SSQ

STRATEGIC STUDIES QUARTERLY

WINTER 2012 VOL. 6, NO. 4

Commentary
An Interview with Gen Mark A. Welsh III
Twentieth USAF Chief of Staff

Industry's Vital Role in National Cyber Security
James P. Farwell

Crisis Management and the Anti-Access/Area Denial Problem
Col Vincent Alcazar, USAF

Technology, Qualitative Superiority, and the Overstretched American Military
Daniel R. Lake

Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game
Matthew Crosston

Deterring North Korea from Using WMD in Future Conflicts and Crises
Bruce W. Bennett

AIR UNIVERSITY

Strategic Studies Quarterly

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

VOLUME 6 WINTER 2012 NUMBER 4

Commentary

An Interview with Gen Mark A. Welsh III Twentieth USAF Chief of Staff 3

Feature Article

Industry's Vital Role in National Cyber Security 10
James P. Farwell

Perspectives

Crisis Management and the Anti-Access/Area Denial Problem 42
Col Vincent Alcazar, USAF

Technology, Qualitative Superiority, and the Overstretched American Military 71
Daniel R. Lake

Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game 100
Matthew Crosston

Deterring North Korea from Using WMD in Future Conflicts and Crises 119
Bruce W. Bennett

Retiring? Moving?

For continued subscription service

Please send change of address to:

StrategicStudiesQuarterly@us.af.mil

NEW WEB PAGE DESIGN

COMING SOON

NEW LINKS, NEW INFORMATION

FREE ELECTRONIC SUBSCRIPTION

SAME SITE ADDRESS:

www.au.af.mil/au/ssq/

An Interview with
Gen Mark A. Welsh III
Twentieth USAF Chief of Staff

SSQ: *General Welsh, what top challenges do you expect to encounter during your term as chief?*

General Welsh: Rather than challenges, I see great opportunities for our Air Force, the foremost being the sharing of our Air Force story with the public, with the Congress, with industry, with our sister services, and our coalition partners. Telling our story is also important when it comes to motivating the force. We've been at war for 20-plus years now—through Northern and Southern Watch, Allied Force, and deployments to and from Southwest Asia over the last 10 years, along with everyone else. Our Airmen are doing amazing things! They move people and cargo around the world. They conduct intelligence, surveillance, and reconnaissance operations in every combatant commander's AOR. They fly lifesaving aeromedical evacuation missions to get wounded warriors off the battlefield and back home for treatment and care. They're on the ground leading convoys, clearing improvised explosive devices, and calling in airstrikes. They resupply ground forces with tactical airdrops. They provide nuclear deterrence for the nation. They deliver space-based communication, navigation, and missile defense warning. They're fighting shoulder-to-shoulder on the battlefield with their Army, Navy, and Marine Corps teammates. They patrol the skies above them, ready to respond when needed most. And they make it all look easy—sometimes too easy. In reality, it's pretty tough to do. Our Airmen are not overstressed, but they are tired, and their families are tired. Part of my job is to tell our story so people understand the skill, the determination, and the resources that it takes for the Air Force to make these capabilities available to the combatant commanders.

The future security environment represents another opportunity for the Air Force. Although the US military must prepare to operate in every domain on, under, or above our planet, I believe the air, space, and cyber domains are likely to be those most contested in the future. The Air Force brings unique expertise to each of these domains, and we

will preserve and fortify those areas where we are most mature, while also exploring and influencing those areas where we are less mature.

For the next five years, the Air Force will not see a lot of new aircraft and equipment. It will take a while for much-needed modernization to appear. But Airmen must know their contributions matter—that what they do makes a difference. So I think for my tenure as Chief, the job is going to be to communicate clearly, motivate as much as I can, and make sure Airmen understand just how good they are, and how proud they should be of themselves and what they represent. If I can do that, they'll take care of everything else.

SSQ: *Do you have a list of priorities you feel must be addressed within the next year, and what are your longer-term priorities?*

General Welsh: Upfront, we have some work to do to rebuild trust and credibility with the Congress. I met with several senators during my confirmation process, and each one mentioned they were concerned about communication and transparency between the Congress and the Defense Department, and specifically with the Air Force. The *perception* is that the Air Force does not tell the whole story—that it does not offer full disclosure. That's no way to do business; it's certainly not our intent or our practice as we see it; and it is clearly something Secretary Michael Donley and I must address. There is absolutely no question that the Congress and the Air Force are both focused on doing what's best for the nation. So we will work harder to ensure timely, open, and transparent communication with the Congress. This won't be a one-time effort; it will be a consistent long-term effort to strengthen and maintain the relationship of trust that we must have with the Hill.

The second focus item is the active-reserve component mix within the Air Force. Our 2013 budget arrived on Capitol Hill and basically ran into a brick wall, principally because of concerns with adjustments made to our active-reserve component mix. This led many people to believe there is a problem with Total Force integration in our Air Force. Nothing could be further from the truth. The *process* that led us to submit the 2013 budget proposal can be improved. We will fix it and move forward together to craft the Total Force that best balances requirements, capabilities, risk, and cost on behalf of our nation's defense and our states' requirements for disaster response.

Out where the Air Force operates, you can't tell a Guardsman from a Reservist from an active duty Airman. The Total Force is still seamless and strong in the US Air Force. But, the Airmen who are on the front end of our business, the ones who are fighting side-by-side doing incredible work

every day, are looking over their shoulder at us wondering, "What are you guys doing back there?" And so we have to figure out how we can improve the coordination and communication process inside the Beltway and with the state governors and adjutants general to make sure everybody has input to, and fully understands, the intent and the approach of our future force structure and resource planning efforts.

Longer term, we must figure out a way to modernize our Air Force. The health of our aircraft fleet has been a lingering problem, and we've been lucky that our equipment has survived well beyond expected service lives and that our great Airmen continue to keep the aging fleet operating. Twenty-plus years of full-time activity in multiple war zones have aged equipment faster than we originally planned. We are flying airplanes at a much higher rate, and this has caused our fleet to age dramatically. There's no secret about that. We've taken great care of the fleet, and it's still getting the job done. But it won't last forever.

Also, we will soon begin the transition to a peacetime Air Force. As the drawdown in Afghanistan continues, I suspect that the Air Force will probably remain there as long as any of our services. But as we reduce our footprint, we must figure out what to do with some of the capabilities we invested in for operations in Afghanistan and Iraq. For example, what do you do with the fleet of remotely piloted aircraft? How might they be used in other theaters, particularly in the nation's rebalance to the Asia-Pacific region? What about Africa? What about the Airmen who make up the ISR enterprise? How will that key mission area adjust to a new environment? And finally, where does the Air Force best contribute in the cyber arena? These are some of my concerns.

SSQ: *It has been said the Air Force will get smaller in the future but will be of higher quality. What do you see as the opportunities and risks associated with this kind of Air Force?*

General Welsh: Given the fiscal constraints we're facing as a nation and in light of the new defense strategic guidance, the Air Force made some strategic choices to get smaller. These weren't easy decisions, but they were necessary to protect our quality and readiness. Failing to reduce our size risks hollowing out the force—there just isn't enough money in the budget to support a large force structure. To do so, you have to take money from modernization and training to pay for it. That's horrible trade space in which to operate.

We need to reduce some of our excess capacity to provide the cost savings needed to modernize the force. A smaller force allows us to modernize

our fleet and repair or replace worn-out equipment. It also ensures our Airmen receive the training needed to be the best on the battlefield. The men and women in our Air Force are proud of what they do and how well they do it. We ask a lot of them, and they always deliver. That pride is an integral part of what makes our Air Force special . . . and successful. Airmen have been at war for 20-plus years. Ninety percent of our team has joined since the 9/11 attacks. The tempo has been tough, but they continue to serve because they're proud and they have a tremendous sense of purpose. Their families continue to support them through the multiple deployments, the missed birthdays, the missed anniversaries, and the missed holidays because they're proud of their Airmen too. But if we can't provide the equipment our Airmen need to do their jobs; if we don't give them the training they need to be the very best at what they do; if we allow frustration to take root and override that pride, they'll walk. I can't let that happen . . . we simply can't be successful without them.

SSQ: *Not long ago you mentioned innovation as important to the success of the Air Force. What areas do you think require the greatest innovative efforts today?*

General Welsh: Innovation is part of our DNA. It's in our institutional fabric. The early airpower pioneers looked at the World War I and II battlefields with a perspective of "over, not through." Today's Airmen use developing technology in new and innovative ways every single day. As I look ahead, innovation—fueled by intelligent, creative Airmen—will remain a key part of who we are and what we value as a service.

The pressures on us from a budget perspective are significant. They include those from sequestration, if it occurs, as well as the pressures from a continuing decrease of our budget, even if sequestration doesn't happen. A smaller budget means that we must find innovative ways and new tactics, techniques, and procedures to use the people, tools, and aircraft that we do have as effectively as possible. This is not a new approach. Technology allows us to do some amazing things on the battlefield, and it's a tremendous force multiplier. As a young officer, I never imagined using a bomber to provide close air support for troops on the ground. But that's exactly what we've been doing. Special Ops C-130s are carrying the small-diameter bomb, allowing them to do the same. And when you think about RPAs, I believe we have just moved out of the "Wright Flyer stage" with these systems. Over the next 20–30 years, these capabilities are going to advance, and advance rapidly. No one knows exactly what will happen next, but it's going to be exciting to watch! The only thing I'm sure of is

that our Air Force will lead the way, because nobody develops and integrates new technology into air operations on a large scale as well as we do.

The security environment will also drive the need for innovative thought and action. The growth of anti-access/area denial (A2/AD) methods and strategies by potential adversaries—ballistic and cruise missiles, guided rockets, integrated air defense systems, submarines, antiship missiles, sea mines, and fast-attack boats—led us to the Air-Sea Battle concept. If you're trying to operate in the A2/AD environment, you're going to look for capabilities that increase platform ranges, link and extend sensor ranges, extend weapons envelopes, and maximize stealth. Interoperability and the ability to communicate and share data with our sister services and key allies and partners are also essential. It takes some out-of-the-box thinking. Gen Norty Schwartz described Air-Sea Battle as a "furnace for ideas." And that's exactly what it is. The concept allows the services to study, evaluate, and pursue synchronized investment to better support the combatant commanders in an A2/AD environment, making more efficient use of the limited resources we have.

SSQ: *Over the last year our Air Force seems to have been rocked by, and in some cases rebuked because of several controversies including the place of religion in the service, the Dover mortuary, sexual assault at Basic Military Training, and the F-22, just to name a few. How would you address our critics who may be questioning the efficacy of the Air Force?*

General Welsh: First I want to say that I'm proud to lead and serve the 690,000 Airmen who fight in our nation's Air Force. We have great people, a great mission, and a great heritage. Like many other large organizations, we've seen our share of headlines, and we continue to work through those issues to make our service better. But I don't measure the worth of our Air Force by those issues. Not one of those headlines detracts in a meaningful way from what our Air Force means to this nation. Only the Air Force gives our decision makers the capability and capacity they need for air superiority, nuclear and global strike forces, ISR, rapid global mobility, and command and control operations, all enabled by space and cyber forces. I truly believe that we are at our best providing those enduring capabilities that our nation relies on, and those are the areas where we must continue to focus.

Gaining and maintaining air superiority is foundational to how we fight as a joint force. The Army, and to a degree the Marine Corps, depends on us to get this right. The fact that no US military member has been killed

on the ground by an enemy combat aircraft since the Korean War reinforces this notion. Our ground troops have grown so accustomed to fighting absent enemy airstrikes that many of my joint counterparts no longer worry about hostility from above. Air superiority is not a birthright, nor is it easy to provide. Today's adversaries have been deterred from meeting us in the air largely due to our technological, operational, tactical, and training dominance. This is an advantage we must not sacrifice. If we can't provide the air superiority that guarantees American ground forces both freedom to attack and freedom from attack, then the way the US military currently fights on the ground will have to change. Air superiority is fundamental to the American way of war.

We have a team of 36,000 Airmen who are focused on the Air Force's number one priority, the nuclear mission, each and every day. They live a standard of excellence. The mission demands it. Their stewardship ensures that our nuclear arsenal—two-thirds of America's nuclear triad—is safe, secure, and able to hold targets anywhere on the planet at risk. I often hear that since the Cold War has passed, so has the nation's need for a robust nuclear deterrent and global strike force. That notion is diametrically opposed to our nation's current policy and deterrence strategy. To implement that strategy, our nuclear and global strike forces require maintenance and modernization, as with any aging capability. We can debate the size of the nuclear force, but its presence and operational surety are nonnegotiable in my book.

Nobody does ISR to the scope and scale of the United States Air Force. RPAs have proven themselves essential in developing situational awareness of the battlespace to commanders and troops on the ground. There's been a significant demand for this capability, and the Air Force has invested heavily in RPAs to support the need. The Air Force is also largely responsible for the processing, exploitation, and dissemination of intelligence data after its collection. The effects of this powerful capability are huge. From responsiveness and timeliness, to accuracy and precision, Air Force ISR provides the data, information, and connectivity to fuse and synchronize joint operations. However, Air Force ISR has largely been conducted these past 20-plus years in a permissive environment. We must plan for and invest in the future of the Air Force's incredible ISR contributions to our nation's defense. It's critically important that those contributions be possible in all scenarios, to include operations in contested battlespace.

Strategic mobility is the backbone of US military power. Airlift, aerial refueling, and contingency response groups fulfill the need to rapidly

move personnel and cargo throughout the world, to deliver humanitarian aid and a helping hand to those in need, to bring our wounded warriors home, and to deploy forces to deter enemy aggression. We launch an airlift sortie every two minutes, 24 hours a day, 365 days a year. Mobility has been an Air Force core mission since its inception—it's a clear warfighting advantage that we must not surrender. Global reach is part of who we are as an Air Force and as a nation.

Everything we do in our Air Force is enabled in some way, shape, or form by capabilities and command and control processes that incorporate assets in the space and cyber domains. From GPS positioning to weather forecasting and ISR collection and dissemination, the Air Force space mission transcends service and departmental boundaries. Our Airmen lead the Department of Defense effort to ensure the same situational awareness and freedom to operate in space that we have in the air domain. It's another mission area where modernization and technological edge must not be sacrificed, but whose effects are often behind the scenes. Air Force cyber warriors protect our command and control infrastructure and networks, ensuring that the connectivity we've come to rely upon is not hacked, spoofed, or jammed. The ability to command and control operations on a regional scale is something our combatant commanders expect from us. It's also a clear advantage we enjoy over our adversaries. Each of these areas is of growing importance to our nation, not just to our Air Force and the joint war fighters we support.

My point here is simple . . . the Air Force matters. We're not more important than any other service, but we are equally critical to the nation. More importantly, our Airmen matter. They serve with pride, living our core values of *Integrity, Service*, and *Excellence*. Without them and their joint teammates, there would not be air superiority, nuclear and global strike forces, persistent ISR, rapid global mobility, or the enabling capabilities that our command and control, space, and cyber assets provide. It's our people who make that all possible—people who are proud, well-trained, well-equipped, and ready. No matter what issue hits the headlines to distract us, it's important that we tell their story enough times, to enough audiences, so there is no question, confusion, or doubt about what our Airmen provide for America. Our job is to stand beside our sister services to fight and win this nation's wars. We have a track record of doing exactly that . . . and we'll remain ready to do it in the future. SSQ

Industry's Vital Role in National Cyber Security

James P. Farwell

The competing demands of economic recovery and protecting critical cyber infrastructure (CI) have heightened the need for stronger partnerships between the US government (USG) and private industry. Developing new technologies, strategies, plans, operations, tools, and techniques are essential to protect cyber security. How we meet this challenge has opened an important philosophical debate in the United States about the role of government and its relationship to private industry.

US Cyber Command chief Gen Keith Alexander has advised Congress that cyber threats to military and commercial sectors are growing and that criminals have exploited 75 percent of our nation's computers.[1] Intelligence and criminal threats have spotlighted discussion on how the military protects its assets, networks, and systems, and no one disputes the military's pivotal role in cyber security.

Yet, 90 percent of US critical cyber infrastructure is owned by the private sector.[2] Melissa Hathaway, who served as the cyber coordination executive for the Director of National Intelligence (DNI), has rightly pointed out that corporate and political leaders "appear to be paralyzed about meeting the needs for our cyber infrastructures and enterprises."[3] This current deadlock undercuts American security interests, and Congress must strike a balance between competing policy perspectives for cyber security. The dilemma is that earning a profit motivates industry, while protecting national security motivates the USG. Although often complementary, these agendas do compete. What is required is a confluent approach that removes legislative obstacles to stronger cyber security, forges robust partnerships between the public and private sectors, and better manages risk in the global supply chain. A review of current US strategy and the threat matrix is instructive in framing a new approach.

James P. Farwell is an expert in strategic communication and information strategy who has served as a consultant to the Department of Defense, the US Strategic Command, and the US Special Operations Command. He has three decades' experience as a political consultant in US presidential, congressional, and other campaigns. He has published numerous articles and *The Pakistan Cauldron: Conspiracy, Assassination and Instability* (Potomac Books, 2011).

The Current Strategy

A 2007 presidential directive ordered the Department of Defense (DoD) to protect its critical infrastructure.[4] The order endorsed a collaborative, coordinated effort to identify, assess, and improve critical infrastructure within the defense industrial base (DIB).[5] The DIB includes "the DoD, US government, and the private sector worldwide industrial complex with capabilities to perform research and develop, produce, deliver, and maintain military weapon systems, subsystems, components or parts to meet military requirements necessary to fulfill the National Military Strategy."[6] Most of the DIB is privately owned. It includes businesses of all sizes, including small, innovative companies that move rapidly and offer cutting-edge ideas that can be translated into usable products.

The Department of Homeland Security (DHS) holds responsibility for protecting civilian critical infrastructure and key resources (CIKR).[7] CIKR includes "assets, systems, networks, and functions that provide vital services to the nation," for which attacks or disruption could produce large-scale human casualties, property destruction, and economic damage as well as damage national prestige, morale, and confidence.[8] To help coordinate protection responsibility, the DHS devised a national infrastructure protection plan (NIPP).[9] In concept, the NIPP provides a unifying structure to integrate efforts to protect the CIKR into a single national program. The plan aims to balance resiliency with focused, risk-informed prevention and preparedness. Eighteen sector-specific plans (SSP) support the NIPP. These address efforts among local, state, and federal efforts, the private sector, and international organizations and allies.[10] Plans provide vision, coherence, and courses of action for a way ahead. But what must be done to more fully implement the current cyber strategy?

