebuke rather than political or military threats.

Conclusion: US Foreign Policy and China

"Treat China as an enemy," goes one piece of well-worn conventional wisdom, "and it will become one."

—Aaron Friedberg, *A Contest for Supremacy*

China is unlikely to sustain its current economic growth rates and surpass the United States, thus leaving US hegemony probable for at least the near future. China and the United States work best on the economic level, with the United States being somewhat successful in

pressuring China into reforms through the weight of economic sanctions. The United States also has significant leverage over China because its wealth is dependent, at least for now, on the health of the US dollar. Historical precedence also demonstrates fiscal power can be a potent tool when applied to other nations.

When considering these aspects of US foreign policy toward China, one must also consider Paul Kennedy's point that economics is the support base of all other forms of national power, and ensuring that defense spending and economic growth remain in healthy equilibrium is essential for long-term national success. The United States may be in danger of overstretch and tipping the balance too far toward military spending at the expense of the US economic engine.¹⁰² Binding together all these concepts could lead to the belief that US foreign policy toward China should allow significantly more flexibility than directed by the 2012 *Sustaining US Global Leadership* strategic guidance emphasis on the "re-balance toward the Asia-Pacific region."¹⁰³ This would possibly ease tensions while also allowing the United States more resources to spend on strengthening its economy. Yet, what about China's continued lack of recognition of international norms?

Chinese economic practices are at times outside of international trading norms as they give China a significant advantage over other trading bodies, but there are also issues such as China increasingly ignoring international and UN convention by claiming much of the South China Sea for its abundant resources.¹⁰⁴ How should the United States react if China's aggressive actions in the South China Sea continue and freedom of navigation in international waters is restricted, or Chinese actions infringe upon the claims of US allies? While these examples are by no means exhaustive and omit important issues such as human rights concerns, cyber intrusions, and Chinese resource consumption, they highlight the US problem. The ultimate challenge then is creating US policy that avoids conflict and promotes a prosperous relationship with a rising China while also ensuring China does not unfairly violate international norms nor threaten US interests or those of US allies.

For Washington to hold the line on its interests, while engaging China in a productive way, US leaders must find a way to maintain their position without becoming so threatening that China feels pushed toward war. On the positive side, the United States has many nonphysical tools at its disposal to achieve this balancing act. With the United States likely

to remain more powerful despite current economic faltering, these tools could include fiscal pressure and sanctions, including limiting China's access to US markets. At the extreme end of the spectrum, should US-China relations turn considerably negative, are measures which take advantage of the US-controlled currency that dominates China's reserve base. The most drastic of these could include defaulting on the vast US Treasuries China maintains to dilute its economic power, accepting that the follow-on effects to the US economy and credit rating are preferable to all-out war.

Taking advantage of a future Chinese economic slowdown or fiscal levers, however, requires Washington to adopt a long-term approach. Unfortunately, this is something US leaders are often not well placed to do within election-cycle politics and the resulting need for immediacy. Notwithstanding, US policymakers must consider digging in and waiting out China's economic boom. Although this may often be difficult politically, the importance of maintaining a working US-Chinese relationship cannot be overlooked, with significant implications or even physical conflict if it is pressed too hard or mishandled. Consequently, US policymakers must factor the potential for China to have less relative power in the coming years than it currently enjoys and make appropriate long-term choices on how hard to press for resolutions as a result.

Along with long-term fortitude, fiscal pressure may be useful to safeguard US interests. This concept should not just apply in the economic arena, but—similar to the British economic attack on Germany in World War One and US economic pressure on the UK through the IMF over the Suez crisis—fiscal action should be the first response to most Chinese actions requiring a US response. The use of economics to push Chinese compliance should apply to a host of issues, both inside and outside of the fiscal arena, such as WTO violations, cyber intrusions, or territorial violations in the South China Sea.

US-Chinese policy will require constant analysis and tending. A fundamental understanding of China's fiscal future with consideration of a long-term approach and economic pressure, or even attack, as the first response will be paramount to success. The United States will always require a strong military to back fiscal pressure. Indeed the diplomatic and military tools of US national power in addition to fiscal pressure will add depth and credibility to any economic policy meant to protect US interests. The balance required to steer the two nations away from

conflict and toward a productive relationship while protecting US interests, however, may be far more achievable if first viewed and conducted from an economic perspective. ■■■

Notes

1. Martin Jaques, *When China Rules the World*, 2nd ed. (London: Penguin, 2012), 8.
2. Paul Kennedy, *The Rise and Fall of Great Powers* (London: Fontana, 1989), xvi.
3. Henry Kissinger, "The Future of U.S.-Chinese Relations," *Foreign Affairs* 91, no. 2 (March/April 2012): 44–48.
4. Kennedy, *Rise and Fall*, 665–78.
5. Aaron Friedberg, *A Contest for Supremacy* (New York: Norton, 2011), 33.
6. Yang Yao, "The End of the Beijing Consensus," *Foreign Affairs*, 2 February 2012, <http://www.foreignaffairs.com/articles/65947/the-end-of-the-beijing-consensus>. The economic growth rate is also supported by "China GDP Annual Growth Rate," *Trading Economics*, April 2013, <http://www.tradingeconomics.com/china/gdp-growth-annual>.
7. "China Overtakes Japan as World's Second-Biggest Economy," *BBC News*, 14 February 2011, <http://www.bbc.co.uk/news/business-12427321>.
8. "China Owns a Lot of US Debt. Why?" Kearny Alliance, 5 September 2011, <http://www.chinaglobaltrade.com/article/why-chinese-holdings-us-government-debt-so-large>; and Arvind Subramanian, "Inevitable Superpower," *Foreign Affairs* 90, no. 5 (September/October 2011): 71.
9. Subramanian, "Inevitable Superpower," 78, 68.
10. Friedberg, *Contest for Supremacy*, 32.
11. Robert Fogel, quoted in *ibid.*, 32–33.
12. Robert Fogel, "\$123,000,000,000,000* (*China's Estimated Economy by the Year 2040; Be Warned)," *Foreign Policy*, January/February 2010, <http://www.foreignpolicy.com/articles/2010/01/04/1230000000000000?page=0,0>.
13. Robert Fogel, "Why China is Likely to Achieve Its Growth Objectives," National Bureau of Economic Research Working Paper Series no 12122, March 2006, 3; and Fogel, "\$123,000,000,000,000."
14. "Dating Game: When Will China Overtake America?" *Economist*, 16 December 2010, <http://www.economist.com/node/17733177>.
15. Fogel, "\$123,000,000,000,000."
16. David Shambaugh, *China Goes Global: The Partial Power* (New York: Oxford University Press, 2013), 8.
17. Salvatore Babones, "The Middling Kingdom," *Foreign Affairs* 90, no. 5 (September/October 2011): 79–80.
18. Martin Indyk, Kenneth Lieberthal, and Michael O'Hanlon, "Scoring Obama's Foreign Policy," *Foreign Affairs* 91, no. 3 (May/June 2012): 32–33.
19. Keith Bradsher, "Sitting out the China Trade Battles," *New York Times*, 23 December 2010, <http://www.nytimes.com/2010/12/24/business/global/24trade.html>.
20. Indyk, Lieberthal, and O'Hanlon, "Scoring Obama's Foreign Policy," 33.
21. Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York: Touchstone, 1997), 83.
22. See Sebastian Mallaby and Olin Wethington, "The Future of the Yuan," *Foreign Affairs* 91, no. 1 (January/February 2012): 137–38; and David Barboza, "China's Treasury

Holdings Make US Woes Its Own,” *New York Times*, 18 July 2011, <http://www.nytimes.com/2011/07/19/business/china-largest-holder-of-us-debt-remains-tied-to-treasuries.html?pagewanted=all>.

23. “China Owns A Lot Of US Debt.”

24. See Salman Khan, “China’s Currency Peg: CNBC Explains,” *CNBC*, 16 June 2011, http://www.cnbc.com/id/43295777/China_s_Currency_Peg_CNBC_Explains; and Barboza, “China’s Treasury Holdings.”

25. Khan, “China’s Currency Peg.”

26. “2012: US Trade With China,” US Census Bureau, <http://www.census.gov/foreign-trade/balance/c5700.html>.

27. Peter Goodman, “China Ends Fixed-Rate Currency,” *Washington Post*, 22 July 2005, <http://www.washingtonpost.com/wp-dyn/content/article/2005/07/21/AR2005072100351.html>; and Michael Wei and Allister Bull, “Peg is Dead as China Vows Yuan Flexibility before G20,” Reuters, 19 June 2010, <http://www.reuters.com/article/2010/06/19/us-china-yuan-idUSTRE65I11B20100619>. Both these articles and the exchange rate index found at “Yuan Renminbi to US Dollar Exchange Rate,” *IndexMundi*, <http://www.indexmundi.com/xrates/graph.aspx?c1=CN¥&c2=USD&days=180> indicate that currency pegging still exists.

28. Goodman, “China Ends Fixed-Rate Currency”; and Zhou Xin and Simon Rabinovitch, “China Expands Yuan’s Role to Overseas Investment,” Reuters, 13 January 2011, <http://www.reuters.com/article/2011/01/13/china-yuan-investment-idUSTOE70C05Z20110113>.

29. Wei and Bull, “Peg Is Dead.”

30. “Yuan Renminbi to US Dollar Exchange Rate,” as of December 2013.

31. Ken Miller, “Coping with China’s Financial Power,” *Foreign Affairs* 89, no. 4 (July/August 2010), <http://www.foreignaffairs.com/articles/66466/ken-miller/coping-with-chinas-financial-power>.

32. Xin and Rabinovitch, “China Expands Yuan’s Overseas Investment.”

33. Maria Levitov, Ye Xie, and Lyubov Pronina, “London Gains First-Mover Advantage in EU’s Yuan Race,” Bloomberg, 13 March 2013, <http://www.bloomberg.com/news/2013-03-12/london-gains-first-mover-advantage-in-eu-s-yuan-race-currencies.html>.

34. See “Australian Central Bank to Invest in Chinese Bonds,” *New York Times*, 24 April 2013, http://www.nytimes.com/2013/04/25/business/global/australian-central-bank-to-invest-in-chinese-bonds.html?_r=0; and Joe Leahy, “Brazil and China Agree Currency Swap,” *Financial Times*, 26 March 2013, <http://www.ft.com/cms/s/0/3e20302e-9632-11e2-9ab2-00144feabdc0.html#axzz2SEhsa5R>.

35. See Mallaby and Wethington, “Future of the Yuan,” 135; Levitov, Xie, and Pronina, “London Gains First-Mover Advantage”; and Barry Eichengreen, “When Currencies Collapse,” *Foreign Affairs* 91, no. 1 (January/February 2012): 117–29.

36. Eichengreen, “When Currencies Collapse,” 117; and “Year of the Yuan: China’s Explosive Currency Goes Global,” *RT.com*, 1 May 2013, <http://beforeitsnews.com/opinion-conservative/2013/05/year-of-the-yuan-chinas-explosive-currency-goes-global-2632242.html>.

37. See Mallaby and Wethington, “Future of the Yuan,” 135; and Eichengreen, “When Currencies Collapse.”

38. Javier Silva-Ruete, “The Development of China’s Export Performance,” International Monetary Fund, 7 March 2006, <http://www.imf.org/external/np/speeches/2006/030706.htm>.