In July 2011, the DoD released its new *Strategy for Operating in Cyberspace*.[11] Five precepts guide it. First, by treating cyberspace as an operational domain, it seeks "increased training, information assurance, greater situational awareness, and creating secure and resilient network environments." Second, calling for "cyber hygiene" in security, it looks to strengthen the workforce and employ new operating concepts to improve security. Third, it recognizes that private-public partnerships form the foundation for an "active, layered defense." Fourth, it embraces international partnerships. Since cyberspace transcends traditional geographic borders, incidents may occur across national jurisdictions, and effective action requires multilateral cooperation among allies. The NATO 2020 report also calls for

incorporating cyber defense into allied strategic thinking.[12] Finally, the strategy aims to catalyze civilian talent and ingenuity to spur new technology. It recognizes that entrepreneurs in small and medium-size companies often stand at the cutting edge in moving concepts from innovative idea to reality and scaled adoption.

The Emerging Threat Matrix

What is a cyber threat and how should that term be defined and addressed? One starts by distinguishing between cyber threats and cyber indicators. The distinction matters. Cyber experts Dan Auerback and Lee Tien suggest that a cyber security threat is what we guard against, while a "cyber security threat indicator" is the activity that allows private or public entities to monitor and execute countermeasures. They note that stealing passwords from a secure government server might be a threat, while a port scan to search for vulnerabilities is an indicator—a vague distinction. Legislative reform needs to clearly define each and address every aspect of cyber security.[13] Definitions need to embrace the notion that counterintrusion is self-defense and clearly define exploitation, counterexploitation, and self-defense tactics. Century Link's chief security officer David Mahon has well summarized the major cyber threats faced by the public and private sector.[14] They fall generally into four categories: nation-state intrusions (also known as "advanced persistent threat"); criminal, which extends to sophisticated organized crime; "hackivism"; and insider attacks.

Fast-evolving technology is altering the strategic implications for cyber capabilities, expanding and intensifying these threats. The world around us is changing quickly, reshaping the political environment. That affects strategic considerations. The Internet stands out as an emblem of this radical transformation. The global digital infrastructure, "institutions, practices and protocols that together organize and deliver the increasing power of digital technology to business and society,"[15] has reconfigured how business is conducted. Preparing for the next threat requires thinking ahead. Defensive strategies that worked before may prove obsolete if one attempts to win the next war by refighting the last one.

The threats are also new. Former assistant secretary of defense William J. Lynn has long worried about the impact of network destruction.[16] The Russian-backed denial of service attacks on Estonia and Georgia[17] and the assault on eBay and PayPal by the hacker group Anonymous illustrate

that governments and companies are both vulnerable. The emergence of cyber weapons like Stuxnet, which impeded Iran's nuclear centrifuge program, opens a window to the future.[18] Initial reports suggested that assets of friendly nations, such as an Indian satellite, also sustained damage,[19] although doubts about that later arose.[20]

Critics of Iran cheered Stuxnet I. But Stuxnet II may target US or allied critical infrastructure. Blended attacks, employing cyber and kinetic weapons in combination, could zero in on military and civilian targets, destroying some while launching sophisticated penetrations of networks that control critical civilian infrastructure. The emerging political ecosystem in which new weapons are originating from nonstate parties, including criminal enterprises, unveils complicated and unpredictable scenarios.[21]

Concerns about Chinese cyber espionage and piracy (or, in obtuse national security jargon, "cyberexploitation") highlight another challenge. The US-China Economic and Security Review Commission has repeatedly warned that the Chinese are guilty of rampant cyber piracy—stealing intellectual property and trade secrets vital to US defense and to keeping it technologically competitive.[22] This concern is one element of a broader challenge, as rivals or foes employ multiple channels to acquire confidential and proprietary data. A 2012 report to the commission points to "collaboration between US and Chinese information security firms . . . over the potential for illicit access to sensitive network vulnerability."[23] What cannot be hacked may yet be obtained through legal acquisition from US companies. These concerns must be addressed as part of a broad strategy to protect our interests.

Human mistakes or errors in judgment challenge our most sensitive networks and systems, as Dr. James Peery of the Energy Department's Sandia National Laboratories warned the US Senate that we must "assume our adversary is in our networks, on our machines." Still, he noted, "We've got to operate anyway."[24] His fears are well founded. In 2008, hackers penetrated the Pentagon's classified Secret Internet Protocol Router Network (SIPRNET) when a flash drive loaded with "Agent.btz," a malicious code devised by a foreign intelligence agency, was left in a Middle East parking lot. Later, someone inserted it into a USCENTCOM laptop.[25] The incident infected computers and even the Joint Worldwide Intelligence Communication System, which carries top-secret information. The damage inflicted remains undisclosed.[26]

Lynn acknowledged that other penetrations remain undetected.[27] He considered the 2008 penetration an "important wake-up call" and a

"turning point."[28] The Pentagon took remedial action, launching Operation Buckshot Yankee that led to banning the use of thumb drives[29] and creation of the US Cyber Command. Still, the incident proved how nettlesome cyber attacks can prove. Cleaning up this single problem took the Pentagon 14 months[30]—proof, one might argue, that private companies may prove more agile in coping with such crises and might have gotten the job done more efficiently.

The Pentagon recognized the problem as early as the 1990s. Solar Sunrise, a series of computer attacks in 1998 that targeted defense networks, led to intrusion detection systems on key nodes.[31] The incident confirmed findings derived from the 1997 Eligible Receiver exercise that had uncovered vulnerabilities in DoD cyber systems and demonstrated the increasing risks to US interests in cyberspace.

Individual attackers have underscored the potential for mischief. Over a decade ago, New Jersey programmer David Smith created "Melissa," a virus that used a Microsoft Word document sent as an e-mail attachment to infect classified US commercial networks, forcing Microsoft and Intel to shut down their e-mail servers.[32] The incident revealed that human beings are often the weak link in cyber security—recognition pivotal to the new US strategy.

At the same time, corporate vulnerability is growing. A Bloomberg survey of the utility, telecommunication, financial services, and health care industries revealed that technology managers in 124 companies—each with at least 10,000 workers—said they could double spending on cyber security and yet their networks would remain vulnerable.[33] An attack originating in China pirated intellectual property from Google.[34] Payments processor Global Payments reported a breach that affected 1.5 million credit card account numbers, forcing VISA to revoke its seal of approval from the company.[35] Mike Blake, chief information officer of the Hyatt hotel chain, commented, "If those guys can be penetrated, so can anyone else. So prepare yourself to be penetrated."[36] Sony Corporation has admitted that hackers accessed personal information on 24.6 million customers on a single online game service in an attack that compromised 100 million accounts.[37] Hackers have stolen data from 77 million Sony customers and compromised over 360,000 accounts at CitiBank.[38] Even highly sophisticated parties remain vulnerable. Worse, many companies remain unaware of hacking and theft.[39]

Stealthy foes can also corrupt hardware and software. Reportedly, Russia and China have probed the US power grid to identify vulnerabilities and have left behind software programs that may be deployed for disruption.[40] Concrete evidence of cyber mischief surfaced in Australia, where a disgruntled employee rigged a computerized control system at a water treatment plant and released over 200,000 gallons of sewage into parks, rivers, and the grounds of a Hyatt hotel.[41]

In a penetrating analysis of the cyber world, Heritage Foundation expert and author James Carafano points out the revolution that Internet technology has wrought. In unprecedented ways, he notes, a very few people can strongly impact masses of individuals.[42] He was writing about influencing crowd behavior, but his point holds for the threats small groups of individuals, acting alone or as state proxies, pose to critical infrastructure. Today one individual can change the way we think about the world and how we do business. At age 20, Mark Zuckerberg upended the way people communicate with one another in creating Facebook.[43] Sean Parker founded Napster and changed the music industry.[44] And over a decade ago, two Filipino computer programmers infamously devised the "I Love You" virus that caused over $5.5 billion in damages and infected more than 50 million computers.[45]

Not only existing networks or systems raise concerns. Microsoft's Eric Warner has cautioned that foes can "manipulate or sabotage systems during their design, development or delivery to determine or disrupt government functions."[46] Peery has labeled the information technology supply chain "a particularly insidious risk" and of "high consequence" to national security systems because of our widespread reliance on commercial-off-the-shelf (COTS) hardware and software technology that is increasingly produced, in whole or in part, by untrusted, non-US organizations. Unfortunately, the growing complexity of these systems also makes it economically infeasible to verify them thoroughly.

Insufficient attention has been given to technical approaches for mitigating supply chain risks. Counterfeiting and subversion of critical components in high-consequence DoD systems could have a devastating effect on our ability to project military power with confidence around the world. "Better methodologies and technologies are needed for assessing and managing supply chain risks."[47]

The Federal Bureau of Investigation's top cyber cop, Shawn Henry, minced no words about where we stand in the battle to fend off hackers.

"We're not winning," he told the *Wall Street Journal*. In his judgment, the current private and public approach is "unsustainable."[48]

The 2011 RSA Security case is illustrative from an industry perspective. RSA manufactures a two-factor authentication token, SecureID. These widely used electronic keys use a two-pronged approach to confirm the identity of the person trying to access a computer system. Their technology is used by many financial networks and defense contractors. Infiltrators breached and compromised the systems of US defense contractors, including Lockheed Martin, who fell victim to hackers using duplicates of RSA's SecureID tokens to penetrate internal networks. The event forced Lockheed to shut down all remote access to its intranet for at least a week.[49] The significance of the infiltration is manifest in the fact that Lockheed and RSA supply coded access tokens to millions of corporate users and government officials.[50]

The event cast into high relief the tension between private and public interests. Although RSA eventually disclosed the problem to customers,[51] critics blasted the company for putting its interest in earning profits and maintaining the commercial viability of its product ahead of the security concerns of customers.[52] It took a week before RSA briefed the press about the problem and much longer to reveal that the attack had compromised its technology. Critics argue RSA's behavior cost clients millions of dollars.[53]

The company finally made a formal disclosure on its 8-K filing to the US Securities and Exchange Commission.[54] Experts like Hathaway argue the commission ought to require companies to make timely disclosures and to take remedial action.[55] The public interest clearly supports Hathaway's position. Why did RSA not act sooner? The most obvious inference is that the company perceived its own interests in a different light. RSA has shown little remorse, and one wonders whether it worried more about its legal consequences than its customers. The challenge underscores the need for Congress to provide strong incentives for information sharing and legal immunity by encouraging manufacturers to make affected stakeholders aware of cyber threats.

The Debate on Legislative Reform

Most agree that stronger cyber security requires legislative reform. Unfortunately, Congress has deadlocked over competing philosophies about government regulation and information sharing. The divide reflects partly whether the debate is about national security or economic growth.[56] The

official report to the Permanent Select Committee on Intelligence in 2012 that supported Rep. Mike Rogers' cyber security bill which passed the US House but faced a White House veto, concluded that "intelligence collection efforts can and should be provided—in both classified and unclassified form (when possible)—to the private sector in order to help the owners and operators of the vast majority of America's information infrastructure better protect themselves."[57] The committee's observation helps frame the challenges.

Although reform efforts in 2012 failed, the issues are important and will likely see renewed debate in the next Congress. Two proposals spotlighted the debate. Senators Joe Lieberman and Susan Collins introduced the Cyber Security Act of 2012 (CSA),[58] while Senator John McCain introduced the SECURE IT Act.[59] Examining the policies that underlie each proposal illuminates the debate on what reform makes sense and what stands a chance of passage.

Competing Legislative Proposals

The Cyber Security Act (CSA) of 2012. Strongly supported by the White House, the CSA took dead aim at companies deemed unwilling to invest resources into providing strong cyber security. It set up a mandatory regulatory scheme that required critical cyber-infrastructure companies to propose DHS-approved security standards or have standards imposed upon them. It directed the DHS to work with industry to assess the risks and vulnerabilities of critical infrastructure and to develop security performance requirements for "covered critical infrastructure."[60] Either relevant federal regulators with authority over a particular industry or the DHS itself would oversee this regime. White House cyber security chief Howard Schmidt insisted that cyber security standards were essential. "As long as there are weak links in the core critical infrastructure," he declared, "there's a risk for everybody."

CSA sponsors also considered the existing patchwork of regulatory authorities inadequate. Regulatory bodies like the Federal Energy Regulatory Commission (FERC) or the Federal Communications Commission (FCC) possess authority to compel action, but they comprise a diverse matrix. Many doubt they can provide strategic cohesion. Complicating matters, states share regulatory authority with parties like the FERC.

Critics insisted that the proposed scheme would unreasonably burden industry, choke innovation, and hurt competitiveness, while failing to im-

prove cyber security. They argued that potential mandates would be costly and potentially unaffordable to many companies. Hitting legislative roadblocks, CSA sponsors amended the bill, arguing the ammendments would make regulation voluntary.[61] The amended bill sought to promote investment in cyber security research, establish public-private exchanges for information sharing, and promote what it characterized as voluntary regulatory practices by companies to secure computer systems in exchange for legal immunity for information sharing. The opponents were not assuaged.

Critics dismissed the amendments as a ruse. They argued that even in this form, the government, not the private sector, would adopt and promulgate all standards. They charged that the bill failed to consider the specific needs and economic interests of small businesses. They complained that the bill carved out technology products, including those manufactured in countries like China, exempting them from characterization as cyber infrastructure.* They argued that the provisions for giving security clearances to companies were too lax† and that the framework for sharing information under the bill meant more government bureaucracy by giving the DHS secretary unchecked authority to designate federal and nonfederal entities as cyber exchanges. The provisions on information sharing were considered complicated and likely to impede rather than encourage private industry to share information and impeded the government's ability to use cyber threat information provided by the private sector to prevent terrorist acts or catch spies.‡ A coalition of business and civil liberty groups, including Fight for the Future and the Electronic Frontier Foundation, joined to help defeat the CSA. Business blasted the revised bill as still unduly burdensome to commerce and denounced the DHS as incompetent to supervise any regulatory scheme for cyber.§ Civil liberties groups worried that the CSA provided a license to spy on web users, provided information gleaned to the USG, and claimed broad legal immunity for actions. Other critics lamented that the bill created a spying regime that enabled surveillance of any threat a company perceived to its network. For instance, the bill provided that a "cyber security threat" existed if a company concluded that a user was obstructing its networks and it authorized

---

*CSA, S 3414, Section 102(b)(5).

†CSA, S 3414, Section 102(b)(5).

‡CSA, S 3414, Section 704(g) and 104(c)(4).

§CSA, S 3414, Section 103(a), (b), and (g) drew fire as empowering the federal government to mandate standards.

blocking action to disrupt user action.[62] Skeptics felt this gave companies overly broad discretion. On the other side, supporters felt privacy groups had been appeased by eliminating the DoD's existing ability to get cyber threat information immediately and directly from the private sector.*

The SECURE IT Act. SECURE IT aimed to facilitate information sharing and assigned the DoD the lead on cyber security. It espoused the view that compulsory regulation was unnecessary, as companies had a vested interest in building and maintaining customer support by providing secure IT services. In the House of Representatives, SECURE IT was preempted by passage of the substitute Cyber Intelligence Sharing and Protection Act (H.R. 3523), sponsored by Rep. Mike Rogers.[63] Bearing certain similarities to SECURE IT, H.R. 3523 facilitated swapping cyber threat intelligence and information between "appropriate, cleared" private companies and individuals and the National Security Agency (NSA) and other government departments like the DHS.[64] The House-passed bill required the head of a federal department or agency that receives cyber threat information to share it first with the DHS. Only by request and DHS approval could that information be shared with other departments or agencies.[65] SECURE IT supporters criticized the proposal for unnecessarily inflating the role of the DHS at the expense of the NSA, the Department of Justice, the DoD, and other stakeholders. The Rogers bill proved a footnote after the White House made clear it would veto the bill. Thus SECURE IT stood as the alternative to the CSA. Perhaps not surprisingly, legislative deadlock killed 2012 reform, arguably a casualty of overreaching. The wiser legislative strategy would have been to enact legislation that addressed information sharing, where common ground might have been found, while delaying debate on the more controversial ideas for regulation.

Prominent Legal Obstacles to Stronger Cyber Security

While debate over whether standards for cyber security should be mandated or voluntary has occupied center stage, other prominent obstacles that require legislative action include (1) US antitrust and unfair business laws[66] and (2) privacy laws such as the Electronic Communications Privacy Act and the Stored Communications Act.[67]

---

*CSA, S3414, Sec. 703(a)(1). Instead, NSA and DoD agencies would be required to obtain such information from DHS-selected exchanges in "as close to real time as possible." Sec. 703(a)(2). Critics argued that these provisions would delay access to real-time cyber threats, including those from China, Russia, and Iran.

The RSA incident illustrates why information sharing and information protection among companies is vital to identify risks and vulnerabilities, counter cyber threats, and create databanks. Companies and government need access to what the other knows or learns. Uncovering errors or problems in software, especially when they may occupy a few lines of code in a product that contains tens of millions of lines, can be difficult. Detection of a vulnerability—a worm, virus, trapdoor, or other risk—as well as countermeasures a party may develop should be shared with other potential cyber targets. Viable cyber security strategies mandate that all parties act on an informed basis.

Equally, the government has a strong interest in ensuring that sensitive or classified information is closely held by appropriate parties. That interest must be balanced with the need to provide innovative entrepreneurs who develop cutting-edge technology access to the information needed to create solutions.

Antitrust Regulation. Companies fear the antitrust division of the Department of Justice and the Federal Trade Commission (FTC). Both watch for activity perceived as collusion that may lead to price fixing, abuse of market power, allocation of customers, and other anticompetitive activity. Their posture underscores another dimension in the tension between public and private interests. No one challenges the conceptual validity of antitrust or unfair-business laws. But the public interest in promoting anticompetitive practices embodied in those laws must be balanced against national security interests.

In practice, larger companies—staffed by top-notch attorneys—are able to manage the challenge of sharing relevant information without breaching the Clayton Act, Sherman Act, or unfair business practice laws. A lot of information sharing takes place among companies. For example, Century Link, one of the top Internet service providers (ISP), advised Congress that when it learns from third-party partners that customer computers are likely infected with malware that makes them part of a "botnet," it notifies customers and directs them to resources to help clean up the malware. It provides educational material, antivirus protection, firewalls, and parental controls. It works with stakeholders and industry partners on border gateway protocol (BGP) security to prevent accidental or malicious Internet route hacking.[68] Other industries engage in comparable information-sharing practices.