39. Mallaby and Wethington, “Future of the Yuan,” 135.

40. Miller, “Coping with China’s Financial Power.”

41. Exports and reserve holdings from Mallaby and Wethington, "Future of the Yuan," and interest rates and Beijing's economic control from Derek Scissors, "The Great China Debate: The Wobbly Dragon," *Foreign Affairs* 91, no. 1 (January/February 2012): 174.
42. Scissors, "Great China Debate," 173–74.
43. Kevin Hamlin, Vincent Ni, and Li Yanping, "China Seen Robbing Consumers with Low Interest Rates," Bloomberg, 6 August 2010, <http://www.bloomberg.com/news/2010-08-06/china-rates-seen-robbing-consumers-to-help-banks-as-5-growth-risk-looms.html>.
44. Adam Hersh, "Chinese State-Owned and State-Controlled Enterprises: Testimony before the U.S.-China Economic and Security Review Commission," Center for American Progress Action Fund, 15 February 2012, <http://www.americanprogressaction.org/issues/economy/report/2012/02/15/11069/chinese-state-owned-and-state-controlled-enterprises/>.
45. Wayne Morrison, *China's Economic Rise: History, Trends, Challenges and Implications for the United States* (Washington: Congressional Research Service [CRS], September 2013), 29, <http://www.fas.org/sgp/crs/row/RL33534.pdf>.
46. Claude Meyer, *China or Japan: Which Will Lead Asia?* (London: C. Hurst and Co., 2011).
47. "China's Interest Rate Regime: Paying a High Price for Cheap Credit," *Knowledge@Wharton*, September 2010, <http://knowledge.wharton.upenn.edu/article/chinas-interest-rate-regime-paying-a-high-price-for-cheap-credit/>.
48. See Morrison, "China's Economic Rise," 29; and Hamlin, Ni, and Yanping, "China Seen Robbing Consumers."
49. Morrison, "China's Economic Rise," 29.
50. Scissors, "Great China Debate," 173–77.
51. Hamlin, Ni, and Yanping, "China Seen Robbing Consumers."
52. Ibid.
53. Zhou Xin et al., "China Reduces Interest Rates for First Time since 2008," *Bloomberg*, 7 June 2012, <http://www.bloomberg.com/news/2012-06-07/china-cuts-interest-rates-for-first-time-since-2008.html>.
54. Jamil Anderlini, "China Cuts Rates amid Growth Fears," *Financial Times*, 5 July 2012, <http://www.ft.com/cms/s/0/a59f6a26-c694-11e1-963a-00144feabdc0.html#axzz2Jkz3jj8C>.
55. Chris Oliver, "China's Central Bank Cuts Lending, Deposit Rates," *Wall Street Journal*, 5 July 2012, <http://www.marketwatch.com/story/chinas-central-bank-cuts-lending-deposit-rates-2012-07-05-81034410>.
56. Mallaby and Wethington, "Future of the Yuan," 139–40.
57. Meyer, *China or Japan*, 36.
58. See Adam Taggart, "Michael Pettis: The Future of China," *Peak Prosperity* (podcast), 17 August 2013, <http://www.peakprosperity.com/podcast/82631/michael-pettis-future-china>; and Meyer, *China or Japan*, 35.
59. Meyer, *China or Japan*, 43.
60. Taggart, "Michael Pettis."
61. Meyer, *China or Japan*, 74–75.
62. Ibid., 75.
63. Hamlin, Ni, and Yanping, "China Seen Robbing Consumers."
64. Meyer, *China or Japan*, 51.
65. Ibid., 44; and "The Most Surprising Demographic Crisis," *Economist*, 5 May 2011, <http://www.economist.com/node/18651512>.
66. Meyer, *China or Japan*, 35.
67. These articles illustrate the issue of differing fertility rates: "Most Surprising Demographic Crisis" (1.4 fertility rate); "China's Achilles Heel," *Economist*, 21 April 2012, <http://>

www.economist.com/node/21553056 (1.56 fertility rate); and Te-Ping Chen, "China Frets Over Low Fertility Rates," *Wall Street Journal: China*, 7 March 2012, <http://blogs.wsj.com/chinarealtime/2012/03/27/hong-kong-frets-over-low-fertility-rates/> (1.1 fertility rate).

68. Both articles cite a 2.1 replacement rate: "Most Surprising Demographic Crisis"; and Chen, "China Frets Low Fertility Rates."

69. Meyer, *China or Japan*, 44.

70. "Most Surprising Demographic Crisis."

71. Ibid.

72. Meyer, *China or Japan*, 56.

73. Somnath Chatterji et al., "The Health of Aging Populations in China and India," *Health Affairs* 27, no. 4 (July 2008): 1052–63, <http://content.healthaffairs.org/content/27/4/1052.full>.

74. Yanzhong Huang, "The Sick Man of Asia," *Foreign Affairs* 90, no. 6 (November/December 2011), <http://www.foreignaffairs.com/articles/136507/yanzhong-huang/the-sick-man-of-asia>. The increasing HIV/AIDS threat is also discussed in Deborah Davis and Nancy Chapman, "Turning Points in Chinese Health Care: Crisis or Opportunity?" *Yale-China Health Journal* 1 (Autumn 2002): 6, <http://www.yalechina.org/docs/26.%20Health%20Journal%202002.pdf>.

75. Huang, "Sick Man of Asia."

76. Ibid.

77. Ibid.

78. Davis and Chapman, "Turning Points in Chinese Health Care," 4.

79. Huang, "Sick Man of Asia."

80. Babone, "Middling Kingdom," 83.

81. Huang, "Sick Man of Asia."

82. Babones, "Middling Kingdom," 85.

83. Jack Chow, Shenglan Tang, and Enis Baris, "Cough It Up," *Foreign Affairs* 91, no. 2 (March/April 2012), <http://www.foreignaffairs.com/articles/137273/jack-c-chow-shenglan-tang-and-enis-baris/cough-it-up>.

84. Meyer, *China or Japan*, 56.

85. Jack Yuan, "China's Productivity Imperative," Ernst & Young (China) Advisory Limited (2012), 10.

86. Ibid., 8.

87. Scott D. Johnson, "Productivity, the Workforce, and Technology Education," *Journal of Technology Education* 2, no. 2 (Spring 1991): 32.

88. Ryan Clarke and Lye Liang Fook, *American Public Opinion on China and US Foreign Policy* (Singapore: East Asian Institute, National University of Singapore, 2010), <http://www.eai.nus.edu.sg/>.

89. Meyer, *China or Japan*, 137.

90. Shambaugh, *China Goes Global*, 311.

91. Marc Labonte and Wayne Morrison, *China's Holding of US Securities: Implications for the US Economy* (Washington: CRS, August 2013), 1, <http://www.fas.org/sgp/crs/row/RL34314.pdf>.

92. Ibid., 4.

93. Ibid., 10.

94. Central Intelligence Agency, "China: Economy—Overview," *World Factbook*, last updated 14 February 2013, <https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html>; and "US Becomes China's Largest Export Market in 2012," *Want China Times*, 13 January 2013, <http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20130113000052&cid=1102>.

95. Labonte and Morrison, "China's Holding of US Securities."

96. Nicholas A. Lambert, *Planning Armageddon: British Economic Warfare and the First World War* (Cambridge: Harvard University Press, 2012), 497–504.
97. James Boughton, “Was Suez in 1956 the First Financial Crisis of the Twenty-First Century?” *Finance and Development* 38, no. 3 (September 2001), 75.
98. Robert Ross, “Engagement in US China Policy,” in *Engaging China*, eds. A. I. Johnston and R. S. Ross (London: Routledge, 1999), 185.
99. “China Joins the WTO—At Last,” *BBC News*, 11 December 2001, <http://news.bbc.co.uk/1/hi/business/1702241.stm>.
100. The concept of the United States spending significant resources on these issues is supported by recent US policy documents such as *Sustaining US Global Leadership: Priorities for 21st Century Defense* (Washington: DoD, January 2012); and “Department of Defense Cyberspace Policy Report,” DoD, November 2011. Significant current journal and press articles such as Brendan Cooley, “A Sea of Change or Wave of Backlash? The South China Sea and Changing Power Dynamics in Southeast Asia,” *Global Security Studies* 3, no. 4 (Fall 2012); and Deborah Charles and Paul Eckert, “China Military Hackers Persist Despite Being Outed by US,” Reuters, 6 November 2013, <http://www.reuters.com/article/2013/11/06/net-us-usa-china-hacking-idUSBRE9A51AN20131106>, demonstrate that despite these policies and the US military’s “rebalance toward the Asia-Pacific region” per the 2012 defense guidance, Chinese activities and tensions in the South China Sea and cyber intrusions continue.
101. Mallaby and Wethington, “Future of the Yuan,” 140.
102. Kennedy, *Rise and Fall*, 665–66.
103. *Sustaining US Global Leadership*, 2.
104. See Dong Nguyen, *Settlement of Disputes Under the 1982 United Nations Convention on the Law of the Sea: The Case of the South China Sea Dispute* (New York: UN-Nippon Foundation, December 2006), 25–27; *Stirring Up the South China Sea (I)*, Asia report no. 223 (Brussels: International Crisis Group, April 2012): 7, <http://www.crisisgroup.org/-/media/Files/asia/north-east-asia/223-stirring-up-the-south-china-sea-i.pdf>; and “United Nations Convention on the Law of the Sea of 10 December 1982,” http://www.un.org/depts/los/convention_agreements/texts/unclos/UNCLOS-TOC.htm.

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.

Act and Actor Attribution in Cyberspace

A Proposed Analytic Framework

Eric F. Mejia, Colonel, USAF

TSgt Joe Pesek rolled out of bed shortly after 0600 to get breakfast at the NCO club. He was assigned to the 5th Bomber Group and had arranged to meet his friends for golf after breakfast. The course in Honolulu was beautiful, and there was no better way to spend a lazy Sunday morning. Waiting for the bus, he admired the beautiful blue sky flecked with distant aircraft. Seeing this many aircraft meant a carrier must be coming into port. Joe wasn't alarmed until the first plane pulled up low over Hickam Airfield with machine guns chattering. The clearly visible rising sun of Imperial Japan on the wings told the story—Japan had attacked Pearl Harbor.¹ The following day, 8 December 1941, the United States and Japan declared war against each other.

Seventy years later, Air Force major Shelly Johnson rolled out of bed looking forward to another day of leave in Honolulu. Taking out her smartphone, she tried to scan a check into her account so she would have extra spending money. Despite several attempts, the check failed to deposit. Frustrated, she used her tablet to access the bank's website; however, the homepage refused to load. She finished breakfast and tried again without luck. Irritated, she gave up and got into her car to enjoy her day of leave. A few days later she read the headline: "Major Banks Hit with Biggest Cyberattacks in History."² The article explained how several of the largest banks, including her own, had been the victim of a cyber attack. The Islamist group Izz ad-Din al-Qassam Cyber Fighters claimed responsibility for the attacks; however, researchers were divided about whether they were responsible. Senator Joe Lieberman claimed the attacks were actually conducted by Iran in response to US economic sanctions. The article provided more questions than answers. Major

Col Eric F. Mejia, USAF (JAG) is currently assigned as staff judge advocate at Eglin AFB. He holds a JD degree from the University of Arkansas at Little Rock Law School, is a 2004 distinguished graduate of the Air Command and Staff College, and graduated from the Air War College in 2013, receiving his Master of Strategic Studies degree with highest academic distinction.

Johnson wondered who actually conducted the attack. Could it even be considered an attack, and if so, what was attacked: the customers, the individual banks, the US economy? Who would respond, and how?

These two scenarios highlight the critical importance of attribution. In the case of Pearl Harbor, there was a hostile armed attack directly attributable to a known state actor. These facts established the proper response—war—and the proper responder: the military. In the second scenario, the act and actor were uncertain; consequently, the proper response and responder were equally uncertain. *Actor attribution* is concerned with determining who is responsible for a hostile cyber act. *Act attribution* is concerned with the relative severity of the act. Both are necessary to determine the appropriate response to an act of cyber hostility, and both help frame which organization should be the primary responder. An analytic framework incorporating both act and actor attribution helps delineate responsibility for hostile cyber acts and determine the appropriate response. This article examines the definition and importance of cyber attribution and proposes such an analytic framework for considering act and actor attribution. It concludes with recommendations to address the problems associated with such attribution.

Defining Attribution

The Basic Legal Framework

It is clear, at least from the US perspective, that cyberspace is not a “law-free” zone and that established principles of international law apply.³ The legal framework for use of force by states is contained in the *Charter of the United Nations*, which generally prohibits states from using force against another state. As specified in Article 2(4), “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”⁴ The charter recognizes two exceptions. First, Article 42 permits use of force if authorized by the UN Security Council. Second, and more important for our analysis, Article 51 permits use of force in self-defense against an armed attack, stating that “nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations.”⁵ These

articles did not originally apply to the conduct of nonstate actors. However, international law has developed so that states may use force in self-defense against another state for acts of nonstate actors attributed to it.⁶ A state may also use defensive force directly against nonstate actors if the host state is unable or unwilling to prevent armed attacks from emanating within its territory.⁷

Finally, the use of force is bounded by the law of armed conflict (LOAC), including the concepts of distinction, necessity, and proportionality. Applying the LOAC to hostile cyber acts may cause unnecessary concern among lawyers and unnecessary hesitancy among commanders. This is because responding to a hostile cyber act will likely involve targeting dual-use objects and because of the perceived increased risk of “knock-on,” or unexpected collateral damage.

Dual-use objects may serve both a military and civilian function. The typical example is a bridge, which is equally useful for conveying both military and civilian vehicles. Similarly, most hostile cyber acts will transit civilian cyber infrastructure, including computing systems, data storage systems, and telecommunication lines. Further, malicious cyber code may be prepositioned on civilian cyber infrastructure. Despite the fact that these are clearly dual-use objects, the LOAC often permits them to be targeted. Addressing the issue involves applying Article 52(2) of the Protocol additional to the Geneva Conventions (GPI) to the facts.⁸ Although the United States has not ratified the GPI, it recognizes Article 52(2) as binding customary international law. Article 52(2) sets out a two-part test for analyzing whether an object is an appropriate military target. The first issue is one of *distinction*—is the object a legitimate military objective? Article 52(2) limits attacks to objects who’s “nature, location, purpose or use make an effective contribution to military action.” In the case of hostile cyber acts, cyber infrastructure may be a legitimate military objective if it is used to conduct a hostile cyber act or if malicious code is prepositioned on it in anticipation of a future hostile use. In either case, the use of the object may make it a legitimate military objective and therefore appropriately targetable. The second issue is one of *necessity*. Does the total or partial destruction or neutralization of the object, in the circumstances ruling at the time, offer a definite military advantage? In the case of an ongoing hostile cyber act or prepositioned malicious code, this is a fairly low hurdle to overcome, especially after

making the initial determination that the object is a legitimate military objective.

The potential for unexpected collateral damage is another issue that appears difficult at first blush. Although the facts may be more complicated, traditional application of LOAC is all that is required. Here, the issue is one of proportionality—an attack is generally prohibited if the damage to noncombatants is excessive in relation to the military advantage gained from the attack. The problem with attacking dual-use cyber infrastructure is that it is difficult, if not impossible, to fully anticipate the extent of the likely collateral damage. Luckily, that is not required. In attempting to predict collateral damage, the commander is “only required to do what is feasible, given the prevailing circumstances, including the time he has to make a decision and the amount of information he has at that time.”⁹ If anything, the difficulty of precisely determining what collateral damage may be expected benefits commanders by affording them significant latitude in the decision-making process.

The basic legal framework may be summarized as follows:

- States may generally not use force against other states.
- States may use force against other states if
 - a. force is authorized by the UN Security Council, or
 - b. force is used in self-defense against an armed attack by (1) another state or (2) a nonstate actor if the act can be imputed to a state.
- Force may be used in self-defense directly against nonstate actors if the host state is unable to prevent armed attacks by nonstate actors.
- Use of force is limited by LOAC principles.

Ultimately, determining an appropriate response to a hostile cyber act requires analyzing who the actor is (state, nonstate, unknown) and what the act is (armed attack or not an armed attack). In other words, actor and act attribution.

Actor Attribution

Actor attribution is simply determining who should be held responsible for a hostile cyber act. As noted in the *2011 Department of Defense Strategy for Operating in Cyberspace*, low barriers to entry for hostile cyber acts, coupled with widespread availability of hacking tools, means

that small groups, and even individuals, can impact national security.¹⁰ However, a significant issue from a response perspective is not the identity of the actors but whether the hostile cyber acts are attributable to a specific state. This distinction helps determine the appropriate response, responder, and rules for engagement.

Hostile cyber acts can be attributed to a state either directly or indirectly.¹¹ The two methods of state attribution are briefly described as follows:

Direct Attribution. States are responsible for the acts or omissions of individuals exercising the state's machinery of power and authority since these actions are attributed to the state even if the acts exceed the authority granted by the state.

Indirect Attribution. Acts or omissions of nonstate actors are generally not attributable to the state; however, the state may incur responsibility if it fails to exercise due diligence in preventing or reacting to such acts or omissions.¹²

Although not universally accepted in international law, it is generally accepted in practice that a state's right to use force in self-defense is also triggered by armed attacks which cannot be attributed to a state. For example, an armed attack may emanate from a state without that state's knowledge or ability to prevent it. In such circumstances, the armed attack is attributed directly to the attackers, and the victim state may defend with force directly against the nonstate actors despite their being located in a neutral or even allied state. As recently noted in the *Journal of Conflict and Security Law*, it is the nature of the hostile act that triggers the right to self-defense, not the nature of the actor.¹³ This simply comports with common sense. A state should not be required to endure an armed attack by nonstate actors when it has the means to defend itself consistent with fundamental LOAC principles. US attacks against terrorists operating within Pakistan are one concrete application of this concept. Once a state has been subjected to an armed attack, it may forcibly defend itself. The decision of whether to do so is a matter of policy, and ultimately the response must satisfy basic LOAC principles including necessity, proportionality, and distinction.

Act Attribution

Act attribution is the process of defining the severity of the hostile cyber act.¹⁴ Hostile cyber acts may range from something as benign as attempting to ping a network computer to an attack on the US power grid leaving millions without power for months.¹⁵ Similarly, there is a broad range of potential defensive actions that may be taken by the victim state. A simple continuum of potential responses is presented in figure 1.

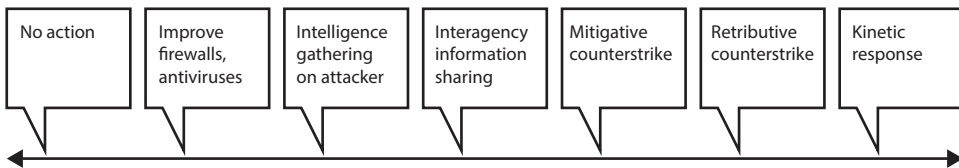


Figure 1. Continuum of potential cyber-attack responses

Supplementing these potential actions is a state's full range of diplomatic and political responses to cyber hostility. However, any response by a victim state must be determined in part by the severity of the hostile act.

A state may passively defend against all hostile actions; however, it may only forcibly retaliate in self-defense against armed attacks. By extension, imminent armed attacks allow states to respond in anticipatory self-defense.¹⁶ International law currently is silent on whether a cyber attack can be considered an armed attack. However, the United States has taken an affirmative position on the issue. The May 2011 *International Strategy for Cyberspace* states, "Right of Self-Defense: Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace."¹⁷ This echoes the language of Article 51 of the UN charter which says that states have the inherent right to engage in individual or collective self-defense in response to an armed attack.¹⁸ So, clearly the United States has adopted the position that a hostile cyber act may be treated as an armed attack. But given the range of hostile cyber actions, how do we determine whether such an act rises to the level of an armed attack? If the *effects* of a cyber attack are the equivalent of a traditional armed attack, then states should be permitted to respond accordingly. The leading proponent of this effects-based approach is Michael N. Schmitt. His effects-based analysis evaluates hostile cyber acts based on six criteria:

1. Severity: Armed attacks threaten physical injury or destruction of property to a greater degree than other forms of coercion.
2. Immediacy: Armed attacks usually occur with greater immediacy.
3. Directness: Armed attacks have a more direct link to the negative consequences caused.
4. Invasiveness: Armed attacks usually cross into the target state to cause harm.
5. Measurability: The consequences of an armed attack are easier to measure.
6. Presumptive Legitimacy: Because of the general prohibition on the use of armed force between states in international law, an armed attack is presumed illegitimate.¹⁹

This framework can readily be applied to cyber attacks to determine whether a given hostile act may be considered an armed attack.²⁰ If so, a forcible response may be appropriate. If not, some lesser form of response may be required.

The Importance of Attribution

An assessment of both act and actor attribution is central in determining the appropriate response to a hostile cyber act. A government may respond in a variety of ways including monitoring, improving passive defenses, applying political pressure, employing active defenses, and counterstriking with both cyber and conventional weapons. *Passive defense* is defined as “measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative.”²¹ Passive defense in the cyber realm includes making systems more difficult to attack through antiviruses and firewalls, educating users to be more security conscious, and reducing postattack recovery times through redundancy and backup systems.²² By contrast, *active defense* is “the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy.”²³ In the cyber realm this translates to initiating a cyber counterattack as a defensive response to a hostile cyber attack.²⁴ Defensive cyber attacks can be broken down into two types. If the goal is to mitigate harm to a targeted system using only the amount of force necessary to protect the

system from further damage, it is considered a mitigative counterstrike. The purpose of a mitigative counterstrike must be to mitigate damage from an immediate threat. If the goal of the counterstrike is to punish the attacker, it is considered a retributive counterstrike.²⁵ Under international law, only the mitigative counterstrike is truly defensive, because its purpose is to defend against an immediate threat.

Actor and act attribution is also critical in determining which government entity should take the lead in responding to a hostile cyber act. Several government agencies are tasked with cyber operations and responsibilities. As summarized by Gen Keith B. Alexander, commander for US Cyber Command (CYBERCOM), these agencies include:

- Department of Defense/Intelligence Community/NSA/CYBERCOM: Responsible for detection, prevention, and defense in foreign space, foreign cyber threat intelligence and attribution, security of national security and military systems, and, in extremis, defense of the homeland if the nation comes under cyber attack from a full scope actor.
- Department of Homeland Security (DHS): Lead for coordinating the overall national effort to enhance the cyber security of US critical infrastructure and ensuring protection of the civilian federal government (.gov) networks and systems.
- Federal Bureau of Investigation (FBI): Responsible for detection, investigation, prevention, and response within the domestic arena under their authorities for law enforcement, domestic intelligence, counterintelligence, and counterterrorism. Importantly, when malicious cyber activity is detected in domestic space, the FBI takes the lead to prevent, investigate, and mitigate it.²⁶

The Difficulty of Conclusive Attribution

Both act and actor attribution are difficult to prove with scientific certainty. Computer networks are not designed to facilitate attribution, and hostile actors exploit this weakness to hide their true identity. For example, the Internet typically does not use sender identification during the transmission process, so source information can easily be forged. Masking the sender information in this manner is commonly referred to as “spoofing.” Hostile cyber actors can also hide their identity and

location by employing a system that transforms data in some manner, known as a “laundering host.” Cyber actors may employ an attack that is complete in milliseconds, or alternatively, is spread out over months. All of these factors make cyber actor attribution difficult.²⁷ The degree of difficulty is subject to some debate. Former secretary of defense Leon Panetta stated in late 2012 that the Department of Defense had made “significant investments in forensics to address this problem of attribution” and that “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.”²⁸ However, such a public declaration raises several issues. First, is the statement an accurate assessment of capabilities or is it more akin to posturing in an attempt to deter potential adversaries? Second, if the statement is technologically accurate, acknowledging this capability and subsequently using it to attribute a hostile act to a specific actor runs the risk of compromising the methods and techniques used in the process. Finally—given the highly adaptive nature of cyber warfare—cyber defenses, including forensics, will inevitably be thwarted by constantly evolving cyber threats. Even if the technical issue of attribution is overcome, what degree of confidence must be achieved to support a finding that a state is responsible under international law? Certain? Very certain? These are subjective political determinations that simply do not lend themselves to precise quantitative analysis.

This same issue exists when trying to assess act attribution. Using the Schmitt model to determine if a hostile cyber act is tantamount to an armed attack requires applying a subjective analysis. How severe is *severe*? What is the definition of *immediate*? What constitutes a *direct link* between a hostile cyber act and the consequences of the act? All of these questions require a subjective, nonscientific assessment.

Fortunately, the legal community has been dealing with the problem of subjective actor and act attribution and has extensively developed the concepts and lexicon related to subjective attribution. This is most evident in the law related to civil and criminal trials. Legal experts refer to these subjective criteria as “standards of proof.” A few of the more common ones, in order of the degree of certainty, are:

- Scintilla of evidence—the least amount of evidence possible.

- Preponderance of the evidence—In a civil trial the issue to be decided is often whether or not one party is negligent, and therefore financially responsible for the losses incurred by the other party. The subjective standard used by courts to assess this question of liability is called the preponderance of the evidence standard. This is simply defined as more probable than not.
- Clear and convincing evidence—creating a firm belief or conviction. It is an intermediate level of proof, being more than a preponderance of the evidence but less than what is required for proof beyond a reasonable doubt.
- Beyond a reasonable doubt—This is the standard used to establish criminal guilt, which is the equivalent of actor attribution, as well as to determine the specific criminal offense committed, which is the equivalent of act attribution. It means entirely convinced and satisfied to a moral certainty. However, it is less than a scientific certainty.²⁹

Employing legal subjective criteria is not a new or novel idea. In a 2009 Microsoft white paper, the author suggested a similar subjective assessment for cyber attribution, noting that

it [is] important to focus on probability of accurate attribution, as opposed to certainty of attribution. In many areas, of course, absolute certainty is seldom achievable. For this reason, a range of different standards have developed (for example, proof beyond a reasonable doubt, a preponderance of the evidence) and individuals and organizations often have to rely upon probabilities when making critical decisions (such as when opting for one medical treatment over another). Of course, the greater the certainty, the easier it may be to choose a course of action, but that does not mean certainty is required before reasonable action can be taken.³⁰

While it would be naïve to assume that one could import the whole of court-based attribution concepts to assess cyber attribution, several key points are evident. First, scientific proof is not necessary for attribution. While scientific certainty is the “gold standard” of proof, it is rarely obtainable, and historically has not been necessary to establish attribution. Second, as previously noted, attribution is routinely based on subjective determinations. Third, when using a subjective assessment of attribution, severity of the consequences is linked to the degree of confidence. A court may assess financial responsibility based on a preponderance of the evidence, but it takes a much higher degree of confidence to establish

criminal guilt. Finally, although many technical experts may be hesitant or uncomfortable using a subjective assessment, the government, through its legal community, has at its disposal established expertise in subjective attribution.

An Analytic Model for Actor and Act Attribution

Based on the foregoing, the factors included in any proposed analytic model should be based on a subjective assessment of act and actor attribution. An assessment of these factors should indicate who should respond to an act of cyber hostility and what the upper range of appropriate responses should be. Ideally, the responses would incorporate basic LOAC principles. Combining these basic concepts yields the analytic model proposed in figure 2.