Large companies have the resources and sophistication to avoid illegal collusive activities, but smaller companies may lack that capacity. There is a solution, and Congress appears to recognize it. Narrowly drawn reforms can limit disclosure of risks, threats, vulnerabilities, and approaches to protection of information systems and personally identifiable information. That would enable information sharing and cyber security without undercutting a competitive marketplace.[69]

All three legislative proposals would have removed antitrust and FTC legal barriers to permit companies to monitor and defend information systems against cyber threats. Each allowed private companies to share cyber threat information,[70] and each prohibited the use of information shared to gain an unfair competitive advantage.[71]

Privacy and Confidentiality. Concerns that information sharing or disclosures may create legal liability for claims alleging breach of confidentiality or privacy are acute. These include potential claims for release of confidential information without prior consent. Information security—confidentiality, integrity, availability—is top of mind for many. Governments, the military, hospitals, and companies amass enormous amounts of information about employees, customers, products, and research and wish to protect it. Each proposal protects privileged or confidential trade secrets and commercial or financial transactions.

Still, industry experts argue that clear, fair, and predictable legal standards are lacking.[72] Ironically, all three bills pending before Congress contained safe harbors for information sharing about cyber security threats. SECURE IT offered the strongest. It exempted from civil and criminal liability private entities that use authorized countermeasures or cyber security systems; the "use, receipt or disclosure of any cyber threat information;" or "subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entities."[73] H. R. 3523 is similar but employed a good faith standard.[74] The CSA embraced a safe harbor, adding good faith as an absolute affirmative defense for sharing information about cyber threats, although as noted above, critics on the right and left found cause for concern with its information sharing provisions.[75]

The safe harbor provision within SECURE IT applied only to information actually related to cyber threats, as defined in the bill. The Rogers bill and the CSA are broader. They provided insulation for good faith disclosure of information[76]—language that is arguably an open invitation to litigation for violation of antitrust and the Electronic Communications Privacy

Act and the Stored Communications Act.[77] All bills protected against contrary state laws through a preemption rule.[78] All clearly intended a narrow exemption to remove obstacles currently posed by antitrust and unfair-business law for sharing cyber risks.

One step legislative sponsors might consider for the next Congress is to create a space on the Internet that invites iterative thinking, ideas, and suggestions from interested stakeholders. That may provide a useful forum to hammer out issues, critique different proposals, and forge solutions that address the real concerns legal barriers pose.

All three proposals sought to promote sharing classified and unclassified cyber security threat indicators with appropriate federal and non-federal entities, although they employ different procedures to achieve that result.[79] The bills sensibly made exemptions for disclosures from the Freedom of Information Act (FOIA), ensured that disclosures waive no legal privilege, permit ex parte communications, and prohibited the government from using disclosed information in a regulatory proceeding.

What about forced disclosure of information? The CSA purported to render it voluntary except to prevent imminent crimes.[80] Critics argued the bill actually requires mandatory, not voluntary disclosure, as companies escape legal liability under antitrust or other laws only if they share risk information with the government. Private sharing affords no safe harbor.

One disaster to avoid is an exemption—which the CSA included—for computer software and hardware.[81] If one adopts this approach to regulation, why exempt the Internet from cyber security requirements, given its well-disclosed vulnerabilities?[82] In March 2012, the DHS reported there were 86 reported attacks on computer systems in the United States that control critical infrastructure,[83] factories, and databases. Ghostnet and other incidents underscore Internet vulnerabilities.[84]

And as information sharing pertains to critical infrastructure, one must ask: What constitutes critical infrastructure? Who makes that determination? The CSA empowered the government—led generally by the DHS acting in tandem with other agencies, like the Federal Energy Regulatory Commission which regulates power companies, to make that determination. An asset, network, or system qualified if damage could cause interruption of life-sustaining services, catastrophic damages to the United States, or severe degradation of national security.[85] These categories are too broad, and if this approach is adopted, they must be more precise.

SECURE IT would require federal contractors to inform the government about cyber threats and make it easier for regulators and corporations to communicate about threats.[86] Both that bill and the one adopted by the House shared a philosophy rooted in the policy judgment that facilitating voluntary information sharing between the federal government and private parties—including easing antitrust laws that restrict information sharing between private companies and offering legal protections to companies that act proactively to protect their networks—would create a more secure cyber infrastructure and protect consumer privacy without creating a new bureaucracy. Senator McCain has stated, "The only government actions allowed by our bill are to get information voluntarily from the private sector and to share information back."[87] The policies that his proposal reflects are rooted in the view that the DoD, the NSA, and US Cyber Command have excellent capabilities that could be utilized for civilian networks. The Lieberman proponents preferred the DHS, and that policy issue lent itself to practical resolution. But they were never able to show convincingly why giving the DHS the lead made more sense.

While the expertise of our national security entities should be leveraged to promote public-private partnerships, security requirements may limit what can be shared, with whom, or under what circumstances. Close engagement, coordination, and cooperation are required on a case-by-case basis to address that issue. While seeking information or intelligence from the government or other parties, companies need to recognize—and take responsibility for—financial and legal risks they incur in operating vulnerable networks.[88]

Robust Private-Public Partnerships

The NIPP rests upon a risk-management framework of cooperation and coordination between the private and public sectors. That enables both sectors to set goals and objectives; identify assets, systems, and networks; assess risk based on consequences, vulnerabilities, and threats; establish priorities based on risk assessments and, increasingly, on return-on-investment for mitigating risk; implement protective programs and resiliency strategies; and measure effectiveness.[89]

Among the key issues that must be addressed in forging robust public-private partnerships are (1) joint planning, (2) creating incentives for in-

novative public-private partnerships, (3) resolving who defends private industry against cyber attack, (4) balancing cost sharing between public and private sectors, and (5) developing a viable approach that authorizes government to reasonably share classified information on cyber security.

Joint Planning

Advances in technology are accelerating the "network speed" at which incidents occur, and this pressures decision makers to act more quickly. Joint planning between government and industry strengthens the ability of each to anticipate looming threats and counter immediate risks.

How acute is this challenge? Defense Advanced Research Projects Agency (DARPA) deputy director Kaigham J. Gabriel has warned the House Armed Services Committee's Subcommittee on Emerging Threats and Capabilities that in today's threat environment, cyber security systems take too long to build and may become quickly obsolete. Once built, they merely set the stage for the next requirement. "Shelf-life of cyber security systems and capabilities," he declared, "is sometimes measured in days. Thus, to a greater degree than in other areas of defense, cyber security solutions require that we develop the ability to build quickly, at scale, and over a broad range of capabilities. This is true for offensive and defensive capabilities."[90]

The quality and nature of technology for cyber attack or cyber exploitation is expanding. "Computing, imaging, and communications capabilities that, as recently as 15 years ago, were the exclusive domain of military systems, are now in the hands of hundreds of millions of people around the world," Gabriel stated.[91] Nearly a dozen countries are producing electronic warfare systems. Many use mostly COTS technology. Decades ago a new system was produced every 10 years. Today, one is produced every year to year-and-a-half.[92] In testimony before Congress, Dr. James Miller pointed out that DoD acquisition processes require an average of 81 months to make new computing systems operational: "That means by the time they are fielded, they are already three to four generations behind the state of the art. We are working to get cycles of 12 to 36 months as opposed to 7 to 8 years."[93]

The military equips itself to protect its own assets, systems, and networks. Joint planning can help enable the defense industrial base to leverage that expertise in establishing a cohesive policy framework to forecast and meet challenges. Adopting this approach will force interested parties to

focus on key questions: What priorities should govern planning? Where should capital investment be focused? How should industry and the government, each of which bears responsibility for security, allocate costs and responsibilities? What are actionable requirements to make cyber infrastructure as secure as possible? Where do we acquire the knowledge vital to making informed judgments in answering those questions?

Smart planning for cyber security is an iterative process. It entails asking the right questions, developing information needed to ensure the right questions, and conducting progressive analysis through public-private engagement. From a public perspective, government can encourage business to invest in security measures that exceed their narrower business concerns. From a private perspective, industry may gain access to expertise it lacks, along with a greater comprehension of its own responsibilities. Too often industry expects government to do all of the heavy lifting for cyber security. Yet, the obligations flow both ways.

Industry is more supple in developing and testing new products. Industry better generates innovative ideas and cutting-edge solutions. Industry owns and operates most of the critical infrastructure, affording it a better understanding of CIKR assets, systems, networks, and facilities. It can move more quickly to reduce risk and respond to incidents. DARPA has recognized through programs like Cyber Fast Track (CFT), which taps into a pool of nontraditional experts, that smaller and medium-sized companies are leaders in innovative technology and has adjusted its funding accordingly. Over the last 12 months, it has made 32 awards to private companies—84 percent of them small companies and performers who have never done business with the government before.[94] Gabriel astutely noted that it is vital to expand "the number and diversity of talent contributing to the Nation's cyber security."[95] The philosophy embraces the far-sighted view of looking to companies that take risks to create new ideas in comparison to larger organizations that by emphasizing greater adherence to established procedures or protocols may prove less adept at creating new products. DARPA's philosophy rightly stresses collaboration between government and industry.

James Peery of the Sandia National Laboratories seconds that view. In 2012 he advised the Senate Armed Services Committee that the federal government needs a new strategy that coordinates investments across government and that taps into expertise offered by academia, government, private-sector, and military users.[96]

In the United States, the public and private sectors already work together in many ways. The DHS National Coordinating Center enables operational and collaborative partnerships. The Communications, Security, Reliability and Interoperability Council (CSRIC) provides an effective vehicle for providing recommendations to the FCC.[97] The FBI's Domestic Security Alliance Council (DSAC) is a strategic partnership between the FBI, DHS, and the private sector to ensure effective exchange of information to keep the nation's critical infrastructure safe, secure, and resilient.[98] The National Cyber-Forensics Training Alliance (NCFTA) serves as a conduit between private industry and law enforcement to fight cyber crime.

Malware pandemics, such as the Conficker computer worm, underscore the need. Conficker targeted Microsoft's Windows operating system. First detected in November 2008,[99] it exploited flaws in Windows software to co-opt machines and link them to a remotely controlled virtual computer—a botnet. Conficker generated strong cooperation among industry, academia, and government. Collaboration grew to more than 100 level-one domain operators and kept Microsoft in daily touch with the Internet Corporation for Assigned Names and Numbers (ICANN) and governments. It also exposed legal challenges. In some countries, contractual barriers and antitrust laws had to be addressed.[100]

Success proved elusive. Conficker's creators have neither been identified nor caught, although in June 2011, Ukraine authorities working with the FBI arrested 16 hackers in Kiev who used Conficker to seal $72 million from bank accounts.[101] Conficker is a warning to those who flinch from strong public-private collaboration. There was more success in fighting DNS (Domain Name System) changer malware, which enables criminals to control user DNS servers and thus what sites the user connects to on the Internet. Criminals could cause an unsuspecting user to connect to a fraudulent website or interfere with a user's online web browsing.[102] More than 4 million computers were infected. Industry provided critical insights into the information environment, helped identify infected computers, and offered remedial action. The FBI is developing evidence and is prosecuting six Estonian nationals arrested and charged after a two-year operation.[103]

The response to these threats underscores that public-private engagement can be effectively achieved, illuminating the path to defense against cyber attacks. It also supports notions of active defense—which remains ill-defined but should include preemptive action, carefully limited and permitted without a structured policy framework—and for offense. Neither

the United States nor other nations have released their offensive doctrine and/or descriptions of capability. What is clear is that the developing technology is providing the operational flexibility to maneuver in the cyber domain and to harmonize resources and capabilities within a coherent systematic strategy that permits the achievement of operational aims despite the opposition.

Forecasting the future can be a fool's errand. What we know is, as much as possible, we must look over the horizon. New technologies will produce new threats. These require evolutions in strategic thinking as well as technical and operational capabilities. Developing vital capabilities, tools, and weapons requires a joint effort between government and industry that capitalizes on the strengths of each.

Nothing underscores that more than the looming development of neuro-cyber weapons. New generations of these will enhance situational and strategic awareness, increasing the ability of humans to absorb, process, and project increasing volumes of data that could overwhelm individuals. Amplifying our ability to collect information and intelligence and properly analyze it will deepen situational and strategic awareness. Crises require humans to digest large volumes of data at a very high rate and to act on that data in a timely manner.[104] Some developments will be technical. Others entail revolutionary developments in medicine. Drugs like Ampakine CX717 may prevent harmful effects of sleep deprivation and enhance attention span and alertness.[105]

DARPA is developing cognitive technology that enables interactive monitoring to facilitate command and control of troops on the ground. These will help detect when an individual has physical limits to operate effectively or loses situational awareness. Robotic prostheses will replace body parts—enhancing capabilities to function in cyberspace—much as pacemakers or artificial legs now do so in medicine. Robotic orthotics will extend human performance.[106] These will improve cognitive skills through sensory substitution and enhancement. Next-generation computers will teach themselves, monitor information, and perform other tasks that augment the human brain. The trend is finding ways to expand distributed situational awareness by extending the human body, brain, and senses.[107]

These developments will enable the military to conduct cognitive hacking and both military and civilian entities to defend against it.[108] Tax incentives for private industry—which should not have to depend entirely upon entities like DARPA to support new technology, ideas, and

products—should be an integral element of strategic thinking. They will help forge cyber strategies for offense or defense that entail tactics such as creating deception, distraction, distrust, and confusion. These tools may be integrated into combined arms strategies to prevent, detect, or interdict cyber security challenges—and to pursue active defense or offensive strategies essential to national security. They can be used strategically or tactically for things like PSYOPS to create operational shock in cyberspace—a tactic that may be used to influence, recruit, intimidate, or surprise.[109]

Incentives for New Partnerships

The ability of the private and public sectors to leverage the strengths of one another to create both new spaces for creative thinking and to spur innovation affords a key incentive to promote these relationships. That synergy will produce better strategic thinking and strong policy frameworks. It will also—and this addresses the core of Kaigham's concern—increase the rate at which innovation takes place. New knowledge is produced every day. It remakes the world and reshapes the political and information environment and the cyber domain. It accentuates the importance of some things, while rendering others obsolete.[110]

DARPA has already recognized this challenge and is moving toward providing more grants to small and medium-size entrepreneurial companies who can meet that need. The DoD and the NSA need to become more flexible in easing access and clearances to companies and their employees to make possible exchange of information and the symbiotic partnerships that will enable public-private partnerships to flourish.

Yet, we should not rely upon DARPA or other government grants to spur innovation and new technology. Providing tax incentives for new technology, products, and innovation would spur development and make the investment of capital more worthwhile. Defining goals and offering appropriate prizes—financial and other—offers a different approach that could yield tangible results. Engagement between companies and the government to ascertain what can most strongly encourage companies to act proactively would be productive.

Where all of these developments will lead is tantalizing. The future offers opportunity and warning. The possibilities currently within our reach would have astounded populations and planners of earlier eras. Clarke's Third Law holds that any sufficiently advanced technology is indistinguishable from magic. Future developments may only seem like conjur-

ing, but the wonders that they hold will continue to astound. That is the perspective in which thinking about our cyber strategy needs to proceed. Collaboration and coordination that mobilizes and recruits the most imaginative talent from government and the private sector underscores the value of working together in developing joint policy frameworks and concrete action.

Who Defends Private Industry against Cyber Attack?

A joint policy framework is essential to forging a strategy to protect industry in real time against cyber attack or cyber exploitation. The challenge raises thorny issues. The DoD has made clear it will defend against attacks. More recently, it is embracing the notion of "active defense" to counter asymmetric threats. As William Lynn put it, "In this environment, a fortress mentality will not work. We cannot hide behind a Maginot line of firewalls . . . our defenses must be active."[111] He has noted that in cyber, milliseconds can make a difference. In that view, the Pentagon has embraced a defensive system with three overlapping lines of defense. Two, based on commercial best practices, are ordinary hygiene—keeping software up to date and firewalls up to date—and the use of intrusion-detection devices and monitoring software to establish a perimeter defense. The third is protecting critical infrastructure, including civilian infrastructure.[112]

That does not answer the question of what one means by an active defense or whether or how private critical infrastructure can mount it. Does it afford a right of hot pursuit? Does it embrace preemptive action? Who has, or should have, the authority to make decisions in mounting an active defense for national security incidents? The issue remains unresolved. One industry leader sees passive defense as reliance upon firewalls, intrusion-detection systems, and hygiene, while active defense means working "actively"—in concert with other parties to identify, intercept, and block attacks. That is a plausible explanation but represents a less aggressive view than that held by many who focus on defending military assets, networks, and systems.

The bottom line is: joint planning between government and industry is essential in thinking through who a company—a financial institution, utility, or other private party—can summon for help or what action it may legally or practically take to actively defend itself. The idea that companies should collect evidence and turn it over to proper law enforcement authorities may be useful down the road for prosecutions but

fails to answer the critical question of how, beyond passive defenses like firewalls, one stops an attack or whether preemptive activity is permissible—and if so, under what guidelines?

The Computer Fraud and Abuse Act makes it a felony to intentionally access a computer without authorization and cause damages of $5,000 or more.[113] A foreign attacker may not be able to capitalize on that, but the Justice Department's responsibility is to enforce the law as written. And what happens if the attack originates in the United States? Does that not compound the problem? Industry currently lacks legal guidance—and recourse—for countering a real-time attack.

A joint public-private policy framework, augmented by legislative reforms that authorize desired strategies, is vital as this nation forges viable strategies that protect, as much as possible, its critical cyber infrastructure.

Balancing Public and Private Interests in Allocating Costs and Sharing Information

Who should bear the cost of continuous upgrades to cyber security? How should such decisions be reached? The answer lies in balancing regulation and volunteerism as resources and interests vary. Larger firms focus on protecting physical, human, and cyber assets. They can more easily bear costs. That begs the question of what security standards should be satisfied or who should formulate them—industry or the government? Smaller companies face stiff challenges as capital requirements may be steep. No single formula applies across the board. A key challenge is, while private business owns 90 percent of critical infrastructure,[114] no USG department possesses the authority to compel companies to meet security performance requirements.

The balance requires information sharing, engagement among DIB partners, and trust.[115] There are competing views on how to surmount this challenge. The approach embraced by SECURE IT and the House bill argues that the market and corporate self-interest in keeping customers satisfied will force companies to take proper measures to voluntarily protect themselves.

No solution is perfect, but what is required is strong engagement and partnership between public and private parties, keyed to specific sectors within industry and the government, to strike a workable balance.

While demand for cyber expertise greatly exceeds the supply,[116] top-tier places like Sandia National Laboratory recruit aggressively. Sandia will

pay for a master's degree and support new recruits with 75 percent of their salary while they attend school fulltime in exchange for two years' service. There is intense competition for their knowledge and skills. Private companies often offer 50-percent higher salaries and benefits. So far, places like Sandia have been able to retain much of their workforce, and that is to everyone's benefit.[117]

The government offers a reservoir of talent, experience, and unique expertise. Places like Sandia offer innovative hands-on computer security programs, skill refreshing, and continuous learning. The government better understands countermeasures and best practices to address risks and vulnerabilities, and the private sector cannot match its intelligence-gathering capacity. All these actions benefit industry—which for its part bears the burden of taking active steps to protect its assets, systems, and networks. Melissa Hathaway offers a practical way forward in addressing this challenge: "DoD and the DNI have the authority to make the policy decision to declassify or 'write for release' to release vital information to a broader user community. That will greatly facilitate private-public information sharing and protection of critical infra-structure."[118]

A key challenge is enabling access to classified information among private-sector parties. The prevailing view would limit information sharing to individuals who possess appropriate security clearances, on a basis consistent with protecting national security. Congress is considering ways to enable cyber security providers, protected entities, or self-protected entities eligible for a clearance to obtain one if they show they are able to appropriately protect classified cyber threat intelligence. What is needed is for parties like the director of national intelligence or other responsible federal entities to work closely with private parties, flexibly taking into account private-sector innovation, corporate information sharing, and security best practices. Close engagement is required to establish realistic procedures that enable each side to access the expertise of the other. One way to achieve this may be to grant a temporary clearance for specific projects.[119]

Securing the Defense Industrial Base Supply Chain

The 2011 strategy recognizes that we have to manage supply chain risks. In protecting against supply chain vulnerabilities, the United States leans toward a combination of creating a secure pool of selected vendors and, for the broader commercial sector, identifying key assets and controls to assure

the integrity of products, testing to mitigate threats, and using trusted companies who use processes like those described in SAFECode.[120] This approach addresses various sources of risk: (1) supplier issues such as the ability to keep costs low and manage inventory levels, managerial and decision-making skills, and overall quality; (2) supply chain collaboration risks raised by supplier firms, logistics firms, and improper collaboration along the supply chain; or (3) uncontrollable events or natural disasters, legal liabilities, market price increases for raw materials, and technology changes.[121]

Employment of carefully selected and screened indigenous manufacturers for sensitive products is one step. There is a compelling reason for countries to build a series of verifiably secure computer and communication systems. Setting specific technical standards and requirements that products and components must meet is important. Yet, these represent partial solutions.

One must be realistic about capabilities. Managing the risk in assuring security in the cyber supply chain can be challenging for private companies. Many companies lack the resources to verify product security. Managing supply chain risk requires active joint, government, and private coordination, trust, and partnership with continuous, vigorous, informed engagement from both sides. No single formula will suit every aspect of the private sector or government. That mandates a flexible, adaptable approach.

At least five confluent strategies make conceptual sense. Yet, it bears stressing—extensive engagement between government and industry is vital. Each offers particular strengths and assets in implementing these strategies. It is possible to establish a finite number of absolutely secure installations. But for most installations, these mitigate but do not eliminate risk. Aspects of the first four have received wide comment:[122]

1. Ensure Transparency

We should work to ensure vendors who supply components or finished IT products provide transparency as to design, production, assembly, acquisition, quality control, assurance of a trusted workforce, record-keeping, traceability within the supply chain,[123] transportation, use of authentication technology, and their own security safeguards.

2. Maintain Continuous Monitoring

Companies or government departments or agencies need to continuously monitor vendors and products to ensure products are secure from

viruses, worms, or other vulnerabilities. Although this can be a logistical challenge, it is critical and will help ensure vendors institute proper safeguards. Conversely, government and commercial organizations need to develop and implement policies that prevent counterfeit parts from entering the supply chains.[124] The Department of Commerce and the Office of Technology Evaluation have offered recommendations to help ensure effective monitoring.[125]

3. Provide Incentives for Security

The private sector works well when presented with incentives to perform. While the threat not to do business provides any government or company with leverage to force vendors to ensure the security of their products, incentives tailored by different parties to vendors or products can pay off.

4. Establish a Database of Trusted Vendors

The United States and its partners should establish a database of vendors deemed trusted and reliable. The National Vulnerability Database provides and tracks vulnerability data for commonly used operating systems and applications, including open source, but it does not identify vendors.[126] It is vital to create fair, clear, and predictable rules and procedures for listing vendors and a workable procedure through which vendors denied a place can in a practical manner lodge an appeal and secure fair and impartial administrative adjudication. Collaterally, government agencies should have authority to refuse to deal with companies deemed unwilling or unable to counter supply-chain risk. Kathryn Stephens has sensibly recommended making the supply chain a part of the overall US cyber intelligence and cyber security strategy and setting up an organization that can handle reports of counterfeit products.[127]

5. Strengthen the Rules Governing the Committee on Foreign Investment in the United States (CFIUS)

Established in 1975 by Pres. Gerald Ford's Executive Order 11858, the CFIUS is an interagency committee of the USG that reviews the national security implications of foreign investments in US companies or operations. Chaired by the secretary of the treasury, it includes representatives from 16 departments and agencies. Companies involved in acquisitions by a foreign firm are supposed to voluntarily notify the CFIUS, but it can

initiate reviews on its own. It has looked at restrictions on the sale of advanced computers to a long list of foreign recipients, ranging from China to Iran.[128]

We need to strengthen the law requiring mandatory disclosure to the CFIUS of proposed foreign investments in technology companies by nations that the White House deems an "intelligence risk." The CFIUS should be required to investigate whether such acquisitions might compromise security.

The CFIUS has exerted its authority in cases involving Huawei Technologies, a mammoth Chinese telecommunications company that has been charged with engaging in corporate espionage against Western firms.[129] US security requirements mandate a more active role.

What nations cannot pirate directly may prompt them to seek access in more indirect ways—and potentially enable those deemed to be intelligence threats to covertly modify technology ostensibly owned by a US manufacturer. For example, China's aggressive strategy to ferret out and seize US technology as well as trade secrets is manifested in parallel ways. It stands accused of cyber piracy. Others point to different strategies that pose risks to US manufacturers—and by extension, to IT security.

Dr. Ron Hart, co-author of the Technology Transfer Act of 1986, advises many emerging technology companies and is recognized as one of the top clean-tech alternative energy analysts in the United States. He reports that in the last six months alone, Chinese emissaries have approached these companies with an offer to invest venture capital in exchange for a minority stake of 20 percent to 30 percent of the corporate valuation. The Chinese employ a greatly inflated valuation compared to normal American venture capital assessments as an inducement to accept the offer. The structure of the offer is always the same. The Chinese require two board seats as well as the right to manufacture and distribute products in the People's Republic of China. US companies such as Cisco and Motorola that have located their manufacturing facilities in China have found their technology pirated.[130] It is a clever strategy and works in tandem with cyber piracy.

Conclusion

We need to move expeditiously but smartly to minimize cyber risks and vulnerabilities to critical infrastructure for both government and in-

dustry. To strengthen cyber security, we must remove legislative obstacles, develop partnerships between public and private interests, and expertly manage global supply chain risks. Government can work with the private sector in ways that offer strong incentives for the private sector to protect its own interests and that of the nation. The challenges posed by state and nonstate actors create a real and present danger that must be confronted. The sooner the better. SSQ

Notes

1. "Statement of Gen Keith B. Alexander, commander, US Cyber Command, Hearing on National Defense Authorization Act for Fiscal Year 2012, Committee on Armed Services, US House of Representatives, 16 March 2011," 4, http://www.fas.org/irp/congress/2011_hr/cybercom.pdf.
2. Richard Weitz, "Global Insights: The DHS' Cybersecurity Logjam," *World Politics Review*, 10 April 2012, http://www.worldpoliticsreview.com/articles/11827/global-insights-the-dhs-cyber security-logjam.
3. Melissa E. Hathaway, telephone interview, 3 August 2012.
4. "Homeland Security Presidential Directive 7: Critical Infrastructure, Identification, Prioritization, and Protection," 17 December 2003, http://www.dhs.gov/homeland-security-presidential-directive-7.
5. Ibid.
6. *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency* (Washington: DHS, 2009), 4, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
7. Ibid., 2.
8. *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan* (Washington: DHS and DoD, May 2007), 3, http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf.
9. *National Infrastructure Protection Plan*, 1–6, well summarizes the plan.
10. *National Infrastructure Protection Plan*.
11. *Department of Defense Strategy for Operating in Cyberspace* (Washington: DoD, July 2011), http://www.defense.gov/news/d20110714cyber.pdf.
12. *NATO 2020: Assured Security; Dynamic Engagement—Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*, 11, 14, 20 (Brussels: NATO, 17 May 2010), http://www.nato.int/strategic-concept/expertsreport.pdf.
13. Dan Auerbach and Lee Tien, "Dangerously Vague Cybersecurity Legislation Threatens Civil Liberties," *Electronic Frontier Foundation*, 20 March 2012, https://www.eff.org/deeplinks/2012/03/dangerously-vague-cybersecurity-legislation.
14. "Testimony of David Mahon, Vice President and Chief Security Officer, Century Links, Inc., before the Subcommittee on Communications and Internet Committee on Energy and Commerce, U.S. House of Representatives, March 7, 2012," 1, HHRG-112-IF16-Wstate-DMahon-20120307.pdf.
15. John Hagel III, John Seely Brown, and Lang Division, *The Power of Pull* (New York: Basic Books, 2010), 31.
16. William J. Lynn III, "Remarks on Cyber at RSA Conference," 15 February 2011, http://www.defense.gov/speeches/speech.aspx?speechid=1535.
17. The Russian Federation denies state complicity, although many suspect it acted through proxies.

18. James Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy* 53, no. 1 (February–March 2011): 23–40, http://www.iiss.org/publications/survival/survival-2011/year-2011-issue-1/stuxnet-and-the-future-of-cyber-war/.

19. Only 60 percent of Stuxnet infections affected Iranian facilities. Ibid.

20. See James Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival: Global Politics and Strategy* 54, no. 12 (August–September 2012): 107–20.

21. Ibid.

22. Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, a report prepared for the US-China Economic and Security Review Commission (Washington: Northrop Grumman Corp., 7 March 2012, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.

23. Ibid., 13.

24. Sydney J. Freedberg Jr., "They're Here: Cyber Experts Warn Senate that Adversary is Already inside U.S. Networks," *AOL Defense*, 21 March 2012, http://defense.aol.com/2012/03/21/they-re-here-cyber-experts-warn-senate-that-adversary-is-alread/.

25. William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no.5 (September/October 2010): 97–108, https://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain; and Sharon Weinberger, "Pentagon Official Says Flash Drive Used in Classified Attack," *AOL News*, 25 August 2010, http://www.aolnews.com/2010/08/25/pentagon-official-says-flash-drive-used-in-classified-cyberattac/. See also Kim Zetter, "The Return of the Worm that Ate the Pentagon," *Wired*, 9 December 2011, http://www.wired.com/dangerroom/tag/operation-buckshot-yankee/.

26. "Operation Buckshot Yankee: Key Players and Networks Infected," *Washington Post*, 8 December 2011, http://www.washingtonpost.com/world/national-security/key-players-in-operation-buckshot-yankee/2011/12/08/gIQASJaSgO_story.html; and Zetter, "Return of the Worm."

27. David Alexander, "Pentagon Tries to Lean Forward in Cyberdefense," *Aviation Week*, 14 July 2011.

28. Lynn, "Defending a New Domain," 1.

29. Weinberger, "Pentagon Official Says Flash Drive Used."

30. Rob Rosenberger, "Gov't Hype Surrounds 'Operation Buckshot Yankee,'" *Vmyths*, 26 August 2010, http://vmyths.com/2010/08/26/oby/.

31. "Solar Sunrise," *GlobalSecurity.org*, 7 May 2011, http://www.globalsecurity.org/military/ops/solar-sunrise.htm.

32. Smith received a 20-month prison sentence and a $5,000 fine. Linda Rosencrance, "Melissa Virus Author Sentenced," *PC World*, 1 May 2002.

33. Ibid.

34. Michael Arrington, "Google Defends against Large Scale Chinese Cyber Attack: May Cease Chinese Operations," *Techcrunch.com*, 12 January 2010, http://techcrunch.com/2010/01/12/google-china-attacks/.

35. Robin Sidel, "Card Processor: Hackers Stole Account Numbers," *Wall Street Journal*, 1 April 2012, http://professional.wsj.com/article/SB10001424052702304750404577318083097652936.html?mod=WSJPRO_hpp_LEFTTopStories.

36. Michael Hickins, "The Morning Download: 'Prepare Yourself to be Penetrated,'" *CIO Journal*, 2 April 2012, http://blogs.wsj.com/cio/2012/04/02/the-morning-download-prepare-yourself-to-be-penetrated/?KEYWORDS=cybersecurity.

37. Devlin Barrett, "U.S. Outgunned in Hacker War," *Wall Street Journal*, 28 March 2012, http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html?KEYWORDS=cybersecurity.

38. Michael Balboni, "Halt, Who Hacks There?" *Newsday*, 27 January 2012.

39. Ibid.

40. Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, 8 April 2009, http://online.wsj.com/article/SB123914805204099085.html. The article stated the intrusions were detected by US intelligence agencies, who said water, sewage, and other infrastructure systems were also at risk.

41. Ibid.

42. James Jay Carafano, *Wiki at War: Conflict in a Socially Networked World* (College Station: Texas A&M University Press, 2011), 9.

43. Jose Antonio Vargas, "The Face of Facebook," *New Yorker*, 20 September 2010, http://www.newyorker.com/reporting/2010/09/20/100920fa_fact_vargas.

44. Steve Bertoni, "Sean Parker: Agent of Disruption," *Forbes*, 21 September 2011, http://www.forbes.com/sites/stevenbertoni/2011/09/21/sean-parker-agent-of-disruption/4/.

45. Paul Festa and Joe Wilcox, "Experts Estimate Damages in the Billions for Bug," *CNET*, 5 May 2000, http://news.cnet.com/2100-1001-240112.html.

46. Eric Warner, "Global Cyber Supply Chain Management," *Microsoft Security Blog*, 26 July 2011, http://blogs.technet.com/b/security/archive/2011/07/26/global-cyber-supply-chain-management.aspx.

47. "Testimony of Dr. James Peery, Director of the Information Systems and Analysis Center, Sandia National Laboratories, Senate Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, 20 March 2012," 7.

48. Barrett, "U.S. Outgunned in Hacker War."

49. Jim Finkle and Andrea Shalal-Esa, "Exclusive: Hackers Breached U.S. Defense Contractors," *Reuters*, 27 May 2011, http://www.reuters.com/article/2011/05/27/us-usa-defense-hackers-idUSTRE74Q6VY20110527; and Christopher Drew and John Markoff, "Lockheed Strengthens Network Security after Hacker Attack," *New York Times*, 29 May 2011, http://www.nytimes.com/2011/05/30/business/30hack.html.

50. Drew and Markoff, "Lockheed Strengthens Network Security."

51. Arthur W. Coviello Jr. (executive chairman, RSA), "Open Letter to RSA Customers," http://www.rsa.com/node.aspx?id=3872.

52. Jaikumar Vijayan, "Caution Urged in Wake of RSA Security Breach," *Computerworld*, 19 March 2011, http://www.computerworld.com/s/article/9214800/Caution_urged_in_wake_of_RSA_security_breach?taxonomyId=203&pageNumber=2.

53. Andrew Kemshall, "The RSA Security Breach—12 Months down the Technology Turnpike," *Huffington Post*, 14 March 2012, http://www.huffingtonpost.co.uk/andrew-kemshall/the-rsa-security-breach-1_b_1344643.html.

54. EMC Corporation SEC Form 8-K, dated 17 March 2011, http://www.sec.gov/Archives/edgar/data/790070/000119312511070159/d8k.htm.

55. Hathaway, interview.

56. Siobhan Gorman, "Cybersecurity Bills Duel over Rules for Firms," *Wall Street Journal*, 9 March 2012, http://online.wsj.com/article/SB10001424052970203961204577269832774110556.html?KEYWORDS=cybersecurity.

57. Permanent Select Committee on Intelligence, "Committee Statement and Views," reporting on H.R. 3523, Cyber Intelligence Sharing and Protection Act, 5, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HR3523CommitteeReport.pdf.

58. S 415, "Spectrum Optimization Act," 17 February 2011, http://www.gpo.gov/fdsys/pkg/BILLS-112s415is/pdf/BILLS-112s415is.pdf.

59. H.R. 4263, "Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012," 27 March 2012, http://www.gpo.gov/fdsys/pkg/BILLS-112hr4263ih/pdf/BILLS-112hr4263ih.pdf. Representatives Mary Bono Mack and Marsha Blackburn introduced SECURE IT in the House.

60. S 415. For an excellent summary in layman's terms, see Stephen M. Spina and J. Daniel Skees, "Cybersecurity Act of 2012 Introduced," *National Law Review*, 21 February 2012, http://www.natlawreview.com/article/cybersecurity-act-2012-introduced.

61. Zach Walton, "Cybersecurity Act of 2012 Killed in the Senate," *WebProNews*, 2 August 2012, http://www.webpronews.com/cybersecurity-act-of-2012-killed-by-the-senate-2012-08; and The Revised Cybersecurity Act of 2012, S 3414, Summary: "This bill creates a 'public-private partnership' with private sector developed voluntary standards."

62. Mark M. Jaycox, "The Cybersecurity Act Was a Surveillance Bill in Disguise," *Guardian*, 2 August 2012, http://www.guardian.co.uk/commentisfree/2012/aug/02/cybersecurity-act-surveillance-bill-disguise; and Andrew Couts, "Senate Kills Cybersecurity Act of 2012," *Digital Trends*, 2 August 2012, http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/?utm_source=twitterfeed&utm_medium=twitter. The American Civil Liberties Union, however, supported the amended proposal because it included protections against passing private information to the National Security Agency or the military.