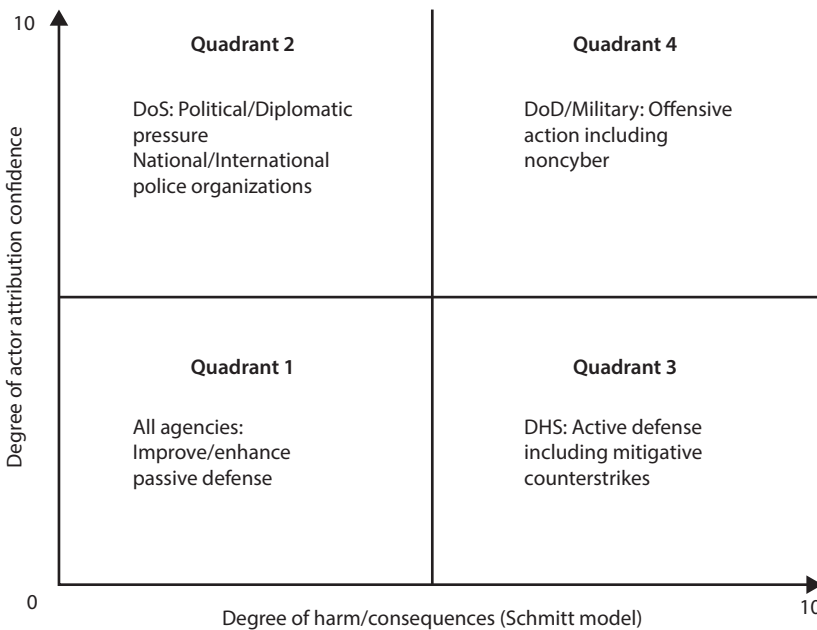


Figure 2. Analytic model for actor and act attribution

Several issues are worth noting. First, act and actor attribution are dynamic. Just as in conventional warfare, the preparation for a hostile cyber act may occur in one location, yet the act itself may originate in a different location or, even more likely, be distributed throughout a variety of locations. Further, although an act may appear harmless at first,

subsequent information or events may show it to be significantly more harmful than initially believed. Therefore, the appropriate response and responder are likely to be dynamic as well, involving several organizations and a potentially escalating series of responses. Second, the responsive actions in each quadrant represent the upper limits of an appropriate response. For example, the Department of State (DoS) may elect not to apply diplomatic pressure to a state actor for a variety of reasons, even if justified by hostile cyber acts. Further, the various instruments of power described are not equally effective on all hostile actors. For example, it is unlikely that a rouge individual would be greatly deterred by political/diplomatic pressure. Although a military strike against an individual would likely be effective, it is politically untenable. As always, effective application of the instruments of power is an art, and a mechanistic approach will likely fail. Finally, the quadrants do not reflect sole responsibility for responding to hostile cyber acts. However, the framework does help assign primary or lead responsibility, with other agencies in a supporting role.

Quadrant 1: Low Actor Attribution Confidence/Low Degree of Harm

In this common scenario, government agencies are faced with numerous relatively innocuous yet unauthorized cyber acts. For example, in 3 June 2010, General Alexander stated that DoD systems are probed by unauthorized cyber actors approximately 250,000 times per hour, or the equivalent of more than 6 million times each day.³¹ Most cause no damage and do not result in a compromise of data. According to the US Computer Emergency Readiness Team (US-CERT), in 2009, approximately 73.4 percent of all reported cyber incidents were categorized as “Category 5: Scans, Probes, or Attempted Access.” This includes “any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.”³² For these types of acts, passive defense is an appropriate response. The vast majority of Quadrant 1 actions are easily defeated by encryption, firewalls, antivirus and anti-malware programs, or other purely passive measures.

Quadrant 2: High Actor Attribution Confidence/Low Degree of Harm

In this scenario, the government is again faced with acts that cause little harm. However, the acts are still unauthorized and may be the harbinger of more serious, and more harmful, future acts. Unlike the scenario in Quadrant 1, these acts can confidently be attributed to an identified actor. Under these circumstances, passive defensive measures alone may be insufficient. However, because the acts are insufficiently harmful to be considered equivalent to an armed attack, offensive strikes and defensive counterstrikes are not necessary or proportional to the harm being caused. In addition to passive defense, employing appropriate diplomatic pressure may be appropriate for state actors. This approach is consistent with the May 2011 *International Strategy for Cyberspace*. This document states that the United States will combine diplomacy, defense, and development to achieve the national goal of cyber security. Diplomatic efforts will be focused on engaging “the international community in frank and urgent dialogue, to build consensus around principles of responsible behavior in cyberspace and the actions necessary, both domestically and as an international community, to build a system of cyberspace stability.”³³ Diplomatic efforts to stem the tide of less serious cyber acts are not new. For several years the United States has been engaged in such efforts to dissuade China from continuing cyber espionage against both the US government and US corporations. Former defense secretary Leon Panetta spent three days in China addressing the issue of its cyber activity. This is an appropriate response to state-attributed cyber acts which fall short of an armed attack. As noted by James Lewis, cyber security expert with the Center for Strategic and International Studies, “The damage from Chinese cyber espionage is easy to overstate but that doesn’t mean we should accept it.”³⁴ To facilitate diplomatic efforts at cyber security, the DoS recently created a new office. The Office of the Coordinator for Cyber Issues is tasked with coordinating DoS global diplomatic engagement on cyber issues, serving as the DoS liaison to the White House and federal departments and agencies on cyber issues, and advising the secretary and deputy secretaries on cyber issues and engagements.³⁵ If the hostile actor is a non-state-affiliated individual or group, the Federal Bureau of Investigation, Department of Justice, or analogous international organizations will be primarily responsible for any investigation and prosecution, if appropriate.

Quadrant 3: Low Actor Attribution Confidence/High Degree of Harm

In this scenario, the government is faced with a hostile cyber act capable of causing significant harm. The harm threatened, or caused, may be sufficient to be considered the equivalent of an armed attack. Within the cyber realm, this may involve harming the nation's key resources or critical infrastructure. However, there is insufficient evidence to confidently attribute the act to a specific state or nonstate actor. One potential example of this would be unidentified actors using a state's IT infrastructure to conduct an attack without the consent, or even knowledge, of that state. Retributive strikes require attribution, which is lacking in this scenario. However, the LOAC still permits action in self-defense. When a state is unable to prevent attacks emanating from inside its borders or the attackers operate independently of the state, the victim state may still use force in self-defense, provided it meets the requirements of necessity, proportionality, and distinction.³⁶ Under these circumstances, active defenses, including mitigative counterstrikes, may be appropriate. The goal of mitigative counterstriking is to "mitigate damage from a current and immediate threat."³⁷ These active but purely defensive measures can trace an attack back to its source and immediately interrupt the attack. Further, mitigative counterstrikes are relatively precise. This precision limits the risk of excessive collateral damage. Limiting collateral damage helps satisfy the requirement of proportionality and helps reduce the risk of escalating cyber attacks into full-scale kinetic attacks between states.³⁸ Finally, because of their precision, reduced risk of collateral damage, and purely defensive nature, automated mitigative counterstrikes are less likely to violate international LOAC norms.

Mitigation of cyber attacks is squarely within the purview of the DHS. *Homeland Security Presidential Directive 7* establishes the national policy for identifying and protecting critical US infrastructure and defines the roles of the various federal and state departments. The secretary of homeland security is responsible for "coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States [and serves as] the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources."³⁹ To fulfill this responsibility, DHS created the National Cyber Security Division,

which is responsible for analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems.⁴⁰ One of its specified missions is safeguarding and securing cyberspace, and one of its key strategic outcomes in performing this mission is that “cyber disruptions or attacks are detected in real-time [*sic*], consequences are mitigated, and services are restored rapidly.”⁴¹

Quadrant 4: High Actor Attribution Confidence/High Degree of Harm

In this scenario, the government is faced with a hostile cyber act tantamount to an armed attack. Further, there is a high degree of actor attribution confidence. Conceptually, this is the equivalent of a kinetic attack against the United States, therefore a DoD response is appropriate. Further, there is no prohibition against responding with kinetic force against a cyber attack provided the response meets traditional LOAC requirements. This, too, is consistent with the 2011 *International Strategy for Cyberspace*, which states: “We fully recognize that cyberspace activities can have effects extending beyond networks; such events may require responses in self-defense. . . . When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country.”⁴²

There is little disagreement that the DoD should be the lead agency in this scenario. As noted by the US CYBERCOM commander, in extreme situations, it is the role of the DoD to defend “the homeland if the Nation comes under cyber attack from a full scope actor.”⁴³ However, some argue that the DoD should take a more expansive role in cybersecurity, essentially performing the DHS’s assigned role. Much of this argument is based on the perceived effectiveness of the DoD, or rather the perceived ineffectiveness of the DHS. However, an expanded role for the DoD in cybersecurity is the wrong approach. First, it unnecessarily expands the role of the military. The military would undoubtedly perform well at securing transportation hubs, power plants, water treatment facilities, critical manufacturing sites, and other critical national infrastructure. However, that is not the mission of the military; the mission of the military is to wage war. Further, effective cyber defense requires a degree of domestic intrusion which should not be conducted by the DoD. As noted by retired major general Charles Dunlap, “The armed

forces are the most authoritarian, least democratic, and most powerful institution in American society. The restraint intrinsic to a domestic law enforcement mind-set is not its natural state. . . . If nothing else, the fact that the armed forces unapologetically restrict the rights and privileges of their own members should militate toward avoiding their use in civilian settings where the public properly expects those rights and privileges to flourish.”⁴⁴

Conclusion and Recommendations

The cyber community must recognize the critical importance of attribution. It is the basis for effective diplomacy, law enforcement, and a prerequisite for offensive military counterstrikes under the law of armed conflict. The first fundamental question that must be answered after a hostile act is: who committed the act? The second is: how much damage was done? An accurate assessment of actor and act attribution helps define both the proper response to an act of cyber aggression and helps determine the appropriate lead agency to respond to such an act.

Because actor and act attribution fundamentally drive cyber defense, efforts to enhance technical attribution should be given priority. Although assessing attribution is subjective, often the evidence used in such an assessment is technical. Attributing a hostile cyber act is a prerequisite to effective deterrence. No hostile actor, whether nation-state or rogue individual, will ever be deterred from hostile cyber activity if they can effectively deny responsibility. Further, the international community is unlikely to support military action unless a hostile act equivalent to an armed attack can successfully be attributed to an offending party. Because hostile actors will continue to develop new methods to mask their activity, effective deterrence demands that the United States continue to enhance its technical attribution capability.

Legal expertise is critical in assessing attribution and framing an appropriate response. Although the cyber domain is relatively new, the art of actor and act attribution is ancient. Every criminal prosecution that has ever occurred fundamentally required a subjective determination of guilt (actor attribution) and offense (act attribution). Legal practitioners, although often ignorant of the technical aspects of the cyber domain, are well versed in the art of attribution. Cyber experts may be technically adept but are often ignorant of the nuances of subjective

attribution. Close integration of both legal experts and technical cyber experts is critical to establishing an appropriate cyber policy and appropriate responses to specific hostile cyber acts.

An analytic framework is an essential tool for cyber practitioners. In a field where significant ambiguity may exist, both as to the nature of the act and the identity of the actor, an analytic construct promotes diagnostic consistency. Additionally, it helps define roles and missions for various responders and provides a common framework and understanding of responsibility. The analytic framework also enhances deterrence by providing notice to hostile cyber actors that the consequences they should expect from committing a hostile cyber act are determined, in part, by the severity of the hostile act and that a severe hostile act will merit a military response. **SSQ**

Notes

1. "Hickam Field—Army Air Corp Sergeant," *PearlHarbor.org*, <http://www.pearlharbor.org/eyewitness-accounts.asp>.
2. David Goldman, "Major Banks Hit with Biggest Cyber Attacks in History," *CNN.com*, 28 September 2012, <http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html>.
3. Harold Hongju Koh, Department of State legal advisor, "International Law in Cyberspace," remarks to the USCYBERCOM Interagency Legal Conference, Ft. Meade, MD, 18 September 2012, <http://www.state.gov/s/l/releases/remarks/197924.htm>.
4. *Charter of the United Nations*, 24 October 1945, chap. I, art. 2(4).
5. *Ibid.*, chap. VII, art. 51.
6. Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2012), 53.
7. Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict and Security Law* 17, no. 2 (Summer 2012): 7, <http://jcs.oxfordjournals.org/content/17/2/229.full.pdf+html>.
8. "Protocol additional to the Geneva Conventions of 12 August 1949 and relating to the protection of victims of international armed conflicts (Protocol I)," adopted at Geneva on 8 June 1977, <http://treaties.un.org/doc/Publication/UNTS/Volume%201125/volume-1125-I-17512-English.pdf>.
9. Eric Talbot Jensen, "Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?" *American University International Law Review* 18, no. 5 (2003): 1186.
10. *2011 Department of Defense Strategy for Operating in Cyberspace* (Washington: DoD, July 2011), 3.
11. Many commentators use the terms *attribution* or *direct responsibility*, and *imputed* or *indirect responsibility*. However, since *imputed responsibility* is functionally the equivalent of attributing the hostile act to the state, the term *indirect attribution* is used to clarify the discussion.
12. Jan Arno Hessbruegge, "The Historical Development of the Doctrines of Attribution and Due Diligence in International Law," *New York University Journal of International Law and Politics* 36 (Winter/Spring 2004): 268.

13. Tsagourias, "Cyber Attacks," 7.
14. Susan W. Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism /Warfare," *Journal of Criminal Law & Criminology* 97, no. 2 (2007): 379, using the terms *attack* and *attacker* attribution, or *who* and *what* attribution.
15. A *ping* is a test to see if a system on the Internet is working. *Pinging* a server tests and records the response time of the server. <http://www.techterms.com/definition/ping>.
16. Carr, *Inside Cyber Warfare*, 58.
17. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington: White House, May 2011), 10.
18. *Charter of the United Nations*, art. 51.
19. Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1999): 914–15.
20. For an excellent example of an application of the Schmitt analysis see Andrew C. Fultz, "Stuxnet, Schmitt Analysis, and the Cyber 'Use of Force' Debate," *Joint Force Quarterly* 67 (4th Quarter 2012): 40–48.
21. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 August 2012), 237.
22. William A. Owens et al., eds., *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington: National Academies Press, 2009), 13, http://www.nap.edu/catalog.php?record_id=12651.
23. JP 1-02, *Department of Defense Dictionary*, 2.
24. Owens et al., *Technology, Policy, Law and Ethics*, 134.
25. Jay P. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," *Harvard Journal of Law and Technology* 25, no. 2 (Spring 2012): 420–21.
26. Gen Keith B. Alexander, "Statement before the Senate Committee on Armed Services, 27 March 2012," 12–13, <http://www.armed-services.senate.gov/statemnt/2012/03%20March/Alexander%2003-27-12.pdf>.
27. Dr. David A. Wheeler, "Planning for the Future of Cyber Attack Attribution," statement before the US House of Representatives Committee on Science and Technology Subcommittee on Technology and Innovation, 15 July 2010, 3, http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/071510_Wheeler.pdf.
28. Secretary of Defense Leon E. Panetta, remarks to the Business Executives for National Security, New York City, 11 October 2012, <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>.
29. *Black's Law Dictionary*, 5th ed. (St. Paul, MN: West Group, 1979), 147.
30. Scott Charney, "Rethinking the Cyber Threat: A Framework and Path Forward," Microsoft white paper (Redmond, WA: Microsoft Corp., 2009), 9.
31. Gen Keith Alexander, "U.S. Cybersecurity Policy and the Role of U.S. Cybercom," address to the Center for Strategic and International Studies, Washington, DC, 3 June 2010.
32. *US CERT Quarterly Trends and Analysis Report* 4, no. 2 (16 June 2009): 2.
33. *International Strategy for Cyberspace*, 11.
34. "China Stonewalls Panetta on Cyber Attacks," *CBS News*, 20 September 2012, http://www.cbsnews.com/8301-202_162-57516541/china-stonewalls-panetta-on-cyberattacks/.
35. "Office of the Coordinator for Cyber Issues," <http://www.state.gov/s/cyberissues/index.htm#>.
36. Tsagourias, "Cyber Attacks," 7.
37. Kesan and Hayes, "Mitigative Counterstriking," 421.
38. Carr, *Inside Cyber Warfare*, 72.

39. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection*, 17 December 2003, para. 12, <http://www.dhs.gov/homeland-security-presidential-directive-7#1>.
40. *Ibid.*, para. 16.
41. *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington: DHS, February 2010), 54.
42. *International Strategy for Cyberspace*, 13–14.
43. Alexander, “Statement before the Senate Committee on Armed Services,” 13.
44. Charles J. Dunlap Jr., “Perspectives for Cyber Strategists on Law for Cyberwar,” *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 93–94.

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.

Book Essay

Airpower Writings of John Andreas Olsen

Dr. John Olsen is a Royal Norwegian Air Force colonel who has served as an educator, teaching at the Norwegian and Swedish National Defence Colleges; an operator, as deputy commander of the NATO advisory team in Sarajevo; and a strategist—as military advisor to the Norwegian Embassy in Berlin and currently the Norwegian Ministry of Defence. He earned a PhD from De Montfort University in Leicester, England, and more importantly, is a student of airpower who thinks deeply and writes eloquently on its role in modern war. This essay looks at five of his most important books.

The first Gulf War, Desert Storm, was one of the most tactically decisive victories in modern history. It is easy to forget that in 1990 Saddam Hussein's Iraq was considered a very formidable opponent. It had the world's fourth-largest army, battle hardened after an eight-year war with Iran. That army, and the Iraqi air force as well, were provided modern equipment by the Soviets, French, and others. It enjoyed interior lines of communication and supply. The "trackless desert" was seen as a natural defense barrier, making it difficult for coalition forces to locate precise targets and causing difficulties for Western equipment based there. The Iraqis had weapons of mass destruction (WMD)—which they had already used against Iran—and a reliable delivery system (Scud missiles). These weapons, as well as many other facilities, were protected by concrete bunkers several feet thick or buried underground. The US-led coalition was broad and sizable, but many saw this as a limitation—how could these various national forces meld their disparate equipment, doctrine, and command and control procedures to form a coherent and effective striking force?

Yet, the campaign to liberate Kuwait was remarkably rapid, overwhelming, and relatively bloodless. We all must remember this war, because it revealed strengths and weaknesses of modern military power that overturned long-held beliefs and pointed to a new future.

Strategic Air Power in Desert Storm (London: Frank Cass, 2003), was Olsen's first book and examined the Gulf War in depth. Although not addressing all aspects of the air war against Saddam Hussein, it covers one aspect too little known or understood.

GEN Norman Schwarzkopf was the US commander in the Middle East when Hussein's forces invaded Kuwait in August 1990. Pres. George H. W. Bush announced that such aggression would not be allowed to stand, and Schwarzkopf began planning for Kuwait's liberation. He was, however, unimpressed by his staff's efforts, so he turned in an unexpected direction for help. Schwarzkopf called the Air Force chief of staff and asked for an air plan that would serve coalition interests better than a bloody, frontal ground assault. This was a controversial move by Schwarzkopf: procedure dictated that a combatant commander needing assistance call the Joint Staff.

Instead, the chief turned to his plans directorate, where an obscure colonel by the name of John Warden was tasked to draw up a strategic air plan. Warden gathered together a group of subordinates and other Air Staff personnel to produce a plan promising great results at low cost. The plan was dubbed "Instant Thunder" in a direct rejection of the infamous Vietnam-era air campaign of gradual escalation termed "Rolling Thunder."

Instant Thunder called for a massive and near-simultaneous attack on Iraqi centers of gravity—its leadership, communications, transportation, electrical power, and the production and storage facilities of its WMD. The plan was given to Schwarzkopf, who was delighted; he directed Warden to brief his air commander, Lt Gen Chuck Horner. Horner recognized the value of the plan but also some of its flaws. Instant Thunder implied that a concerted attack on Iraqi centers of gravity would be so devastating as to make a ground offensive unnecessary. Schwarzkopf and Horner rejected such optimistic thinking. Instead, they directed an air campaign to isolate Saddam's regime and fatally cripple its fielded forces. Indeed, Schwarzkopf insisted that airpower reduce Iraq's frontline divisions below 50 percent before a ground offensive would even begin.

The Instant Thunder planning cell in Washington did not welcome these changes but fell in line. Olsen notes that only 2 percent of the coalition's air effort was directed at the leadership targets that Warden and his Instant Thunder planners thought so important. Nonetheless, Olsen contends these strikes were disproportionately effective, because Saddam was largely cut off from his military forces and unable to direct them effectively. The result was reminiscent of what military theorist J. F. C. Fuller once termed "brain warfare"—the spinal cord of the enemy army was severed, leaving the appendages still alive but twitching spasmodically and devoid of central direction.

The main value of the Instant Thunder strategic air campaign, according to Olsen, was to reframe the debate on war strategy. Instead of a plan focusing on a bloody ground assault (early projections feared more than

20,000 coalition casualties), the air campaign destroyed the bulk of the Iraqi army before a major ground offensive even began. US Central Command (CENTCOM) intelligence estimated the air campaign had reduced all Iraqi frontline divisions to below 50 percent before G-day in late February, and this assessment was confirmed by the CIA. In other words, the Iraqi army was, by definition, “combat ineffective” before major ground operations even began.

Olsen’s second book was a biography of the air planner who played the major role described above: *John Warden and the Renaissance of American Air Power* (Washington: Potomac Press, 2007). The term *renaissance* in Olsen’s title bears some explanation.

The advent of nuclear weapons had a profound psychological effect on military and civilian populations worldwide, not the least of which were airmen themselves—the keepers and deliverers of the new weapons. Despite the Korean War that saw the United States and Soviet Union refrain from their use, military planners nonetheless planned for a major war in Central Europe against the Soviet Union—a war that presumed the use of nuclear weapons. Consequently, during the early Cold War era, air planners envisioned war largely at the high end of the conflict spectrum. Because war had never occurred between nuclear powers, the plans they drafted had a high theoretical content—as was the case before World War II when major strategic air operations had yet to be extensively conducted. The result in the 1930s—and for the three decades following World War II—was air doctrine based on little historical experience, because such history had not yet occurred. Thinking the unthinkable was dominated by civilian academics adept at the ethereal and theoretical discourse comprising nuclear strategy. On the other hand, the tactical air battle remained crucial. Fighter pilots, although increasingly tasked to deliver nuclear weapons during the 1950s and ’60s, still saw their main function as gaining and then maintaining air superiority. More specifically, they envisioned the air battle as the supreme test of piloting skill.

The result was a peculiar situation where airpower thought gravitated toward the two extremes: nuclear war as imagined by eggheads vs. the tactical air battle craved by the fighter pilots. The area in between—conventional strategic warfare—was largely ignored.

Olsen argues that John Warden, beginning during his days as a cadet, taught himself the principles of grand strategy and strategic airpower. While a graduate student at Texas Tech University (political science) and then the National War College, he continued to focus his studies. His thesis for the latter was published as *The Air Campaign: Planning for Combat* (Washington: National Defense University Press, 1988) and outlined

Warden's ideas on the importance of strategic conventional air operations. The book proved controversial. Although in retrospect his emphasis on air superiority and air interdiction are hardly unusual, he also noted there were times when the ground scheme of maneuver could be used to support the dominant air campaign. To many, this was heretical thinking. It is a measure of how profoundly war has changed over the past two decades that Warden's basic concepts are now accepted as a starting point for joint doctrine.

Warden's career as a fighter pilot in Vietnam and then as an F-15 wing commander in Germany are well covered, but the heart of the book centers on the events of 1990–91 when, from an office in the basement of the Pentagon, Warden devised the Instant Thunder air campaign plan. Olsen notes that the plan was limited. It promised results too extravagant—what if Saddam Hussein did not surrender after his infrastructure was reduced to rubble? Nonetheless, Warden's vision of a strategic air campaign that would avoid the bloody land battle advocated by ground officers was to become the winning option adopted by Schwarzkopf.

Not everyone was pleased with Warden's role in steering the coalition away from a ground-based slugfest. The other services and the Joint Staff were irritated that Schwarzkopf had bypassed normal channels. Within the Air Force itself, some at Tactical Air Command were similarly vexed by being shunted aside.

Desert Storm was of course an incredible success—although, as is often the case, military decisiveness does not always translate into political victory. Yet, instead of being hailed as a hero and promoted to brigadier general, Warden was ignored. Indeed, he never even received a medal for his efforts. Upon leaving the Pentagon, he served in the White House as an advisor to the vice president for a year and then moved to Maxwell AFB to become commandant of Air Command and Staff College (ACSC). Despite occupying that general officer's billet for three years, he was never promoted.

Warden seemed unfazed by the slights. He turned the ACSC curriculum upside down, redirecting the faculty to teach airpower at the broadest level, while also understanding the dynamics and mechanics of actually writing an air campaign. There were dissenters on the faculty and others around the academic circle who resented and feared the forward-thinking radical at ACSC.

What was Warden's lasting impact? Olsen argues it was limited. Like most academic institutions, the old guard professors were able to outwait him. Moreover, and this is important to bear in mind, not all of Warden's ideas were good ones. Yet, 20 years after his tenure at ACSC, concepts such as parallel warfare, effects-based operations, and the need to think strategically are common currency within the Air Force.