63. H.R. 3523, amending the National Security Act of 1947 (50 U.S.C. 442 et seq), http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523eh/pdf/BILLS-112hr3523eh.pdf.

64. The committee report on H.R. 3523 notes that while the bill does not define "private sector," it includes public, private, and quasi-public utilities that provide power, water, gas, and other critical services.

65. H.R. 3523, § 1104(b), pg. 6, line 11. The definitions sections of H.R. 3523 as passed are also subject to criticism as less than those contained in SECURE IT.

66. See Sherman Antitrust Act (Sherman Act), 15 U.S.C.A. 1-7, as amended by the Clayton Anti-Trust Act of 1914, 15 U.S.C. 12 et seq, notably § 1(a); the Federal Trade Commission Act of 1914, 15 U.S.C.A. 45 et seq, notably § 5 that applies to unfair methods of competition. The Sherman Act prohibits business activities that reduce competition in the marketplace and requires the federal government to investigate and pursue trust, companies, and organizations it suspects may violate the act. It makes illegal contracts, combinations in the form of trust or otherwise, or conspiracy in restraint of trade or commerce. The FTC Act authorizes the commission to enforce the antitrust laws.

67. 18 U.S.C. 2510, et seq; and 18 U.S.C. 2701-12. This legislation deals with protecting the privacy of stored electronic communications. The Uniting and Strengthening America by Promoting Appropriate Tools Required to Intercept and Obstruct Terrorism—the USA PATRIOT Act, 18 U.S.C.A. 1 (Pub. L. 107-56, 107th Cong.) et seq, arguably weakened some provisions of the ECPA.

68. "Testimony of David Mahon," 2.

69. See Paul Rosenzweig, "Senate Cybersecurity Bill: Not Ready for Prime Time," *Heritage Foundation*, 7 March 2012, http://www.heritage.org/research/reports/2012/03/senate-cybersecurity-bill-not-ready-for-prime-time. Though critical of the proposed legislative, in his excellent assessment of Senator Joe Lieberman's bill, Rosenzweig agrees that provisions that enhance information sharing with other private-sector actors without fear of being prosecuted are a "solid improvement over current law." This author concurs with that view.

70. S 415, Title VII, § 701 et al.; H.R. 4263, Title 1, § 102; and H.R. 3523, § 1104 (b)(2).

71. S 415, § 702(b)(3); and H.R. 4263, §102.

72. The author conducted off-the-record interviews with attorneys who specialize in this challenge.

73. SECURE IT, § 102(g).

74. H.R. 3523, § 1104(b)(4), 9.

75. S 415, § 706.

76. Ibid.; H.R. 4263, § 102 (g); and H.R. 3523, § 701(b)(3).

77. 18 U.S.C. 2510, et seq; and 18 U.S.C. 2701-12. This legislation deals with protecting the privacy of stored electronic communications. The Patriot Act arguably weakened some provisions of the ECPA.

78. S 415, § 707; H.R. 4263, § 102 (f); and H.R. 3523, § 701(e).

79. S 415, § 703(a); H.R. 4263, §§ 101 et al.; and H.R. 3523, § 1104(a).

80. H.R. 3523, § 704.

81. S 415, § 103(b)(2) and § 104(b)(2).

82. The problem is irrelevant to the other two bills, neither of which sets up a comprehensive regulatory scheme.

83. "Computer Security," *New York Times*, 27 April 2012, http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_security/index.html.

84. See "Computer Security," *New York Times*, 14 March 2012, http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_security/index.html; "Tracking Ghostnet," *Information Warfare Monitor*, 29 March 2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-NetworkidUSL2E8EGGI320120316; "Shadows in the Cloud," *Information Warfare Monitor*, 6 April 2010, http://www.nartv.org/mirror/shadows-in-the-cloud.pdf; and Joseph Menn, "Microsoft Says Hacking Code Could Have Leaked," *Reuters*, 16 March 2012, http://www.reuters.com/article/2012/03/16/microsoftsecurity-commerce.senate.gov/public/?a=Files.Serve&File_id=e1244f6d-24ac-44b0-872e-61e1ce6509e6. See also Dian Bartz, "SECURE IT Act: Senate Republicans Introduce Softer Cybersecurity Bill," *Huffington Post*, 1 March 2012, http://www.huffingtonpost.com/2012/03/01/secure-it-act_n_1314213.html. SECURE IT would also reform federal cyber security standards.

85. S 415, Title I, § 103(a).

86. Text of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology Act of 2012, or SECURE IT.

87. See comments of Cong. Marsha Blackburn quoted in Amber Corrin, "House Republicans Issue Answer to Senate Cybersecurity Bills," *Federal Computer Week*, 1 March 2012, http://fcw.com/articles/2012/03/01/republican-cybersecurity-bill-secure-it-act.aspx.

88. Barrett, "U.S. Outgunned in Hacker War," remarks of Shawn Henry.

89. Ibid., 4.

90. "Testimony of Dr. Kaigham J. Gabriel, House Armed Service Committee, Subcommittee on Emerging Threats and Capabilities," 29 February 2012, 8.

91. Ibid., 7.

92. Ibid., 6.

93. "Statement of Dr. James N. Miller, Principal Deputy Undersecretary of Defense for Policy, U.S. Department of Defense, Hearing on National Defense Authorization Act for Fiscal Year 2012, Committee on Armed Services, U.S. House of Representatives," 16 March 2011, 4, http://www.fas.org/irp/congress/2011_hr/cybercom.pdf.

94. "What Keeps DARPA Leadership up at Night: Gabriel Testifies before House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities," DARPA news release, 29 February, 2012, http://www.darpa.mil/NewsEvents/Releases/2012/02/29a.aspx.

95. "Testimony of Dr. Kaigham J. Gabriel," 9.

96. "Testimony of Dr. James Peery."

97. See "Communications Security, Reliability and Interoperability Council III," *FCC Encyclopedia*, http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii.

98. See Domestic Security Alliance Council homepage, http://www.dsac.gov/Pages/index.aspx.

99. John Markoff, "Defying Experts, Rogue Computer Code Still Lurks," *New York Times*, 26 August 2009, http://www.nytimes.com/2009/08/27/technology/27compute.html?_r=1. It could be used to generate spam, steal passwords and logins, deliver fake antivirus warnings, and trick people into paying by credit card to have the infection removed. Ibid. See also Mark Bowden, *Worm* (Washington: Atlantic Monthly Press, 2011), which takes an in-depth look at the incident.

100. See Roger Hurwitz et al., "A Preliminary Report on the Cyber Norms Workshop," Center for Global Security Affairs, University of Toronto, 9, http://www.citizenlab.org/cybernorms/preliminary_report.pdf. This discussion of the Conficker challenge and how it was addressed is taken from their report.

101. Bowden, *Worm*, 231.

102. See "DNS Changer Malware," FBI, http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf.

103. Melanie Hick, "DNS Changer Virus Spells 'Internet Doomsday,'" *Huffington Post UK*, 25 April 2012, http://www.huffingtonpost.co.uk/2012/04/25/dns-changer-virus-internet-doomsday_n_1451606.html.

104. See Jurgo-Soren Preden, "Enhancing Situation-Awareness, Cognition, and Reasoning of Ad-Hoc Network Agents" (PhD diss., Tallinn University of Technology, 2010), 46.

105. Jonathan Y. Huang and Margaret E. Kosal, "The Security Impact of the Neurosciences," *the bulletin.org*, http://www.thebulletin.org/web-edition/features/the-security-impact-of-the-neurosciences.

106. See Jonathan D. Moreno, *Mind Wars: Brain Research and National Defense* (New York: Dana Press, 2006), which focuses on the future in neuro-cyber weapons.

107. Preden, "Enhancing Situation-Awareness, 50.

108. See Preethi Vinayak Ponangi, "Cognitive Cyber Weapon Selection Tool Empirical Evaluation," Wright State University, 2007, 19.

109. See James Farwell, "PSYOP: A Tool for Administering Operational Shock in Cyber Space," *Perspectives* 22, nos. 1 and 2, (2012).

110. See, e.g., Hagel, Brown, and Division, *Power of Pull*, 134.

111. William J. Lynn, "Remarks on Cyber at the Council on Foreign Relations," 30 September 2010, http://www.defense.gov/speeches/speech.aspx?speechid=1509.

112. Ibid. Lynn also noted that collective defense with allies is a fourth strategy.

113. 18 U.S.C. 1030.

114. Richard Weitz, "Global Insights: The DHS' Cybersecurity Logjam," *World Politics Review*, 10 April 2012.

115. *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2009* (Washington: DHS, 2009).

116. Eric Chabrow, "Damn the Economy! IT Employment Rises to New Heights," *CIO Insight*, 1 July 2008, http://www.cioinsight.com/c/a/Trends/Damn-the-Economy-IT-Employment-Rises-to-New-Heights/.

117. "Testimony of Dr. James Peery," 8. Dr. Peery has asked Congress to support a Scholarship for Service Program that would strengthen the government's ability to recruit and retain top students.

118. Hathaway, interview.

119. See, e.g., "Committee Report on H.R. 3523, Permanent Select Committee on Intelligence," Report 112-445, 112th Cong., 2d sess., 8–9, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HR3523CommitteeReport.pdf.

120. See, e.g., Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain (Wakefield, MA: SAFECode, 2010); *The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain* (Wakefield: SAFECode, 2009); and Scott Charney and Eric T. Werner, "Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust," *Microsoft.com*, 25 July 2011, http://www.microsoft.com/en-us/download/details.aspx?id=26826.

121. Sandor Boyson, Thomas Corsi, and Hart Rossman, "Building a Cyber Supply Chain Assurance Reference Model," SAIC/Robert H. Smith School of Business, http://www.slamtheonlinescam.com/pdf/Cyber-Supply-Chain-Assurance.pdf.

122. See, e.g., Kathryn Stephens, "Cyber Supply Chain," NASCI white paper, 18 November 2010, http://www.nsci-va.org/WhitePapers/2010-11-18-Cyber%20Supply%20Chain%20Whitepaper-Stephens.pdf; Boyson, Corsi, and Rossman, "Building a Cyber Supply Chain"; Charney and Werner, "Cyber Supply Chain Risk Management"; and "Cyber Threats to National Security."

123. See Stephens, "Cyber Supply Chain."

124. Mark Crawford et al., *Defense Industrial Base Assessment: Counterfeit Electronics* (Washington: Department of Commerce, 2010), http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf. See also Stephens, "Cyber Supply Chain."

125. See Crawford et al., *Defense Industrial Base Assessment*.

126. "National Vulnerability Database Version 2.2," DHS/National Institute of Standards in Technology (NIST), http://nvd.nist.gov/.

127. Stephens, "Cyber Supply Chain." Her insightful analysis also recommends building a limited number of absolutely secure systems, creating a federal database of counterfeit products and suppliers, utilizing the General Services Administration to provide market incentives to provide security in hardware and software designs and the NIST to provide input. The NIST has recommended a risk management framework. See John Sankovich, "Cybersecurity: Continuous Monitoring Action Plan," *Information Week*, February 2011.

128. See, e.g., Wayne Rash, "Suppose IBM-Lenovo Deal Doesn't Happen," *eWeek.com*, 24 January 2005: http://www.eweek.com/c/a/Desktops-and-Notebooks/Suppose-IBMLenovo-Deal-Doesnt-Happen/.

129. See Michael Smith, "Spy chiefs fear Chinese cyber attack," *Sunday Times*, 29 March 2009; Jeffrey Carr, "China's Silent Cyber Takeover?" *Diplomat*, 17 April 2011, http://the-diplomat.com/flashpoints-blog/2011/04/17/chinas-silent-cyber-takeover/; and John Tkacik Jr., "Trojan Dragon: China's Cyber Threat," Heritage Foundation backgrounder 2106, 8 February 2008, http://www.heritage.org/research/reports/2008/02/trojan-dragon-ch.inas-cyber-threat.

130. Dr. Ron Hart, interview by author.

Crisis Management and the Anti-Access/Area Denial Problem

Vincent Alcazar, Colonel, USAF

America's political and military leaders rely on unimpeded US force movements across strategic distances to stabilize regions and deter threatening regimes. That reliance depends on assured air and naval superiority as a precondition. US leaders assume that with air and naval superiority during wartime, the United States can secure its interests and attain its objectives through robust military intelligence, logistics, maneuver, and firepower. But the rise of anti-access (A2) and area denial (AD) strategies and capabilities poses a problem for US foreign policy: A2/AD thwarts US ability to project power and force on its own terms. By using an A2/AD strategy, regional adversaries are able to contest US power projection and presence. This strategy and capability allows adversaries to oppose the United States across its operational and strategic depth.

When Pres. Barack Obama and Secretary of Defense Leon Panetta unveiled the new DoD strategic guidance, *Sustaining US Global Leadership: Priorities For The 21st Century Defense*, on 3 January 2012, Secretary Panetta wrote in his introduction, "this country is at a strategic turning point after a decade of war and, therefore, we are shaping a Joint Force for the future that will be smaller and leaner, but will be agile, flexible, ready, and technologically advanced."[1] Additionally, "it [joint force] will have cutting edge capabilities, exploiting our technological, joint, and networked advantage." The document referenced the challenges to US power projection by A2/AD and identified competitors to US power projection. Specifically, China and Iran were cited as "[pursuing] asymmetric means to counter our power projection capabilities, while the proliferation of sophisticated weapons and technology will extend to nonstate actors as well."[2] The A2/AD verbiage in the document indicates what must be done: the United States must have

---

Col Vincent Alcazar was the founding lead of the Air-Sea Battle concept development group at Headquarters Air Force. He served as the Air Force subject matter expert and service author developing the Joint Operational Access Concept for the chairman of the Joint Chiefs of Staff. He is currently the air attaché–designate to Iraq.

The author would like to thank Maj Robert Murray and Maj Jeremy Olson for their contributions to the development of this article.

assured methods of projecting military force where presence of that force will be contested.[3] The DoD strategic guidance document also discussed the recently completed Joint Operational Access Concept (JOAC).[4] While the JOAC addresses how US forces must be able to enter highly contested places, it is not a conceptual design that promotes strategic theories for shaping and deterring A2/AD adversaries.[5]

Without a better understanding of the A2/AD problem and new ideas to assure its power and force projection, the United States will gradually lose its ability to shape regions and deter A2/AD adversaries. The A2/AD challenge demands an offsetting strategy, a retooling of US power and force projection concepts, and an examination of the ways US power projection can shape A2/AD crisis management. This article presents the concept of A2/AD, including the nature of the problem, and amplifies the A2/AD strategy. It then offers a new crisis management design framework, followed by planning considerations for the future of A2/AD.

The terms in figure 1 make the case for an applied design concept to better manage crises in A2/AD settings. They imply the notion of the "A2/AD portfolio"—an adversary's all-of-their-government method of undermining regional stabilization that also blunts US projection of power and force. The US "offsetting strategy" refers to a multilinear whole-of-government method geared to overcome the resistance and effects of a rival's A2/AD strategy.

* **Anti-Access (A2):** adversary capabilities, actions which impede (preclude, prevent, mitigate) the movement of US forces to their desired locations (war-fighting positions, staging locations, etc.).

* **Area Denial (AD):** adversary capabilities which impeded the free movement of US forces within the employment envelopes of maximum effectiveness, efficiency, or advantage to US forces.

† **Linear Strategy:** conduct of operations with identified forward line of troops; rear area security implied from logistics areas and fighting forces; useful when outnumbered or forces lack the information needed for nonlinear operations.

† **Nonlinear Strategy:** a focus on objectives without geographic references to adjacent forces; emphasis is on delivering effects on multiple decisive points. Requires high situational awareness and use of precision fires.

‡ **Multilinear Strategy:** an amagamated linear/nonlinear approach across all five war-fighting domains; assumes ability to integrate all kinetic/nonkinetic forces in a cross-domain operations approach to create more effects paths, options.

* Undefined in JP1–02; see JOAC for related definitions.
† Undefined in JP 1–02; see operational discussion, JP 3–0, pgs V–51 to V–53.
‡ Based on theoretical discussion initiated by LTC Christopher Paparone, US Army ALOG, Nov–Dec 1996.

Figure 1. A2/AD definitions and concepts

The primary benefit of this design concept for crisis management is to ensure the United States can continue to use assured military presence and whole-of-government synchronized effort to strengthen its influence in key regions. Other benefits include improved understanding and specified design that allow the United States to better shape a crisis with an A2/AD adversary; or alternatively, better position its entry into conflict against an A2/AD threat. There are three premises which underlie this concept for crisis management: (1) the nature of war does not change, but the character of war does change from era to era,[6] (2) the United States will need fresh theories and concepts of shaping, deterring, and war fighting less tethered to its traditions of annihilation warfare, and (3) A2/AD will multiply US force attrition, erode its conventional deterrence, and undercut its ability to manage escalation and deescalation.

A2 and AD: The Problem and Its Nature

Understanding of anti-access and area denial is not common across the US military establishment. Within the armed forces are generations of war fighters who know only warfare in permissive operations where the United States has the initiative—not the conditions caused by A2/AD. Moreover, to the extent A2/AD appears in US defense writings, there is a frantic focus on systems versus systems rather than strategies for success. At the tactical level, the impact of these and other A2/AD capabilities is and will remain important. However, at the strategic and operational levels of war, the mural which depicts how A2/AD jeopardizes US projection of power and force is incomplete.

The A2/AD concept describes but does not explain the training, organizing, and equipping activities observed in four potential adversaries: the People's Republic of China (PRC), Iran, Russia, and North Korea. A2/AD consists of a regional strategy with tactical-to-strategic effects designed to preclude the United States from reinforcing its conventional power—its over-the-horizon mobilized forces. How far away from a given region an A2/AD adversary will oppose US forces and what form that opposition takes will depend on adversary capabilities and will. However, the diffusion of defense technologies is enabling A2/AD adversaries to develop weapon systems of greater reach, immediacy, and accuracy, such as cyberspace global reach at the speed of light, offensive counterspace technologies, and long-range surface-to-air missiles. To a force that intends to

deter, counter, or defeat an adversary's defenses, A2/AD can be thought of as a grand military porcupine.