Olsen does an excellent and balanced job of portraying an unconventional airman. At times charming and engaged while at other times distracted and preoccupied, Warden inspired both devoted advocates and bitter enemies throughout his career. As Olsen perceptively notes, Warden's greatest strengths—his aggressiveness, bureaucratic fearlessness, creativity, and disregard for rank that made him often bypass recalcitrant superiors—were at the same time his greatest weaknesses that frequently found him in hot water.

A History of Air Warfare is an edited work (Washington: Potomac Books, 2010) and arguably one of Olsen's best. He calls upon 15 authors—he also writes one chapter himself—to trace the history of air warfare from World War I to the present, with a look into the future. Nearly all the essays are excellent. John Morrow notes that the airplane transitioned in a remarkably short time from its initial use as a reconnaissance asset in World War I to conducting most of the combat functions exercised today: air superiority, close air support, air interdiction, strategic bombing, and airlift. Its initial function, reconnaissance, had unintended consequences: aircraft severely limited the chances of achieving strategic surprise along the static western front—planes could watch the flow of supplies and personnel that indicated an imminent offensive.

Ground commanders pretended to scoff at the capabilities of the new weapon but were eager to exploit its vertical strike capabilities to assist their own operations. This insistent focus on the tactical nature of airpower would remain for the next century. It should be no surprise, therefore, that it was Britain's Royal Naval Air Service that first theorized—and then experimented—with strategic airpower. Navies have long seen themselves as strategic weapons with global concerns, and it seemed natural that maritime strategists would first explore the use of strategic bombing to attack an enemy's vital centers and disrupt its economy. Such operations were, however, severely limited in their effectiveness due to the rudimentary nature of air technology.

That would change in World War II. Although interwar theorists would speculate on the decisive nature of strategic bombing and how it would revolutionize war, effective technology—the aircraft, engines, bombs, and electronic/intelligence apparatus—was not yet available. Richard Overy also points out that none of the belligerents entered the war intending to conduct “terror bombing” or to target civilians. Prewar doctrine in Britain, Germany, and the United States specifically proscribed such tactics. Yet, technology was not yet available in 1940 to carry out the precision daylight campaign envisioned before the war. Both Germany and Britain retreated to the relative safety of night operations—something for which

they were neither technically nor doctrinally prepared. These problems were eventually overcome, and the United States and Britain instituted a combined bomber offensive that had a devastating effect on Germany's industry and its military capability. Once again, it was probably not by chance that the two great sea powers turned to another form, albeit more direct, of strategic warfare; whereas Germany, France, and the Soviet Union, traditional land powers, saw the airplane as a tactical weapon designed to assist armies in the pursuit of their battlefield goals. Strategic airpower was not very effective before 1944—and it must be remembered that fully 70 percent of all bombs dropped on German targets occurred after D-day—but then again, Allied ground and sea operations had not been all that successful against Germany up until then either.

Rich Muller notes in an excellent essay that in the Pacific, the tyranny of distance made strategic air operations virtually impossible until late 1944. But then, such an air campaign began in earnest using B-29s based in the Mariana Islands. The war ended with the atomic strikes.

Alan Stephens recounts the role of airpower in the Korean War. This war was unexpected and unplanned. Neither the US Army's occupation forces in Japan nor the US Air Force, whose primary mission in the Pacific was air defense, was trained or equipped to conduct conventional war on the Korean Peninsula. Airpower saved the soldiers from being pushed off the peninsula at Pusan, but political constraints prevented its use against the real sources of North Korean power—China and the Soviet Union. Yet, the battle for air superiority over North Korea was crucial to preventing the defeat of the vastly outnumbered United Nations forces once China intervened in October 1950. UN aircraft had largely destroyed the North Korean air arm, but the massive influx of Soviet-made jet fighters into China—and thence into Korea—threatened to reverse the fortunes of the war. The MiG-15 was an excellent aircraft and superior to anything but the F-86. Although heavily outnumbered, the F-86s would venture daily into "MiG Alley" in northwest Korea to engage the MiGs based across the Yalu River in China. Air superiority was crucial. The Chinese repeatedly attempted to build air bases in North Korea to harry and interdict UN ground forces further south. UN aircraft denied these bases by maintaining air superiority above them.

The Vietnam War cast a pall over the US military for two decades. Despite vastly superior technology and manpower, the United States and its allies were never able to defeat North Vietnam. Wayne Thompson, the most authoritative historian of airpower in Vietnam, writes a masterful chapter on the military, political, and technical problems facing the United States. The interdiction campaign termed Rolling Thunder was so encumbered

with political constraints—down even to tactical details—that it was doomed from the start. There is an old adage that superior tactics cannot overcome strategic folly, and this was proven in the skies over North Vietnam. Moreover, airmen themselves were partly to blame for not better anticipating major and prolonged *conventional* air operations. World War III against the Soviet Union and its satellites was the dominant paradigm—in all the services—and airmen, soldiers, and sailors were unprepared to fight an insurgency on the ground or a highly constrained war of attrition in the air. The debate will never end as to whether a more enlightened political and military strategy could have been effective at keeping South Vietnam free.

The chapter by Shmuel Gordon on the Arab-Israeli wars between 1967 and 1982 is one of the most interesting in the book—perhaps because most Americans are unfamiliar with the details of those wars. During the first part of that period the United States was engaged in Vietnam, and the trauma of that disaster overshadowed military thought in this country. That was regrettable, because the operations of the Israeli Air Force (IAF) had much to inform. Gordon reviews the key strategic issues that have confronted Israel since its birth in 1948: lack of strategic depth, a small population, and lack of natural resources, but an abundance of enemies. Consequently, the basis of national security, as articulated by its first prime minister David Ben-Gurion, was that Israel must maintain air superiority over the region.

Gordon argues that this insistence on maintaining air superiority by focusing on a technically first-rate air force piloted by outstanding personnel has resulted in great success. In the Six-Day War of 1967 the IAF was outnumbered 3:1 in aircraft, but on the morning of 5 June it struck Egyptian, Syrian, and Jordanian airfields by surprise, destroying 402 aircraft at a loss to themselves of 28 planes. Over the next several days, 56 more Arab aircraft were shot down in air-to-air combat at a loss of 18 IAF planes. During the two-year war of attrition that followed, the Egyptians were reinforced by the Soviets, particularly with surface-to-air missile (SAM) batteries. These SAMs pushed back the operating area of the IAF, essentially denying it air superiority over the Suez Canal. Even so, when the forces did meet in air combat, the IAF enjoyed an 18:1 kill ratio.

The Yom Kippur War of 1973 caught Israel by surprise. It was a close-run conflict, and the plight of the Israeli ground forces necessitated a concentration on close air support rather than air superiority. The superiority campaign then made a tactical blunder that resulted in heavy losses: the IAF, with a doctrine that had hardened into dogma, focused on Arab airfields rather than on the more deadly—and more vulnerable—SAM sites

near the front. This decision “delayed gaining air superiority over the Egyptian front for at least two weeks” (p. 145). In other words, the IAF saw its main threat as coming from the air—other fighters—when in reality the danger came from ground-based air defenses. This was a mistake repeated by other air forces.

Itai Brun completes the story of the IAF by examining the Second Lebanon War of 2006. Hezbollah, based in Lebanon and backed by Syria and Iran, kidnapped two Israeli soldiers. Military operations were launched to retrieve the soldiers, punish Hezbollah, and destroy its base in southern Lebanon. Israeli leaders decided to rely heavily on the IAF to limit casualties—on both sides. The IAF’s task was to destroy the long-range and medium-range rockets that threatened Israel. This air campaign was successful—few such rockets were fired against Israel during the conflict. Short-range rockets were another matter. These weapons were too numerous and too small to locate and target. On the other hand, Syria’s air force played virtually no role in the campaign, probably because in the Bekaa Valley operation of 1982 the Syrians had lost 87 aircraft to the IAF’s zero.

After three weeks, the Israeli Defence Force began to employ ground troops to establish a six-kilometer buffer zone along the border. Rockets continued to rain down on Israel, and 84 soldiers were killed. Suffering heavy casualties, the Israeli army withdrew, and Hezbollah—intact and still maintaining a large inventory of rockets—claimed victory.

There are also excellent chapters covering the Falklands War (Lawrence Freedman) and those detailing the overwhelming airpower victories in Desert Storm (John Olsen), Bosnia (Rob Owen), Kosovo (Tony Mason), Operation Enduring Freedom (Ben Lambeth), and Operation Iraqi Freedom (Wick Murray). These operations will be discussed more below. The final chapter is a superior overview by Dick Hallion. The former Air Force historian outlines the history of air warfare from 1911 to the present with some peeks into the future. He traces how airpower was crucial in World War I, decisive during World War II, and dominant over the past two decades. Airpower has evolved continuously and rapidly over the past century, and one of the keys to this revolutionary impact has been precision weaponry. Precision-guided munitions (PGM) have permitted parallel warfare and true effects-based operations (EBO). Destruction is rarely a worthwhile goal in air warfare; rather, the intent is to deny options to the enemy. PGMs allow this, but EBO has been resisted by the ground services that see it as a threat to their own model of Clausewitzian, attrition-based warfare. Hallion sums the issue eloquently: “EBO is more than an air war concept: it is intrinsically ‘common sense,’ essential to the efficient employ-

ment of all forms of combat power and particularly suited to the capabilities of joint and combined force air (and space) power” (p. 386).

Global Air Power (Washington: Potomac Books, 2011) was intended as a companion volume to the previous work. Also edited by Olsen, it contains nine chapters that briefly cover the histories of the world’s major air forces: the US (Dick Hallion), UK (Tony Mason), Russian (Sanu Kainikara), Israeli (Itai Brun), Chinese (Xiaoming Zhang), Indian (Jasjit Singh), and three regional overviews of the Pacific Rim (Alan Stephens), Latin America (Jim Corum), and Europe (Christian Anrig). Due to this historical narrative approach, there is some redundancy with the *Air Warfare* volume, but even so, each chapter is a model of concise style and clarity.

Kainikara argues that because of its long tradition as a continental land power, Soviet airpower was largely tied to the army, so tactical aviation received the bulk of funds and doctrinal focus. The advent of nuclear weapons changed this focus, but aside from a projected holocaust, doctrine and force structure remained fixed on the land battle. This evolved with the Gulf War of 1991 when Russian leaders were astounded by the rapid victory of the coalition and the dominant role of airpower. Strategic conventional operations were indeed possible, and for the first time, Russian airpower “cast off its shackles and was allowed to develop as an independent force” (p. 215).

Singh’s chapter on the Indian Air Force notes its contradictory influences from the UK’s Royal Air Force with its tradition of strategic airpower versus the land-oriented Soviet model. At the same time, India finds itself wedged between nuclear adversaries—China and Pakistan. This, combined with persistent budget concerns, has resulted in a stretched air arm that must prepare for both offensive and defensive operations that could occur in a two-front war.

Since the Korean War, China’s air arm has been characterized by its great size and poor quality. It had a great deal of metal on the ramp, but that metal was obsolescent and flown by pilots with mediocre skills. Most of its aircraft were single-seat fighters designed as defensive interceptors. As with other countries, the shock of Desert Storm woke Chinese leaders to the fact that its air force was largely useless against a modern power. Today, numbers have been cut dramatically, but quality has increased. New-generation aircraft are proliferating. More importantly, training has increased—although not yet to Western levels—and technical support has improved. Precision weapons, modern ISR aircraft, and, most importantly perhaps, airlifters and air refuelers have entered the inventory. If it is China’s goal to become a world power with the ability to project its airpower over

great distances, then it has begun taking steps over the past two decades to achieve that aim.

Throughout the Cold War era, the air forces of Europe lay in America's shadow. The US Air Force dominated NATO, and Europe had but a meager air refueling, strategic airlift, or ISR capability. Because of NATO's oft-stated defensive posture vis-à-vis the Warsaw Pact, the alliance had a large number of fighter aircraft focused on air defense. Once again, Desert Storm, which occurred immediately after the collapse of the Soviet empire, signaled great change.

The defensive posture of most European nations began to shift to a more offensive mind-set. In this regard, the Balkan Wars were decisive. Even Germany, whose constitution seemed to prohibit involvement in such operations, redefined itself and took part. The size and capabilities of the US air forces meant that Europe had to adapt to fit into coalition operations. PGMs were essential, as were standardized doctrines and command and control lash ups. Because most European countries could not afford "full service" air arms, they have banded together to develop and procure aircraft to be used by all—AWACS and ISR assets, as well as the A-400 airlifter and the new Boeing tankers. Several NATO nations participated in operations in Afghanistan and Iraq, and new members—Poland and the Czech Republic—labored to upgrade and standardize their air forces to become useful partners.

The concluding essay by Lt Gen Dave Deptula (USAF, retired) is excellent. Deptula has long been recognized as one of the most forward thinking and capable airmen in the West. He begins by noting that we now live in an "aeronautical era" in which commercial, civil, and military aviation are preeminent. Thousands of aircraft carrying passengers and high-value cargo are in the air over the globe at any one time. More importantly, airpower now dominates war.

Deptula argues that airpower has been revolutionized in three areas: At the micro level, computing, sensing, and data compression have made formerly single-mission aircraft now able to perform multiple tasks. At the meso (operational) level, airpower has moved from being linked to massive land forces toward greater cooperation with special operations forces, producing disproportionately great effects at low cost and risk. And at the macro level, strategic airlifters, tankers, and global ISR and communications platforms linked by satellites have shrunk the world while also placing great leverage in the hands of the nations, or coalitions, which possess such global power-projection forces.

Controversially, Deptula also argues that air and space technology is evolving so quickly that strategy based on a historical perspective is becoming almost

dangerous. The focus must be forward. He argues instead for strategies based on trends and threats to chart the future. He concludes that success or failure will be determined by “how well a nation can seamlessly integrate airpower across permissive, contested, and denied environments, rapidly synchronizing multiple aerospace missions and functions across the domains of air, land, sea, space, and cyberspace ahead of both competitors and adversaries” (p. 415).

Air Commanders (Washington: Potomac Books, 2013) consists of biographical sketches of US Air Force combat commanders. All are of high quality: some written by established historians (Wick Murray, Alan Stephens, Rich Davis, Dick Hallion, Jim Corum, Rich Muller, Rebecca Grant, and Tom Keaney); others by newcomers (Case Cunningham, Mark Bucknam, Steve Randolph, and Jim Kiras).

The air commanders chosen fall into three groups: World War II and the Cold War; Korea and Vietnam; and Desert Storm to the present. This last was an inspired choice. Most Americans will not have heard of the airmen who led the astoundingly successful air campaigns of Desert Storm (Chuck Horner), Deliberate Force (Mike Ryan), the air war over Serbia (Mike Short), and operations in Afghanistan and Iraq after 9/11 (“Buzz” Moseley). These generals should be remembered.

The sketches of Carl Spaatz, George Kenney, Curtis LeMay, and Otto Weyland are excellent. All except the latter have been much written about and are familiar. The addition of George Stratemeyer—the air commander during the first year of the Korean War—is an anomaly in that 1950 was a near-run thing, and Stratemeyer’s performance was not exceptional. After suffering a heart attack in May 1951, he retired. William Tunner is another unusual but sounder choice. Tunner was an expert airlifter who commanded the “Hump” operation over the Himalayas during World War II, the Berlin airlift, and the airlift of men and supplies to Korea. Too often these essential power-projection air forces are ignored.

The additions of Generals Horner, Ryan, Short, and Moseley are particularly appropriate. In all five of their air campaigns, it was the combination of stealth aircraft and precision weapons—laser-guided and then GPS-guided bombs—combined with ubiquitous ISR and nearly instantaneous command and control, which brought airpower to a pinnacle of success. These air campaigns teamed with special operations forces and indigenous troops—Bosnians, Kosovars, the Northern Alliance, and Kurds—achieved alliance goals with an amazingly small loss of life—on both sides. Conventional US ground forces, when they were even used, confronted enemies largely defeated.

Drawing conclusions regarding the combat leadership of these airmen is difficult, but the first lesson is that they were outstanding pilots and tacticians. William Momyer, who commanded Seventh Air Force during much of the Vietnam War, is considered one of the greatest air tacticians in US history. He was also an ace in World War II, as was John Vogt, Seventh Air Force commander at the end of that war. It would seem that piloting skills were essential in giving airmen the credibility to rise in rank and become air strategists. Second, most of those discussed took a deep interest in the use of intelligence. Although surface warfare is also dependent on sound intelligence, air operations have taken this essentiality to a new level. Because precision weapons with three-meter accuracy can now hit a specific window in a building hundreds of miles deep in enemy territory, it is essential to identify the correct window.

These airmen also had an unusually sound grasp of the political environment in which they operated, a necessity in the politically charged milieus found in the “small wars” that have been the US lot since Vietnam. When every bomb dropped can have major political significance, air commanders must be acutely aware of consequences and implications. Finally, it is apparent there is no single, successful leadership style: Spaatz was shy and taciturn; Kenney outgoing and friendly; Momyer cerebral; and Short was gruff and irascible. Successful leadership style is defined by success.

Taken together, these five works by John Olsen are an outstanding overview of airpower past, present, and future. Olsen and his contributors introduce and explain several ideas that bear emphasis.

From the very beginning, airpower was recognized as a revolutionary weapon that could transform war. Operating in the third dimension, it took a surprisingly short time for aircraft to move from an interesting tactical adjunct of surface battle to a decisive factor in war. Even so, in an age where everything happens with such numbing rapidity compared to previous centuries, airpower—and space power—has sometimes moved more slowly than airmen wanted. The two decades between the world wars saw much theorizing and speculation regarding how technologies not yet invented would revolutionize war. The opening years of World War II demonstrated that aeronautical science was not moving as quickly as airmen had prophesied. And yet, the war with Japan did indeed end with the atomic bombs delivered by B-29s, avoiding a bloody invasion of the home islands that would have cost millions of lives—both Allied and Japanese.

Air and space power are dominated by technology—a notion that has often produced ridicule from the other services who speak derisively of airmen’s “toys” and who contend that battle today is little different than

that experienced by the hoplite armies of the ancient Greeks. This is a silly belief. Yes, fog, friction, fear, thirst, and anxiety are still present in war, but war is not always bloody and violent—as blockade, embargo, and cyber attack illustrate—nor is it always dominated by fear and fatigue. The use of remotely piloted aircraft (RPA) has fundamentally altered the dynamic of combat: aircraft striking targets in Pakistan are controlled by technicians sitting in hangers in Nevada half a globe away. And drones can be very brave indeed.

The use of military force is shaped by technology, budgets, domestic politics, and the geopolitical situation. Instant worldwide communications and information transfer have made military operations subject to intense scrutiny, and this scrutiny falls most heavily on the West. Actions must be seen as politically reasonable—diplomacy must be exhausted before force is sanctioned. When force is applied, it must be measured and discriminant. Collateral damage must be held to a minimum. For domestic political reasons, the “wars of choice” now fought by the West must incur low cost—both in blood and treasure—and those costs should be kept to a minimum even among adversaries. Precision weapons *must* be used to limit damage and death. Decisive victory is still sought, but it cannot be *too* decisive and result in large numbers of enemy dead or unnecessarily excessive physical destruction.

If low cost, low risk, and low collateral damage are the standards measuring success or failure, then air and space power are the obvious solutions. Only a handful of manned aircraft have been lost in combat by the West over the past two decades. In several cases—Bosnia, Kosovo, Libya, and in the initial stages of Operation Enduring Freedom in Afghanistan—conventional ground troops were not even employed. When they were finally introduced, often for occupation duty, the enemy was already defeated. It is a disturbing fact that the vast majority of casualties sustained by the United States and its allies in OEF and OIF occurred after large numbers of conventional ground troops were introduced for occupation duties and counterinsurgency for which they were neither trained nor equipped.

Olsen’s books also touch upon the issue of coercion versus denial. This is an old issue that has generated much debate. Coercion involves a targeting scheme that strikes or threatens what the enemy holds valuable. The intent is to change its behavior. A denial strategy targets an enemy’s military forces or their support structure—the intent is to destroy the ability to continue the war. In essence, coercion targets the enemy’s will, while denial focuses on its capability. Both targeting schemes have been used successfully in war, and they have also failed. In truth, the dichotomy is more imagined than real. Virtually every targeting scheme contains

elements of both coercion and denial, and it is usually impossible to separate them: the destruction of an armament factory or transportation system or the death of a national leader affects *both* the enemy's will and capability. Every situation and every enemy is different, and it is futile to attempt to focus on one target set—leadership, fielded forces, the power grid—and assume it will be the crucial target in any situation. War is not that determinable.

This realization tends to support the claim noted by Deptula: airmen must look to the future rather than the past to determine how to employ their chosen weapon. As a historian, that notion grinds my gears, but in truth, the lessons of history have often been vague, contradictory, or simply wrong. The lessons learned process enshrined in our joint doctrine is a useful intellectual exercise, as long as we always remember that no two situations will ever be the same. Moreover, as World War I and its aftermath proved: lessons learned are not necessarily *correct* lessons learned.

These books show that the introduction of PGMs, stealth technology, and real-time ISR and command and control capabilities have revolutionized war, and even the most obtuse observers recognize how air and space power have changed the conflict environment, at all levels. Interestingly, one major theme continues to appear in all five of the books regardless of the author actually writing each individual chapter. That truism concerns the essential nature of air superiority. All the services recognize this unalterable fact, even if they disagree on how such superiority is to be gained and maintained. In fact, even the basic definition of air superiority is not clearly understood.

There are two aspects to air superiority. First, we are able to prevent the enemy's air forces from attacking our vital centers and fielded forces. This is the aspect understood by everyone. The second is, if an enemy is not attacking us from the air, then we assume we have achieved air superiority. That is not the case. Superiority also includes our ability to strike the enemy's vital centers, sources of supply, or fielded forces at the time and place of our choosing—an important distinction. US joint doctrine is predicated on operating under a curtain of air superiority—and in fact, today we strive for air supremacy. It is questionable if our joint force would know how to operate if that supremacy were lost—we have not had to fight without it since early in World War II. Today, the joint force is absolutely dependent on the unfettered air missions of close air support, air interdiction, ISR, and airlift. If we lose air superiority, those other crucial air missions are difficult or impossible to conduct. If that happens, the joint force is lost. Note, however, that this dual concept of air superiority is a peculiarly US and Western notion. The Vietcong and al-Qaeda never enjoyed air

superiority, and yet they fought extremely well and often successfully against US forces that controlled the air above them.

We also must recognize that the major threat facing our continued enjoyment of air superiority comes from the ground. Since World War II, more than 95 percent of US combat air losses have resulted from anti-aircraft artillery, SAMs, or ground attack by special forces. In fact, since Vietnam, the USAF has not lost a single aircraft in air-to-air combat, even though some of our opponents—Iraq, Serbia, and Libya—possessed modern air arms. However, as SAMs proliferate and become increasingly capable, even our stealth assets might be at risk. Olsen notes the danger of ground-based air defenses, which will increase in the years ahead. What are we doing to address this threat?

Olsen and most of his authors are advocates of airpower. They have studied air operations since their inception, while also looking into the future. They have concluded that air and space forces have been increasingly successful in achieving political and military goals, while doing so at low cost and low risk. There are limitations and weaknesses for these forces, but over the past century the inherent strengths of airpower—its ubiquity, speed, range, and flexibility—have grown stronger; while its weaknesses—cost, the constraints of weather or darkness, its transitory nature, and its inability to hold ground—have grown ever weaker. Radar, infrared, and GPS have done much to eliminate the problems of weather and darkness; air refueling, satellites, and RPAs allow near-continuous air and space operations, and as experiences in Iraq and Afghanistan have demonstrated, occupying ground is often the worst thing we can do if we truly wish to achieve our goals at the lowest cost in blood and treasure.

Col John Olsen is one of the dominant voices in airpower history and operations in the world today. His books should be required reading for everyone in uniform.

Phillip S. Meilinger, PhD
Colonel, USAF, Retired

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.

Book Review

Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security, edited by Scott Jasper. Georgetown University Press, 2012, 272 pp., \$29.95.

Conflict and Cooperation presents potential international security strategies for global commons challenges as they grow more congested, contested, and competitive. Jasper addresses four global commons—maritime, air, space, and cyberspace—and defines them as, “those areas no one state can control but on which all states must rely.” He sees three complex and challenging security areas influencing the commons: violent extremist organizations, regional antagonists, and a rising China. This work includes 13 essays in five sections: security dynamics, conflict methods, cooperative opportunities, interface mechanism, and behavioral norms. Although the entire text strives to emphasize collaborative efforts in each sphere, the emphasis is weighted toward cyberspace and maritime domains.

The first section evaluates security dynamics and introduces the reader to public goods as nonexcludable and nonrival; hence, use cannot be denied, and individual use does not detract from others. All essays support these shared qualities. The shared environment describes the causation behind both the second article’s conflict and the deterrence model used in the third. No essay provides a revolutionary viewpoint, but all contribute to building basic understanding.

The next three essays detail where conflicts could originate within the commons. All three are wide-ranging but primarily discuss Chinese military modernization impacts within the maritime, aerospace, and cyberspace commons. An interesting analytic point emerges on how China’s ballistic missile improvements could potentially undermine the US-Russian Intermediate Nuclear Forces Treaty, demonstrating how any changes within the global commons can affect all players.

Jasper bundles the next two sections as cooperative opportunities and interface mechanisms to provide alternative conflict solutions. Two essays address maritime security, two address cyberspace concerns, and one discusses the US joint operational access future. The primary maritime or cyberspace commons solution is building partnerships and then sharing technological tools to increase awareness and security across the domain. The essay merges cyberspace and space despite the obvious differences. Their only similarities are that both are global commons and both use information. If anything, space requires cyber access much more than cyber requires space access.