Therefore, to US policymakers, military leaders, and campaign planners, A2/AD is a *wicked* problem.[7] A2/AD strategies are not self-referential; their character is not fully explained by their existence. It is a nonlinear opposing strategy that leverages diplomatic, information, military, and economic (DIME) activities. A2/AD unfolds in peace, crisis, and war to gradually erode confidence in the perceived ability of US forces to *project* strategic strength and stability. It is an expression of the uniqueness or difficulty in attaining comprehension of the underlying nature, structure, and organization of a given military problem.[8] While each of the four potential A2/AD adversarial regimes has substantive ideological differences, those differences take a backseat to the commonality of A2/AD military effects. At the micro level, an advanced missile is still a missile to be defeated. At the macro threshold, their similarity is, they seek to carve out their respective regional spheres of influence by bringing to bear military capabilities across all operating domains to control strategically valuable places and spaces.

Interestingly, A2/AD is not explicitly mentioned as a doctrinal term in known PRC military literature; however, the intent of preclusion and preemption can be found in the PRC's "three warfares" concept.[9] This concept refers to an ongoing effort by the PRC to use the media, psychological messaging, and illegal actions to promote the expansion of Chinese authority.[10] It is not known if Russia's contemporary organizing doctrine is explicitly built on A2/AD, but indications in recent years suggest it has a good grasp of A2/AD. First are the alleged links between the massive cyberspace denial of service attacks in Estonia during 2007 that originated from within Russia without apparent strenuous objection or intervention by the Russian government.[11] Second, during Russia's 2009 military incursion into Georgia, Russian cyber effects were used to degrade the functions of the Georgian government and posture of its armed forces.[12] Meanwhile, the PRC and Iran are building vast ballistic and cruise missile inventories that are significantly out of proportion to the scale of any postulated regional threat.[13]

The strategic effects of A2/AD produce challenges to the United States in three broad areas: inadequate access, curtailed freedom of action, and eroded influence. Inadequate access may result from choices US allies and friends feel compelled to make to avoid facing retribution or retaliation

from a regional hegemon. Feeling compelled to choose between a future with a belligerent neighborhood threat and a United States whose interest might wane, current friends may see no choice but to appease the A2/AD rival. Appeasement could take the form of curtailing air and naval port access or prohibiting overflight, thus weakening the deterrent abilities of US forces in peacetime. It could also stymie US ability to effectively manage a crisis or prosecute a conflict over great distance.

Curtailed freedom of action is another important A2/AD strategic effect. It is important that US forward-based forces operate throughout and across vital regions to effectively shape conditions and deter hostile actors. AD measures such as hostile diplomacy, contrary media operations, and numerous offensive and defensive systems can inhibit US effectiveness. To one degree or another, all four A2/AD rivals develop and deploy large missile forces for asymmetric advantage. Indeed, the Chinese are going one step farther by expanding their air force and coupling it with immense army missile forces to create a formidable regional air defense.[14] Chinese international territorial disputes in the South China Sea and elsewhere have provoked naval force buildups by governments along Asia's southern and eastern periphery so that these states can better protect their sovereign interests.[15]

Russia's reinforcement of military capabilities adjacent to its European near abroad, force modernization, and military reorganization all suggest an adversary reinventing its approach to asserting itself.[16] Though a much smaller military since the Cold War, Russia's advanced surface-to-air missile systems, advanced fighter aircraft programs, extensive cyberspace capabilities, and WMD inventory make it a formidable A2/AD adversary. Meanwhile, Iran's ongoing missile force buildup and aggressive posture holds at risk a growing number of Persian Gulf states. Iran is able to disrupt international shipping that can jeopardize the transit of petroleum through the Strait of Hormuz and northern Arabian Sea.[17] If it succeeds in developing a nuclear weapon, the region's security and stability contours will be significantly altered, producing yet more complexity and volatility. In this sense, Iran's A2/AD strategy could be used both as a tool to erode US regional power and a shield behind which to continue a domestic nuclear weapons program with little concern for accountability to the international community.

Weakened US influence and assured defense are concerns for allies in areas with an A2/AD adversary. If they perceive US regional influence is waning or fragile, they may decide to create different alliances or continue

their US partnership on different terms. If the United States does not oppose A2/AD with an offsetting strategy composed of coherent regional approaches, it risks sending the wrong signal for regional stability. Additionally, weakened US overseas influence presents more difficulties in defending its vital interests in areas with an A2/AD adversary. If the United States cannot protect its vital interests against an A2/AD competitor, it risks ceding control of these interests to opposing, illiberal ideologies.

A2/AD strategies undercut the US preferred union of power and force projection by preempting or precluding force options. Suffering blunted or attenuated projection of forces decreases the relevance of US power. Further, the defense logistics enterprise—the engine of force projection—will most assuredly be the focus of extensive cyber attack. Not only do cyber attacks on its logistics enterprise mean US forces deploy forward at decreased rates of movement, but once forward, their range of operations will be diminished and restricted.

Whether the United States would be deterred by the prospects of war against an A2/AD adversary with the ability to eliminate theater safe areas, interdict US marshaling areas, disrupt US information networks, or promote fear of extreme cost is an absorbing topic for war-game inquiry. However, if A2/AD rivals can effectively use their multilinear strategies as templates of coercion, the result will be destabilized regions where control is tilted away from the United States and its allies. The resultant instability could enhance the likelihood of strategic miscalculation while inflating and emboldening the rival's sense of strength. If the United States cannot preserve a sufficient range of force options against an A2/AD threat, it cannot adequately mitigate the rival's actions. In essence, an adversary's strategic goals become foregone conclusions and its military campaigns a fait accompli. While crisis and war take on many forms, a crisis against a multilinear A2/AD threat essentially gives rise to two probable warfare scenarios.

The first scenario is a rival's use of force that wantonly restricts access to the commons (air, maritime, etc.). Such a scenario could pose an imminent, destabilizing threat to the sovereignty of the targeted nation.[18] If the target nation perceives that only resorting to armed force will lead to restoration of its lost access, then the goal must be cessation of the rival's effects. For example, globalization has increased the importance of global maritime trade. It follows that actions which interrupt that trade will produce political-military clashes.[19] In such a scenario, the United States, leading an effort to restore the target nation's commons access,

will be faced with the task of sufficiently mitigating the A2/AD effects to bring about conditions for a satisfactory peace. Such a campaign would raise questions of its ability to limit the scope of the campaign to avert a widening of hostilities.

Under the second scenario, an adversary's aggression involves conquest or occupation. Thus, if a belligerent A2/AD rival chose to unilaterally occupy contested territory, the resulting military assignment could be to dislodge the newly entrenched forces. An ensuing effort for restoration of proper sovereign control may call for a sizeable US or coalition counter–A2/AD campaign.

For either of these scenarios, the time before an adversary commences hostile action presents the best opportunity to manage the crisis through deterrence and shaping actions.

In looking at these and other scenarios of A2/AD crisis and conflict, readers may ask if the United States has previously confronted similar actors and circumstances. Earlier twentieth-century wars demonstrate that in some ways A2 and AD are not entirely novel. Studying illustrative examples of A2 and AD can help inform US understanding of their consequences in future war. To be clear, this is not to say the United States has been here before and need only reprise previous counter–A2/AD solutions; invariably, this proves to be yesterday's solutions to yesterday's problems. A helpful place to begin is three interesting chapters of enemy A2 and AD in three theaters of World War II. Germany's *Kriegsmarine* campaign to isolate England from Allied maritime support lasted from 1939 to 1945. Its A2 strategy in the Atlantic presented a clear and present danger to the Allies. The German U-boat threat was eventually overcome through improved Allied tactical integration, fledgling military operations research lessons, new technology, and the exploitation of German signals.[20] In particular, this battle offers a persuasive case for the effectiveness of a marriage of land-based air, maritime, and electromagnetic spectrum capabilities.[21]

At least two other WWII chapters are worthy of note relevant to A2 and AD. Nazi Germany's extensive V-1 and V-2 missile programs rained destruction on England. The Allied counter to these missile raids was Operation Crossbow, the bombing of German missile staging and launch sites in Europe's Low Countries.[22] Among Crossbow's insights was that, lacking rapidly acquired and widely disseminated accurate missile location data, preplanned or real-time redirected aerial attacks would be of incremental success at best.[23]

The final illustrative chapter was the application of Japanese airpower against US surface combatants in the US Pacific island-hopping campaign.[24] At its height, kamikazes were more than a WWII phenomenon; they demonstrated the founding principles of guided, long-range antiship attack. As demonstrated since WWII, ship attack technologies will hold navies at increasing risk of catastrophic attack across littorals and push them farther into oceanic areas.

Any treatment of A2/AD must be balanced with a discussion of how the attributes of US forces accentuate their vulnerabilities to attack. In the name of economies and efficiencies, the Pentagon reorganized its forces and support architectures in ways that, paradoxically, made them more vulnerable to the effects of A2/AD information disruption and network attack. Two prominent examples of this paradox come to mind: first, connectivity is critical to US intelligence-surveillance-reconnaissance (ISR) constellations. Its dependence on reach-back/push-forward data architectures, while conferring great strength, represents a range of vulnerabilities too tempting for hegemons to overlook.[25] The implication is that disruption and degradation of the ability to both see and sense will mean US forces not being able to rapidly attack the full range of time-sensitive, high-value targets of an A2/AD regime.

A second prominent example is the civil-military enterprise of just-in-time logistics services and the US approach to the use of globally dispersed lift and supporting service providers. The vulnerability of the US military's logistics enterprise to larger global information grid disruptions caused by cyber attack has been documented in related analytic work stretching back years.[26] Attacks on US military logistics forces and infrastructure are more serious than corrupting information network data, although that is significant. Impeding US sealift freedom of action by under/above sea attack, striking US airfields to disrupt strategic airlift, interdicting overseas US petroleum storage-handling sites, and conducting cyberspace counter-logistics attacks in US home zip codes are but a handful of actions A2/AD adversaries can undertake to degrade US forces.

Some of the A2/AD measures described thus far straddle peace, crisis, and conflict, while others may not be unfurled until the onset of hostilities. Yet, if any of these events are viewed as simply liabilities of war, the costs of mitigating them will be seen as costs of doing business during war. They will remain remote and apart from a peacetime investment strategy to counter A2/AD effects before war. That mindset will weaken the US

ability to stair-step into crisis and beyond. But peacetime costs are only a slice of the pie for how the United States must effectively shape and deter A2/AD adversaries. Another significant aspect is the improved employment of US assets in ways that can either lessen tension or demonstrate resolve in a crisis when deterrence fades.

Of the concepts, weapons, and tactics the United States develops to respond to A2/AD, the human factor may represent the most formidable—and the greatest opportunity. No one currently in the US military, from its most senior four-star flag leaders to the newest recruit, has served in an era when the United States could not permissively transport its forces throughout the global commons to disparate places with names like Chosin, Pleiku, An-Nafud, Anbar, Nangarhar, and others.[27] To prevail against A2/AD, the United States must visualize itself apart from what it has been doing for the last 20 years to something different: nonpermissive warfare where everything will be intensely challenged, US superiority may not be attainable, and our resolve to enter a conflict will be powerfully tested.

Amplifying the A2/AD Strategy

If there is weakness in contemporary defense writings, it is a failure to put aside the numerous A2/AD systems of the PRC, Iran, Russia, and North Korea to answer a fundamental question: What is the "so what" of A2/AD? To arrive at some initial understanding, A2/AD aims must be overlaid along with their capabilities in the five domains (including electromagnetic spectrum) to determine the potential range of nonlinear operations.

Referring to figure 2, the first aim of A2/AD is *strategic preclusion*. Allies rely on the United States to underwrite the treaty guarantees of mutual defense. An A2/AD adversary would seek to create an environment where US allies question the US ability to defend them. Erosion of confidence in the United States could cause an ally to step back from honoring access arrangements, or it could otherwise limit freedom of action through decreased commitment to host US forces, refusal to grant overflight, unwillingness to demarche the aggressive acts of a regional hegemon, or an absence of cooperative training with US forces.

The second aim is *operational exclusion*. An adversary will plan and execute actions to set the conditions for the campaign they envision. One such preparatory effort could be to infiltrate important US cyberspace networks with intelligence-gathering and destructive malware to yield

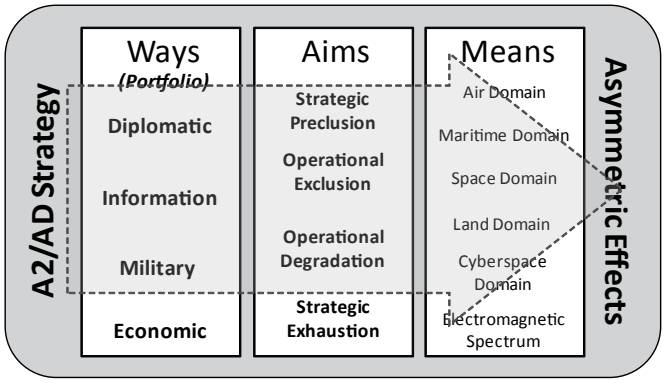


Figure 2. Breakdown of A2/AD strategy

exploitable intelligence in steady state and act as the forward offense in crisis and conflict. Other exclusionary measures would be to jeopardize key sea lanes to impede US maritime force flows, or an adversary could seek to exclude US space-based capabilities by disabling orbiting platforms, creating orbital debris bands, or using antisatellite technologies to attack certain on-orbit platforms.[28]

The third aim is *operational degradation*. Increasingly, using cyberspace to conduct unattributed attacks allows A2/AD actors to amplify their effects in other domains and reach into the US homeland. Due to the vulnerability of commercial cyberspace infrastructure, there is strategic advantage in large-scale cyber attacks executed by proxies. Another example would be extensive degradation of the electromagnetic spectrum to sever the connectivity of US fielded forces from their distant senior commanders.

Figure 3 illustrates at what point in crisis and conflict each A2/AD aim becomes relevant. As shown, a successful A2/AD strategy will create a void where US shaping is attenuated by lack of opportunity space. The center parallel shaded arrow shows the "Needed US Region Shaping Range" and depicts the approximate ideal placement of A2/AD aims in thwarting US power. The arrow, "Opposing Strategic Effect of A2/AD"—pushing against the US shaping range—illustrates how its range of options is truncated by A2/AD strategy. In steady state, A2/AD effects seek to shrink US opportunities to shape; in conflict the lack of shaping and deterring translates into preempted and precluded US force.

The fourth and final aim is *strategic exhaustion*. Key objectives within this aim include exploiting the vulnerabilities of lengthy US exterior logistics lines contrasted with an A2/AD adversary's shorter interior lines of logistics. More than ever, global military logistics is dependent upon the

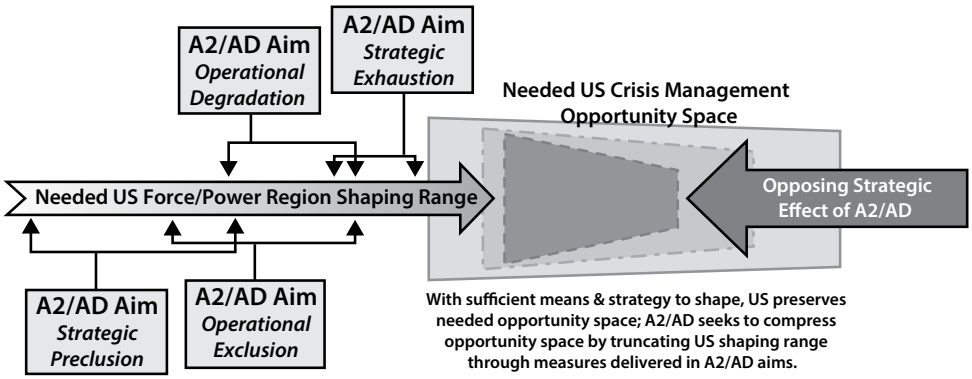


Figure 3. Employment of A2/AD aims

rapid exchange of accurate time-critical data within stable information networks. Any disruptions to timely, accurate data exchange will inevitably inject delays into US force generation, deployment, and resupply. The goal of exhaustion in an A2/AD crisis or conflict is to cause the US expeditionary offense to crumble due to the inability to sustain its effort or to defeat US resolve through fear of strategic failure.

Crisis Management Design Framework

A brief design introduction is appropriate before describing the dynamics of this concept. As shown in figure 4, design is essentially a three-step process that begins with the *system frame* and culminates in the proposed *concept design*. An important point is that design is cyclical; that is, while it seeks to achieve understanding of complex problems, design theory acknowledges that once anyone acts on a problem, this gives rise to a new problem that necessitates the third design cycle begin anew at the system frame. This crisis management concept does not propose a discreet design for every possible encounter with any A2/AD adversary; rather it advocates for a useful design framework from which to enter into A2/AD crisis management planning.

Three important ideas form an underlying latticework for this crisis management design concept. RAND defense researcher, Dr. Forrest Morgan, establishes that crisis management is

> a process by which policy makers seek to diffuse the threat of war with other powerful states without surrendering important national interests. It employs elements of deterrence, coercive diplomacy, assurance and inducement. . . .

> Crisis management is largely about strategy . . . effectively managing a crisis can be perilously difficult if the underlying structure of the geopolitical environment is unstable. Military forces comprise an important element of that structure, either contributing to stability or undermining it.[29]

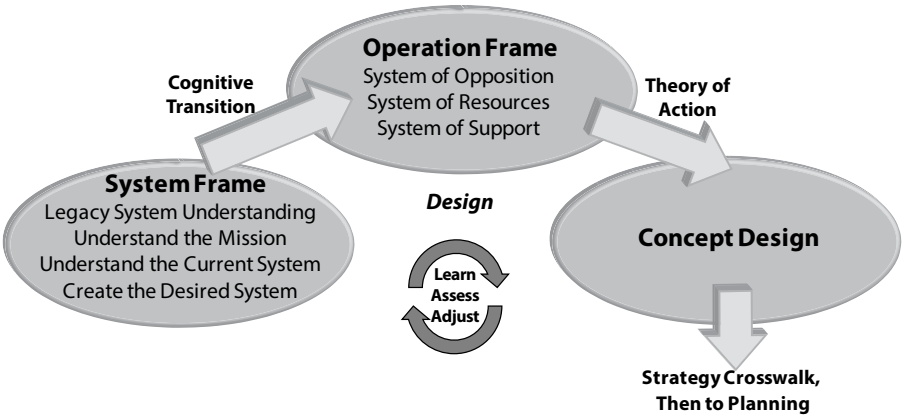


Figure 4. Operational design process

In an important sense, Morgan captures the effect of A2/AD: a nonlinear strategy and associated capabilities combined with an adversary's willingness to act as a regional destabilizer for its advantage. This point ties into the second piece of the lattice, geopolitical instability.