One particular article stands out from this group; Paul Giarra’s “Assuring Joint Operational Access” summarizes the intellectual changes required by US strategists to deal with complex challenges. Giarra highlights operational access needs embedded in traditional US war models of getting forward, staying forward, and operating along secured lines of communication. Adversary modernization highlighted in earlier essays could prevent the

United States from enjoying these advantages as fully as in the past. Giarra suggests elevating operational access planning to a new strategic context by recognizing our past assumptions, en-route and forward infrastructure demands, and how our competitors exploit the commons. Ultimately, he correctly states that moving forward cannot occur if the United States falls back to old strategic mind-sets.

New mind-sets must be shaped with new behavioral norms: Jasper's last section. Unfortunately, these essays only address space and cyberspace. Adjusted behavioral norms reinforce those cultural standards the United States wants expressed in the global commons. The whole process matches a suburban "Keep off the Grass" sign. The space article highlights state and nonstate actors' responsibilities to provide debris mitigation, prevent harmful interference, and manage space traffic within the domain.

"Establishing Rules for Cyber Security" by Eneken Tikk is the second exceptional article within the text. Tikk offers 10 standards as a code of conduct within cyberspace. The most interesting requires state and nonstate actors to assume responsibility for any cyberspace actions initiated from their environment. One other central element suggests all actors using cyberspace are responsible for ensuring they possess sufficient security. A patch is the commonly used term to fix a known cyber vulnerability. This patch mandate could close many cyberspace vulnerabilities, but the problem remains who will enforce the issue. Tikk hopes laying out ground rules will encourage all users of the commons to increase the collective standard.

My overall impression is the text never solidly falls behind any of the proposed solutions. Although all ideas are interesting, some could be contradictory during implementation. Most articles were under 20 pages and could use additional depth and discussion. Jasper defined five sections but splitting the work into two halves, conflict dynamics and collaborative techniques, would have been more efficient. Limiting the editorial selection to a narrower scope or a single area would improve the work, as the articles did not blend smoothly. The widely ranging subjects disguised any shared themes, and the editorial wrapper at either end failed to provide a clear path.

Overall, *Conflict and Cooperation in the Global Commons* provides many excellent thoughts, but Jasper may have overreached his goal in his desire to fit everything into a single work. The two articles singled out above are definitely highlights, but all were relatively well written and concise. As an Air Force officer dealing with many A2/AD issues, I would have liked more emphasis on potential strategic considerations. Future conflicts will turn on those strategic elements bridging the commons and they were rarely mentioned. The text whets the appetite for those challenging and complex issues waiting within the commons, but the main course never materialized.

Lt Col Mark Peters, USAF

*Senior-rated cyberspace operator
Wright-Patterson AFB, Ohio*

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.

Book Review

The Generals: American Military Command from World War II to Today
by Thomas E. Ricks. Penguin Press, 2012, 466 pp.

Tom Ricks is imminently qualified to write such a book as *The Generals*. This widely published author has an extensive background in military affairs and knowledge of civil-military relations. This book does not disappoint. It is in fact two books in one. The stated thesis is that military leaders should discipline their subordinates by relieving them rather than prolonging incompetence to the point of having civilian leaders take that action. The book is also a treatise on the shortcomings of Army leaders over time and critiques attempts by the Army to change its process for selecting and protecting general officers.

The five-part tome opens with what Ricks terms “the Marshall system,” beginning in World War II. The following four parts are comparisons to Korea, Vietnam, the interwar period, and the Middle East/Southwest Asia wars since 1990. Under GEN George C. Marshall, senior officers were in many cases relieved without prejudice and given other assignments as rehabilitation (or punishment) before being offered another chance. Marshall preferred senior leaders who could produce results, which required competence and performance. He also expected senior officers to remain apolitical but become politically astute. With the high stakes of World War II, leaders were expected to perform rapidly or be relieved by their immediate commander. Subsequent to that war, according to Ricks, the Army drifted from the Marshall system, and the results were devastating. He notes many examples from Korea, most notable the firing of Douglas MacArthur by President Truman, but saves his most convincing examples for Vietnam when the Army abandoned any semblance of Marshall’s system. During this period the Army descended into an organization of risk aversion, micromanagement, conformity, caution, and lack of moral courage (see p. 257 for exchanges between the president and the joint chiefs).

After Vietnam the Army began rebuilding its image, but that effort focused on tactical levels of fighting—particularly against the Soviets in Europe—rather than strategic and operational levels of war. While some senior leaders within the Army tried to change this focus, most of their efforts were stymied. Thus, most of the senior generals leading the Middle East/Southwest Asia wars were trained tactically for the wrong war and lacked the “flexibility of the mind” both Marshall and Clausewitz insisted upon. Ricks’ evaluation of the post-World War II conflicts shows that far too many senior leaders were allowed to remain in command despite glaring deficiencies in understanding the context of the conflicts.

There is not much to criticize in Ricks’ book, but several issues bear consideration. First, there is no discussion on the impact of the 1986 Goldwater-Nichols law and how this impacted civil-military relations. In some respects this law increased the number of general officers reporting directly to the civilian leadership—without a senior military boss. Ricks cites two examples in the work (Generals Dugan and Woerner) that in fact

did not report to military leaders and thus were correctly relieved by their a civilian boss. Secondly, the context of the number and age of military leaders in World War II relative to the size of the Army today should be considered. Did Marshall have a deeper “bench” from which to “hire and fire?” Surely he did, and perhaps this made it easier to execute his system. Additionally, relative to the size of the Army today, civilian oversight is also larger than in the past and could account for the increase in civilian meddling—regardless of the actions of senior military commanders.

The second thesis of this book—shortcomings of Army generals—may be just as important given the Marshall system basis. Most of the work is a critique of the foibles of senior Army leaders, and this creates some imbalance by presenting more extensive evidence to this effect. The last section, covering the latest Middle East/Southwest Asia wars, is understandably shallower than the previous sections due to the timing of publication. Coverage of Lt Gen Ricardo Sanchez is adequate and relevant to the thesis, but that of Generals McCrystal and Petraeus lacks the same level of detail. None of these critiques detract materially from the keen insights provided about how the US Army and the other services should grow senior leaders, nor do they invalidate the usefulness of a Marshall-type system.

Ricks offers many suggestions on the best ways to restore US military leadership. He intimates the transformation should begin with education, particularly advanced schools for midcareer officers and rigorous war colleges for more senior officers. This is surprising given his penchant of PME bashing. But these institutions will help create and educate the kinds of officers who have the flexibility of mind Marshall expected. Ricks also recommends the services offer second or even third chances to certain officers rather than being a “one mistake” organization—although he thinks this will be difficult to pursue in our current environment. The services should focus on performance, innovation, accountability, and a greater tolerance for risk taking—an implication of the “second chance” system. Finally, Ricks suggests that relief should not be seen as a failure of the system, but rather a strength of the system, and it should be acknowledged publicly to prevent any misconceptions.

The Generals is a very enjoyable read and particularly useful for those officers and civilians from midcareer to senior levels. Even though the content is Army-centric, it may well be one of the best books, along with Cohen’s *Supreme Command*, for newly minted general officers to read before assuming their new rank and position.

W. Michael Guillot

Editor, Strategic Studies Quarterly

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.

Book Review

International Law, International Relations, and Global Governance by Charlotte Ku. Routledge, 2012, 228 pp., \$130.00.

The title of Charlotte Ku's latest book leaves little to the imagination. The professor of law and assistant dean for graduate and international legal studies at the University of Illinois College of Law provides a relatively thorough, if not overly pedantic, breakout of how international relations and international law are conducted in today's global environment and how they shape global governance. She urges the development of a broader understanding of the needs of governance in a global environment.

Ku postulates that the current world order has entered a post-Westphalian stage where the dominant governing body is no longer the sovereign state. Instead, we have entered a stage where international organizations (IO), nongovernment organizations (NGO), and even individuals play roles along with the state in what she describes as global governance. Ku examines global governance from a normative theoretical lens. She sees things as how they *ought* to be in contrast to the realist who may view the same thing from a *factual* perspective, leading her entire book to take a generally positive view of how states, IOs, NGOs, and individuals interact to form global governance.

Her introduction sets the stage for the rest of the book by describing the current impetus for this new global governance. Ku suggests the application of technology and the expansion of cross-border interaction have effectively changed how states relate to one another. This change has had the added effect of creating an increased interdependence among countries and a deep intersection that has made it much harder for one entity to rule. Additionally, she believes states face an erosion of their authority combined with a growing sentiment of distrust among their own citizens. This has led to a loss of their competitive advantage over other possible forms of governance.

To support her thesis, Ku meticulously examines how state and international players have developed over the years and considers how international law and international relations contribute to understanding these developments. Her book is full of examples of how IOs, NGOs, and individuals may interact with the state and shape state behavior. Without a doubt, she provides significant evidence to show that states function much differently than they did even 100 years ago. Some examples include how states need to legitimize the application of force by receiving the endorsement of an IO, how they turn to NGOs as sources of information and guidance related to a variety of different subjects, how they may be faced by legal challenges from their own citizens, or how they may incorporate international legal decisions into domestic law.

Despite these many examples, Ku's argument of a developing global governance is somewhat undermined by the fact that she never fully defines governance or what governance entails. Instead, her book focuses mostly on substantiating that states function differently in relation to other global bodies, but it is not necessarily clear what that means in relation to global governance. While various international parties may have greater interaction with the state, this interaction involves concepts that are more related to how these organizations and legal manifestations induce behavior rather than how they are

codified in some type of global governance. She highlights three elements of governance that include power, authority, and legitimacy, focusing mostly on legitimacy. Although Ku provides a number of examples showing that states interact with or adjust behavior in response to a variety of different global actors, this does not necessarily constitute the manifestation of a new global governance. In some respects, much of what Ku outlines can be described more as effective global activism as opposed to global governance. Without a definition of governance, readers are left to question whether the supremacy of the sovereign state is actually being supplanted.

The biggest problem, however, with Ku's argument relates to her normative lens, which generally sees her conception of global governance developing as things ought to be. Ku rejects the idea that IOs are the agents of their member states and value-free and promotes the idea that they are actually founded on certain assumptions that reflect liberal values. Although they may be independent of any state, she contends that IOs typically bear the heavy imprint, and thus the value systems, of those countries that founded them, to include the United States and the countries of Western Europe and South and Central America, among others. Much of her argument is based in Western democratic ideals and concepts, which ignores that a great number of the players involved in the politics and direction of IOs include states that lack dedication to liberal values. This becomes incredibly important when considering the role that both China and Russia play in the international arena. Both countries cling to the Westphalian concept of noninterference, and their influence over global politics is arguably becoming stronger relative to a weakening West. Any argument postulating the development of a global governance liberally based in IOs, NGOs, and individuals needs to address how these two countries will function, shape, or be shaped by global governance and fall into any such global governance.

Ultimately, Ku's book was written for a specific audience interested in expanding its knowledge of the interaction between international law and international relations as it relates to the complexities of global governance. The average reader is likely to find the book overly academic and beyond the requirements necessary to provide a basic understanding of international law, international relations, and, in turn, global governance. As for the average Air Force reader, the book may provide some insights into the nature of global politics that would affect the application of airpower, whether in pursuit of objectives specifically central to US national security or as part of an internationally endorsed humanitarian operation. But the academic nature of the book may go beyond what the average reader seeks. Although insightful, Ku's book is probably best left for students of international law and international relations.

1st Lt Joshua D. Bower, USAF

Travis AFB, California

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.

Mission Statement

Strategic Studies Quarterly (SSQ) is the senior United States Air Force-sponsored journal fostering intellectual enrichment for national and international security professionals. SSQ provides a forum for critically examining, informing, and debating national and international security matters. Contributions to SSQ will explore strategic issues of current and continuing interest to the US Air Force, the larger defense community, and our international partners.

Disclaimer

The views and opinions expressed or implied in the SSQ are those of the authors and should not be construed as carrying the official sanction of the United States Air Force, the Department of Defense, Air Education and Training Command, Air University, or other agencies or departments of the US government.

Comments

We encourage you to e-mail your comments, suggestions, or address change to: **StrategicStudiesQuarterly@us.af.mil**.

Article Submission

The SSQ considers scholarly articles between 5,000 and 15,000 words from United States and international authors. Please send your submission in Microsoft Word format via e-mail to:

StrategicStudiesQuarterly@us.af.mil

Strategic Studies Quarterly (SSQ)

155 N. Twining Street, Building 693

Maxwell AFB, AL 36112-6026

Tel (334) 953-1108

Fax (334) 953-1451

View *Strategic Studies Quarterly* online at <http://www.au.af.mil/au/ssq/>

Free Electronic Subscription

A forum for critically examining,
informing, and debating national and
international security.

SSQ STRATEGIC STUDIES QUARTERLY

SPRING 2014

AU PRESS



"Aim High . . . Fly-Fight-Win"