In a broad treatment of escalation written in 2008, a RAND group studying structural instability in the geopolitical environment determined that when an adversary has unique capabilities or can successfully challenge an opponent's capabilities where there is no counter, perceived advantages could embolden that adversary to escalate in ways it perceives its opponent cannot answer.[30] As a result, an A2/AD adversary will perceive it can act—perhaps escalate—without fear of an effective use of counterforce or credible armed response. The resulting instability creates opportunities and tipping-point incentives toward the A2/AD actor.

The third ingredient of the lattice is that a central outcome in recent US wars was regime change and/or decisive victory. A continuation of these policies could inadvertently undermine US ability to manage escalation and deescalation in crises. From their perspective, A2/AD adversaries—for example, a nuclear-armed regional adversary—could perceive little to no value in self-restraint, especially with regard to its use of WMD.[31]

Contemporary deterrence scholars such as Dr. T. V. Paul assert that for much of the past 20 years, its unipolar status has led the United States

to focus on deterring rogue states and transnational terrorists seeking WMD.[32] Paul's work holds that US deterrence of state actors appeared to come to an end with the demise of the Soviet state.[33] Indirectly, he hints at the demand signal for an effective applied deterrence construct to meet future challenges, among them, A2/AD. However, the issue is not so much about theoretical deterrence as it is countering A2/AD with applied deterrence. The ability of A2 and AD to undermine US power projection and force points to a conundrum: if the United States cannot project power and force because A2/AD contests its access and freedom of action, then in point of fact, the deterring effect of its power-force combination is precarious.

Escalation is best undertaken against an A2/AD adversary in a manner that emphasizes eliminating US "say-do" gaps. This is difficult in an A2/AD environment without an appropriately developed force, a crisis management design, and an effective counter–A2/AD theory of victory. Figure 5 is the design's cognitive transition, the conceptual answer to the challenge imposed by the problems described in the design system frame. The key design problem is that a weak joint deterring force will not ensure the United States has sufficient escalation agility to credibly move at will along the entire range of operations. This limitation opens the door for an A2/AD opponent to prevail through strategic preclusion.

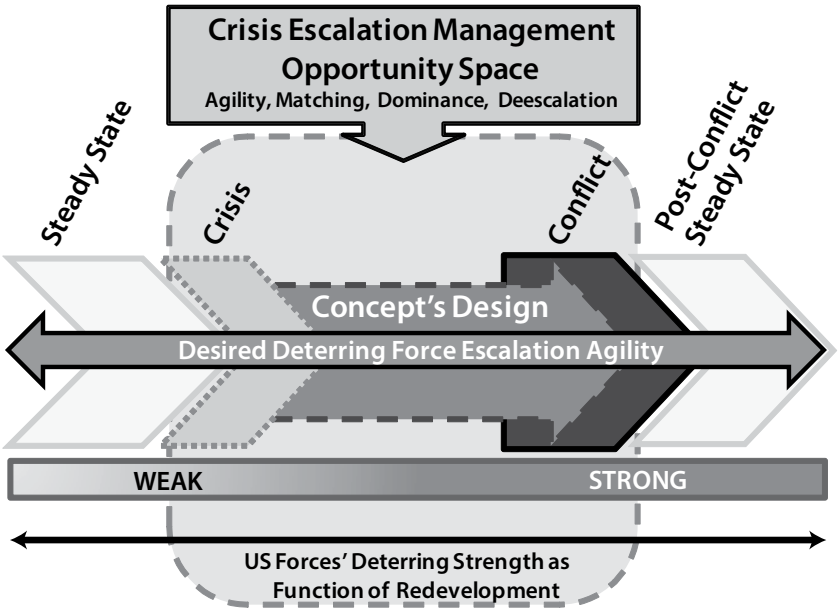


Figure 5. Crisis escalation management design

The design of this applied concept begins with its first component and lynchpin: the *deterring force*. A2/AD forces threaten to push US forces to ever farther operating ranges with increasing intelligence, logistics, firepower, and maneuver inefficiencies while decreasing the ability of the joint force to deter. US military force must be relevant, effective, and efficient within a region. Relevance rapidly diminishes if the force cannot enter important regions and operate with sufficient latitude. The idea of the deterring force is, in essence, what it takes to ensure US forces remain relevant and do not have to accept being driven to disadvantageous operating ranges to survive and operate.

Figure 6 portrays the continuum of strong-to-weak deterring forces with an associated range of attributes. Some of the key assumptions of the deterring force are that the United States possesses national political will (commitment of populous not assumed); some credible intelligence warning and indications are available; some margin of military defense technology leadership (not necessarily supremacy) exists in certain areas; and relevant allies/partners remain committed to the use of power, including force. At the far left of the range, the *weak* deterring force is a notional joint force with no redevelopment—little to no changes undertaken to counter–A2/AD effects. In contrast, the *strong* deterring force depicts a fully redeveloped force in all domains enabled by robust US access and assured freedom of action.

Against a regional A2/AD hegemon equipped with substantial political-military capability and capacity in one or two domains, a less than fully

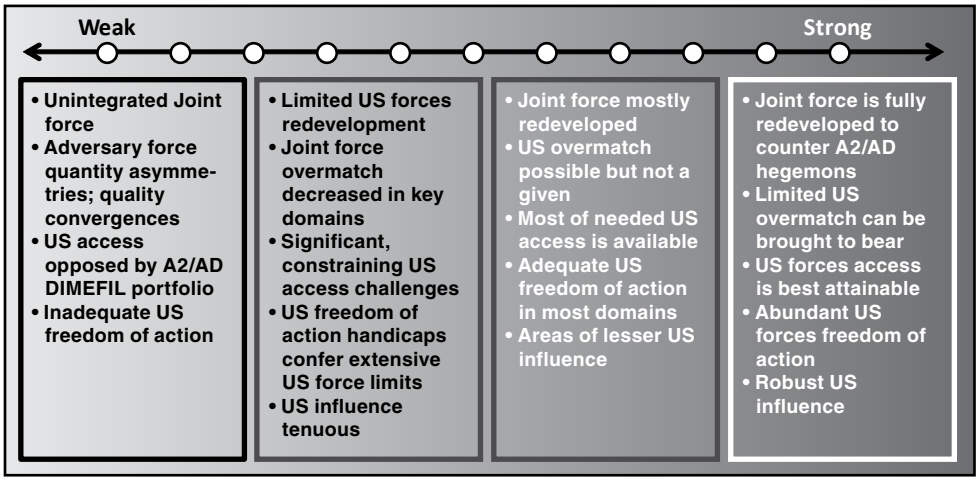


Figure 6. A2/AD deterring forces with associated range of attributes

redeveloped joint force may be able to prevail with only modest difficulty. But against a near-peer competitor, that same joint force may be unable to prevail, even with the most strenuous effort. For the purposes of this essay the most demanding crisis scenario is assumed: US power and forces perform most of the heavy lifting. The point of the continuum is that without an appropriately developed deterring force, access, freedom of action, and regional influence, a US force would be unable to satisfactorily achieve crisis management goals.

If one assumes that the joint force can overcome access and freedom-of-action barriers, one must explain what it does in steady state that assures shaping, enhances stability, and mitigates the potential for crisis and conflict. One of the key ways to foster stability is through continuous regional presence in peacetime and persistence during crisis and conflict. Persistence is the force's ability to be present in highly contested places and spaces of every domain (see fig. 5). The kind, frequency, and locales of persistent presence must be less like domination zones and more like control positions.

America's ability to pivot its escalation approach points to the second component of this concept, *escalation agility*. This component goes hand in hand with the first, because escalation agility is what the US deterring force must accomplish in all A2/AD conditions. Escalation agility informs US understanding of how much latitude it has in its crisis design in relationship to the rival's ability to preclude, exclude, preempt, and degrade (the aims of A2/AD, fig. 2) US power and force projection. Underlying the escalation pivot is the extent to which US strategy preserves needed opportunity space to act (see fig. 3). If the adversary reduced opportunity space below some minimal level, it would crowd out the US ability to execute actions that best confront the opponent's strategy.

Again, figure 5 demonstrates that the stronger deterring force will ensure the joint force has enough agility to overcome a range of A2/AD threats, from regional powers such as Iran or North Korea to near-peers such as the PRC or Russia. So long as the United States can escalate with confidence versus an A2/AD rival, escalation-matching moves and countermoves could be viewed as a chessboard with different levels corresponding to diplomatic, information, military, economic, finance, intelligence, and legal (DIMEFIL). As such, US crisis objectives on any of these separate but interrelated levels need not be "checkmate." The whole-of-government moves, rooted in a single design, must be about protecting and preserving

key matching board space as opposed to the outright commanding position game style of escalation dominance.

The United States cannot count on a cooperative and predictable escalation rival, so respective sides will likely continue matching until actor patience is exhausted or matching is no longer viewed as a rewarding approach. When or if crisis participants seek another approach, the United States must be confident it can pivot to a new design and the associated strategy to meet the dynamic demands of the crisis.

In US defense literature, the phrase "escalation control" is prominent both as an approach and an implied mind-set. However, the limits of US ability to control any situation is really about its ability to form a union of its means and ends despite an A2/AD adversary's ways and means to deny that opportunity. Because of the nature and severity of adversary counteractions, this concept advocates for a new way to think of and operationalize escalation: *escalation management*. A2/AD's goal is to keep US forces at bay and, in so doing, attenuate their relevance and combat power. Any proposition of US crisis response against an A2/AD strategy that is based on a US theory of escalation control is inherently misaligned to a situation where the United States cannot control escalation because it cannot get its forces into a region to establish control. This may compel US leaders to forego escalation matching and instead opt for a leap to escalation dominance that will bring its own kind of A2/AD crisis destabilization risks.

The fourth component of this concept for design is *escalation matching*. Because of US military overmatch, its leaders have taken on something akin to disdain for matching adversary escalation moves within a political-military crisis. An explanation could be that military leaders more readily identify with dominance in a crisis because they perceive the leap to dominance is the shortest path with the least jeopardy toward victory, preservation of things, and protection of US vital interests. While that simplified view of escalation in crisis seems sensible, its common sense does not reflect the uncommon twists and turns inherent to disruptive A2/AD strategy. The present mind-set of escalation dominance trains leaders to dominate the adversary; however, in an A2/AD crisis, dominating could aggravate the crisis or make it acute by ineffectively responding with force that is blunted by the opponent's strategy.

The notion of matching an adversary's escalation measures is not about US capitulation or passivity; it is about pacing. The advantage of pacing is it sets a tempo that provides opportunities to build in actions such as

pauses to encourage leader assessment on both sides. Additionally, escalation matching is not built on a leader-follower paradigm; rather, it is an intuitive actor approach. Other key points in escalation matching are determining what actions to undertake and how to accomplish those actions. What to do can be concisely stated as a series of interrelated US moves and countermoves that minimize adversary upside while simultaneously minimizing (minimize/minimize) the US downside in the crisis.

That minimal up/minimal down approach inherently emphasizes the US advantage in terms of mitigating adversary actions that would seek to accelerate the crisis or jeopardize US interests. Another way of thinking of matching is to visualize it as opportunity space with the attributes of a physical maneuver space where actions and counteractions are not linear. Escalation matching is the space between actor-on-actor engagement where, at one end, the parties lapse into a mutually agreeable postcrisis settlement. In contrast, at its upper limit, escalation matching space gives way to another larger, diverse space: the area of escalation dominance. Discerning the upper bounds of the matching space is where adversary intent and the strength of its responses produce risk to the United States that must be mitigated rapidly through escalation dominance.

Escalation matching requires that US estimates of the adversary be grounded in an accurate understanding of the rival's appraisal of the situation. The conceptual structure of escalation matching ought to eliminate the perception that it cedes crisis opportunity, advantage, or initiative to an opponent. Against an A2/AD rival using a rheostat approach, a controlled escalation framework could provide both the utility of incremental methods within a pacing construct and a tempo that provides the opportunity for reassessment to minimize miscommunication and miscalculation.

Escalation dominance is the fifth component in this design concept. Simply stated, domination ensures the United States can escalate in ways that allow it to gain and maintain the upper hand in a crisis. Unlike the minimize/minimize of matching, dominance seeks to maximize US upside while simultaneously minimizing (maximize/minimize) the adversary's upside potential. Looking through the prism of A2/AD, escalation dominance could be metaphorically described as the sum weight of all US national instruments exerting more downward pressure than the opponent's counteracting upward pressure that seeks to expand the crisis or initiate conflict.

A2/AD seeks to diminish US ability to dominate escalation by deploying numerous active defense layers up to hundreds of miles in depth to

make penetrating and ultimately closing with the opponent both difficult and costly. Consequently, a weak deterring force must operate from disadvantaged distances that decrease its deterring potential and combat power. The only US options may be either to cede the object of the crisis or inherit a menu of least-preferable options that further destabilize or accelerate the crisis.

Completing the Concept: Deescalation

During the ramp-up to an A2/AD crisis, this concept for design calls attention to continuous deescalation opportunities. In contrast, the lack of thorough deescalation discussion in US military doctrine produces incompletely formed understanding of the ramp-down phase of any crisis. The belief could arise that ramp-down is not worthy of US attention because of the perception that deescalation resembles capitulation. This lack of understanding sends a message to the military that bringing any crisis to a conclusion is, at bottom, a situation for which the prescription is more overwhelming military force. The danger of such a one-dimensional mind-set is reigniting of the crisis, displacement of the crisis elsewhere, failure to recognize a ramp-down opportunity, or failure to remain committed to a deescalation plan. Any of these could prolong the crisis or cause preventable conflict. The need for a deescalation framework can be understood as: once high in the branches of a tree of crisis, a nation's leadership may not be able to determine acceptable ramp-down methods that can help it descend from those limbs. Without more precepts to guide deescalation, the United States risks inculcating a perception in the minds of its competitors that it does not back away from crisis nor can it. To its allies and partners, it risks the perception of a lack of nuance below the threshold of war.

There are three components of deescalation. The first, *appropriateness*, requires assessment at some relevant point that identifies the most useful deescalation measure in a given context. War gaming deescalation measures in the crisis can be useful; however, the time to identify and war game responses may cede initiative and momentum to an opponent. Any deescalation measure offered must involve things held mutually important by the United States and its rival. While understanding can never be perfect, an important consideration is the avoidance of ambiguous US measures that can take a crisis down unintended paths. If in its crisis design (fig. 4) the United States cannot make an adversary traverse a specific path of crisis

actions, perhaps the adversary can be herded to an intersection and presented with courses of action.

The next deescalation facet is *demonstrability*. This idea holds that whatever deescalation measures are used, they must be verifiably observable by the adversary. This raises the question of the accuracy of US understanding with regard to what it believes an A2/AD opponent can observe and the probable immediacy of the opponent's observation.

The third deescalation component is *credibility*, something US leaders must bear in mind throughout a crisis. Namely, that deception, obfuscation, and subterfuge, while of some utility in attaining escalation advantage, are the very things that could undermine opposing leader confidence in attempted deescalation measures, by either side. If at the signal of bona fide deescalation, sufficient interregime mutual trust cannot be established, deescalation could paradoxically produce the opposite outcome.

Priming the Design Pump

During the Cold War, Dr. Alexander L. George developed seven principles of geopolitical instability.[34] While his principles (fig. 7) are somewhat dated, they have relevance to the challenges of A2/AD strategy. George's advocacy for political-military synchronization, continuous control of fielded forces, and a rheostat employment approach of military forces speaks to the need and benefit of design. It helps guide further development of this concept to better manage crises against an A2/AD opponent. In a larger sense, George's position is that initiating a crisis or entering a war ought to be choices of last resort. Additionally, his work commissions leaders to maintain cognizance of the crisis exit or, as a minimum, crisis ramp-down opportunities. Those ideas speak to the utility of design in defining a given A2/AD problem and the most effective escalation and deescalation actions against it. Unfortunately, his principles are not the vital elements of a campaign plan against an A2/AD adversary whose strategy and capabilities are purposely built to mitigate US steady state shaping, blunt US access, mitigate its influence, suppress freedom of action, and, ultimately, crowd out operational latitude. In these ways, George's precepts are not the theory of action (fig. 4) but valid foundational ingredients in this concept for design.

A2/AD crisis management design leverages US power, but design cannot make something strong if it is inherently weak. Power and forces have their own values, which lie within a weak-to-strong continuum. As an example

George's Crisis Instability Principles

1. **Continuous Forces Control:** political leaders must retain control of the actions of their respective military forces in crisis
2. **Rheostat Forces Control:** force movements [and composition] should occur in a design that allows leaders to speed up and slow down their deployment and movement; assumes desired pauses can be built into the situation
3. **Synchronized Pol-Mil Actions:** assumes that political leaders can conceive of a construct and employ
4. **Unity of Objectives:** military force employment is right-sized to the associated diplomatic objective(s) in the crisis context
5. **Measured Use of Force:** intent is to ensure that movement and use of force is not misconstrued—when and where it is not our intent—to be a step that presages major war
6. **War is Preferred Last Resort:** signals our intent that US seeks a negotiated path one not single-mindedly culminating in armed hostilities
7. **Build in an Egress:** leaves the adversary a face-saving path out of crisis to militate the perception that war is the only path of resolution

Alexander L. George, "A Provisional Theory of Crisis Management," in Alexander George, ed., *Avoiding War: Problems of Crisis Management* (Boulder, CO: Westview Press, 1991).

Figure 7. George's principles amplified

of how interagency relationships fit into this concept, US combatant commanders continue in their key role in shaping and regional influence that supports other US agencies or are, in turn, supported by them. Without an offsetting US strategy, or at least its outline, a design for crisis management cannot perform the strategy currency conversion function between an A2/AD challenge and the planning to overcome that opponent's strategy. In a broader sense, the US offsetting strategy must aspire to crowd out the A2/AD strategies of regional and near-peer competitors.

As heightened tensions lead to crisis, cognitive transition—the key deliverable in the early stage of crisis management design (fig. 4)—leads to a campaign plan that employs salient tools of US power. With regard to military power, the deterring force's escalation agility is the measure of the joint force redevelopment and sufficiency to handle the rigors of an A2/AD challenge.

There will be barriers to implementation of this concept. For example, describing the components of the concept is not difficult, but executing them in the interagency context ahead of the speed of crisis will be daunting. That is due to A2/AD's reach, scope, immediacy, and being

grounded in years of shaping campaigns. Therefore, ready-made internal US national power and force relationships must preexist to deliver supported/supporting interagency actions to seize and, where needed, regain the information and operations initiatives.

Crisis management design cannot be an ad hoc undertaking of the moment. A given design must be informed by the steady state shaping plan lines of operation. Experimentation, development, and deployment of this concept must be undertaken in conditions where US designers and leaders have an opportunity to reflect upon situational factors, known threats to execution, desired outcomes, and likely US commander guidance. A cornerstone of this concept is not how other DIMEFIL instruments are subordinated to the "M"; rather, it is about how all US tools form an agile, integrated, interdependent design.

As the JOAC, Air-Sea Battle, and other efforts hone the tactics, techniques, and procedures of a redeveloped joint force, this concept for crisis management design must be coupled to those efforts. With this concept, US political leaders and senior war-fighting commanders will have a conceptual vehicle to counter A2/AD with conceptual design that averts conflict or puts the United States in a position to degrade a hegemonic rival while remaining strong.[35]

The Offsetting US Strategy

Formulating a national strategy to offset and overcome the competition of A2/AD should drive the development of regional steady state counter–A2/AD shaping plans that are composed of lines of operation that unfold over years. This proposal is not simply advocating for better cooperative security planning to counter A2/AD, though that would be helpful. The concept puts forward the idea of an offsetting strategy where US agencies do not work in silos but actively share common goals, priorities, processes, and a scorecard to conduct DIMEFIL shaping progress. Figure 8 illustrates a notional offsetting strategic approach of ends, ways, and means. The end states in this national strategy transcend the ends of specific campaigns. The ends in this strategy framework are rooted in enduring US policy objectives and outcomes: strong US conventional deterrence, robust extended deterrence, and protected interests to include the shared interests of partners. The arrows radiating from the ring of continuous strategization are enduring shaping actions that deliver DIMEFIL outcomes focused

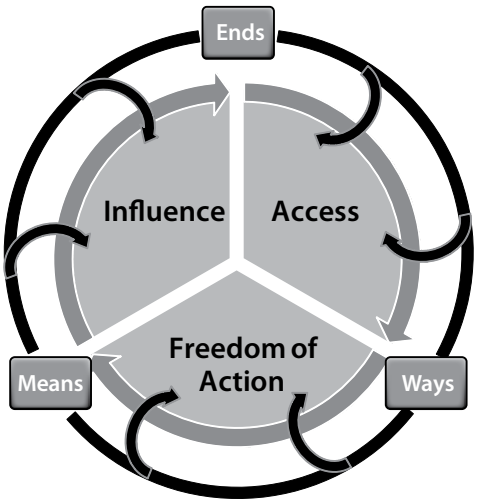


Figure 8. Counter–A2/AD strategy

on the products at the figure's center: assured access, enhanced freedom of action, and strengthened influence.

The first product of a US offsetting strategy, *access*, translates into places, bases, infrastructure, and overflight enabled by agreements that allow the United States to distribute its forces to reinforce security and stability during steady state shaping and crisis response.

The second strategy product is *freedom of action*. Often conflated with access, it is a related but separate idea. Freedom of action is an expression of US operational latitude once forces are deployed forward—wherever "forward" is. For the purposes of crisis response planning, operational latitude is a measure of ability to freely maneuver and arrange forces in all domains, including the electromagnetic spectrum. Out of this understanding flows force employment options out to the tactical edge through the combatant commander's campaign plan.

Influence is the third strategy product and flows from a national offsetting strategy. Regional US influence is the aggregation of shaping efforts in each key region over years to reassure allies and friends of its steadfastness to deliver on its regional stability and security commitments. US influence helps bring about an environment where nations with shared interests feel they can enable US access and freedom of action.

The US offsetting strategy must not be confused or conflated with either strategic planning or strategic programming; rather, it requires candid assessments. While the dynamic of multiple A2/AD actors brings a new kind of complexity and multiple threats, it is unlikely domestic politics will allow a marked increase in future defense budgets to build separate counter–A2/AD acquisition programs for the PRC, Iran, Russia, and North Korea. The offsetting strategy must be composed of coherent regional counter–A2/AD strategies whose DIMEFIL means are flexible enough to apply to all A2/AD threats. The successful long-term competitive approach used against Russia during the Cold War is an example. Figure 9 shows the relationship of steady state shaping to the entire crisis

phase. In a larger sense, it depicts the major developmental components of US offsetting strategy.

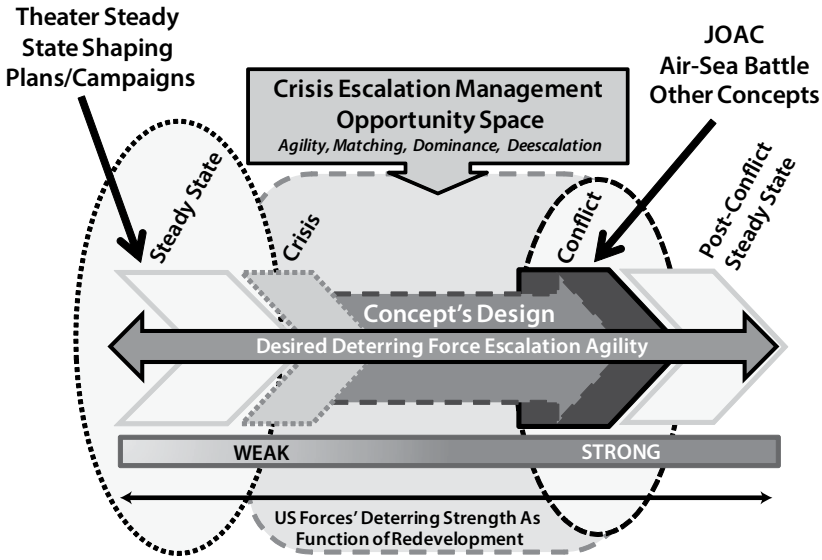


Figure 9. Components of US offsetting strategy

Planning for the Future of A2/AD

Even if US relations with the PRC, Iran, Russia, and North Korea ultimately remain nonconfrontational and the respective ideologies eventually moderate, those nations aggressively develop, deploy, and proliferate many of the A2 and AD technologies US military forces will inevitably confront. This yields something called the 10/90 Rule: there may be a 10-percent chance of a hot war between any of those nations and the United States, but there is a 90-percent chance the US military will confront the A2/AD stuff each rival proliferates. Therefore, much of US counter–A2/AD effort could be justified by identifying ways to mitigate systems, but such an approach would leave the nation bereft of strategic vision and purpose.

In the US defense establishment, some voices advocate for counter–A2/AD efforts directed at specific nations, especially the PRC. Arguably, there is some utility in such an approach for the formulation of US defense policy and force development. However, a focus on a single nation would likely overlook the advantages of an approach which spans all A2/

AD adversaries. By offsetting the commonalities across the group of A2/AD opponents, no adversary will believe the United States has ceded any regional competition.

To aid planning of present and near-term counter–A2/AD shaping, it is appropriate to examine some relevant initial ideas. While not all-inclusive, these efforts comprise important planks in any combatant commander's counter–A2/AD shaping framework. As a minimum, the following should comprise any campaign to shape a region with an A2/AD threat:

- Targeted diplomacy which strengthens alliances and cultivates friends and partners.
- Continued military-to-military engagement that broadens relationships, deepens understanding, and helps eliminate miscommunication and miscalculation.
- Multination defense technology investing and, where appropriate, risk-reducing acquisition in relevant systems, platforms, and technologies.
- Realistic counter–A2/AD combined training in the air, naval, cyber, space, and land forces domains.
- Continued growth in diverse sharing of relevant strategic and tactical A2/AD and adversary intelligence.
- Development of equipment and procedures for collaborative domain awareness to enhance security and eliminate piracy and ungoverned sovereign air, maritime, and land spaces.
- Assured uncontested access to air, maritime, and space commons to provide for the stability of commerce to ensure protection of US and shared partner interests.
- Winning the media and public opinion narratives and getting ahead of competing information operations.

Currently there are important initiatives which signal a beginning in counterweighting the regional hegemonic efforts of the PRC. On 16 November 2011, the United States and Australia announced the establishment of a US Marine Corps training location in Darwin, Australia. This demonstrates how access improves out of active international relationships that promote influence and protect shared interests.[36]

Prior to the start of a conflict with an A2/AD hegemon, the United States must shape events to either prevent a crisis or enter the conflict in the most advantageous position. However, it is important to concede that none of this concept or any other US counter–A2/AD efforts will entirely eliminate strategic miscalculation. If an A2/AD adversary miscalculates, trained US military and interagency experts using crisis management design will likely be the best hedge against uncertainty.

Warfare continues its inexorable march of change, and the meaning of that change is coming into focus. Due to advocates in the US defense establishment, counterinsurgency will remain part of the spectrum of warfare; however, such conflicts will not involve the preponderance of US vital interests. At war's high end, regional and near-peer A2/AD hegemons can jeopardize numerous US vital interests. The United States must be ready to vigorously defend its interests wherever they come under attack.

For the time being, the United States must not suffer the winner's curse: believing that because it prevailed against past challenges, future victory will happen with little additional work and no infusion of new ideas. Military planning and strategic assumptions are not exempt from breakdown. Clausewitz, Sun Tzu, and Jomini admonish America that successful theories of victory are dependent on, but are not exclusively dictated by, the advancements of war-fighting technology. US theories of victory in crisis and conflict against A2/AD nonlinear strategy depend on the soundness of a superior US offsetting strategy coupled with excellent strategic practice rooted in better ideas.

The focus here was to acquaint the reader with the effects and challenges of A2/AD on US power and force projection while presenting an innovative design to manage crisis against A2/AD rivals and suggest new ideas on the deterring force, escalation agility, escalation management, and de-escalation. The objective was to present organizing precepts for a design to effectively manage a military crisis against the PRC, Iran, Russia, or North Korea. A subsidiary objective was to link US shaping to both A2/AD and this concept's design for crisis management. If A2/AD adversaries believe their approach can successfully keep the United States out of a regional situation or impose devastating costs, then it could be faced with an inability to unite its means to ends. From a design perspective, this concept locates and sets the A2/AD problem, but it does not present campaign solutions; that is local work yet to be done. Armed with this concept for

mitigating A2/AD effects, US power and force can benefit by being more relevant throughout the range of crises brought on by any A2/AD actor.

Inasmuch as they will alter the US post–Cold War deterrence mindset and its doctrinal way of battle, the changes wrought by A2/AD must not be ignored by hubris that results in an unwillingness to recognize its strengths. A failure to fully comprehend A2/AD's implications may cause the United States to unwittingly forfeit a window of innovation and redevelopment opportunity to reinvent its power and force projection. In the decades since Pearl Harbor, history teaches that strategic shock with crippling, perhaps lasting, consequences can occur if a determined adversary believes it can attain its goals and realize its ends when the United States neglects to be a nation of foresight and action. SSQ

Notes

1. *Sustaining U.S. Global Leadership: Priorities For 21st Century Defense* (Washington: Office of the Secretary of Defense, 2012), 3.
2. Ibid., 4–5.
3. Ibid.
4. *Joint Operational Access Concept* (Washington: Joint Chiefs of Staff, 2012). The term *concept* can mean different things to different people in different places within the DoD. However, as used in this essay, a military concept identifies a military problem and a proposed range of solutions. Broadly speaking, US military thinking on the utility of a concept is that it describes how current capabilities could be better leveraged; some aspect of military operations could be improved or innovations harnessed to improve war-fighting advantage.
5. The word *locate* is not meant in the sense of position; rather, in the sense that the true essence of a problem has been revealed through reflection and analysis. Furthermore, military designers hold that once a problem is located it can be plotted in relation to all the contextual actors, forces, and relevant entities.
6. Joint Publication (JP) 3.0, *Joint Operations*, 2011, A-1–5. As discussed in this essay, the nature of war is encompassed by the 12 principles contained in appendix A of JP 3.0. The principles are formed around enduring ideas of warfare and as such are present throughout the range of military operations across all eras and locations. Also see Carl von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1984), 89, for one of Clausewitz's immortal truisms, "War is more than a true chameleon that slightly adapts its characteristics to the given case." As more than one defense commentator has noted: although war is a chameleon, regardless it remains an animal. This truth serves as a lead-in to an oft-stated defense maxim: the nature of war does not change, only its character changes.
7. Robert Buchanan, "Wicked Problems in Design Thinking," *Journal of Design Issues* 8 (Spring 1992): 15–16. This essay is an early survey which chronicles the development of design theory since its inception. See also Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," *Journal of Policy Sciences* 4, (1973): 155–69. The article made the case for the existence of wicked problems within a framework. The premises of that framework endure to this day.

8. *Commander's Appreciation and Campaign Design,* TRADOC Pamphlet 525-5-500 (Fort Eustis, VA: Army Training and Doctrine Command, 2008)—a high-level primer on characterizing military problems for US Army commanders. See also Ben Zweibelson, "Does Design Help or Hurt Military Planning: How NTM-A Designed a Plausible Afghan Security Force in an Uncertain Future," *Small Wars Journal* blog, 9 and 16 July 2012, http://smallwarsjournal.com/blog. Major Zweibelson's two-part blog articles depict advanced, specialized military design within a wartime campaign context. From academic articles on design theory to real-world application, design is as versatile as it need be.

9. Timothy L. Thomas, "Google Confronts China's Three Warfares," *Parameters* 40, no. 2 (Summer 2010): 101–13. A retired US Army officer and foreign area studies expert at the Army's Foreign Military Studies Office, Mr. Thomas has emerged as one of the DoD's China cyber warfare experts. See also Timothy Walton, *China's Three Warfares* (Washington: US Navy, 2012), 1–11. Walton, a civilian employee of Delex Consulting, wrote the report under contract for the Navy. The text is best when read in combination with Thomas's related work.

10. Walton, *China's Three Warfares*, 1–11.

11. William Ashemore, "Impact of Alleged Russian Cyber Attacks," *Baltic Security & Defense Review* 11 (2009): 4–40. In a detailed essay, Major Ashemore lays out not only the case for Russian involvement in the large-scale cyber attacks of April and May 2007 in Estonia, but also provides useful analysis as to why the precedent of the 2007 attacks is a matter of significance to NATO and America.

12. Eneken Tikk et al., *Cyber Attacks Identified against Georgia: Legal Lessons Identified* (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2008), 1–45. This is one of a small group of unclassified works on Russia's cyberspace attacks and activities associated with the 2008 incursion into Georgia.

13. Michael Elleman, "Iran's Ballistic Missile Program," *Iran's Ballistic Missile Program* (blog), US Institute of Peace, 9 August 2012, http://www.iranprimer.usip.org/resources/irans-ballistic-missile-program/html; and *Annual Report To Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington: DoD, 2011), 27–32.

14. Mark Stokes and Ian Easton, "China and the Emerging Strategic Competition in Aerospace Power," in *The Next Arms Race*, ed. Henry D. Sokolski (Carlisle, PA: Strategic Studies Institute Press, 2012), 141–78.

15. Desmond Ball, "Asia's Naval Arms Race: Myth or Reality," paper presented at the Asia Pacific Roundtable, Kuala Lampur, Malaysia, May 2011. For a more lengthy treatment of the naval arms race in Southeast Asia, see Charles A. Meconis and Michael D. Wallace, *East Asia Naval Weapons Acquisition in the 1990s: Causes, Consequences, and Responses* (Westport, CT: Praeger, 2000).

16. Rod Thornton, *Military Modernization and the Russian Ground Force* (Carlisle, PA: Strategic Studies Institute Press, 2011) is a compact, well-written monograph which lays out the major components to Russia's determined efforts to professionalize, reorganize, redistribute, and reestablish the capabilities of its ground forces. There are clear implications in this monograph for all branches of the Russian armed forces.

17. William Komiss and LaVar Huntzinger, *The Economic Implications of Disruption to Maritime Oil Chokepoints* (Washington: Center for Naval Analysis, 2011). This report studies the impacts to global regions based on evaluating the disruption of oil through six of the world's major international shipping routes. Although not all regions of the world would see a disruption in imported crude oil supply, four continental regions—more so than the closure of any of the five remaining chokepoints—would experience crude oil disruption in a closure of the Strait of Hormuz.

18. *America's National Interests* (Washington: Commission on America's National Interests, 1996). Although this report was written to identify only US vital interests, its utility is the insight into international relations, hence its usefulness in identifying the interests of US allies and partners.

19. Abraham Denmark et al., "Contested Commons: The Future of American Power in a Multipolar World," Center for New American Security, 25 January 2010. This report lays out the case for the economic value of the global commons and their importance to the economies of nations and international trade.

20. David White, *Bitter Ocean: The Battle of the Atlantic, 1939–1945* (New York: Simon & Schuster, 2006). Called by some naval historians the longest-running naval war at sea, the Battle for the Atlantic began in 1939 and did not end until the conquest of the Third Reich in 1945. Of the numerous books and articles available, the following were utilized in this essay: Clay Blair Jr., *Hitler's U-Boat War: The Hunters, 1939–1942* (New York: Random House, 1996); and its companion volume, Blair, *Hitler's U-Boat War: The Hunted, 1942–1945* (New York: Random House, 1998). The following was written by a WWII RAF Coastal Command pilot: Andrew Hendrie, *The Cinderella Service: RAF Coastal Command, 1939–1945* (Barnsley, UK: Pen & Sword Aviation, 2006).

21. *Electromagnetic spectrum* (EMS) refers to the utilization of nascent radar and ASDIC technologies as well as the robust use of Allied countersignals intelligence against the Third Reich, of which ULTRA was an essential source.

22. Maj Merrick Krause, "From Theater Missile Defense to Anti-Missile Offensive Actions: A Near Term Strategic Approach for the USAF," (School of Advanced Airpower Studies thesis, 1998), 11–14, http://www.au.af.mil/au/awc/awcgate/saas/krause_me.pdf. See also, Lt Col Mark Kippihut, "Theater Missile Defense Reflections for the Future," *Airpower Journal* 10, no. 4 (1996): 35–52. A benchmark WWII reference series of texts remains *United States Strategic Bombing Survey (USSBS), V Weapon (Crossbow) Campaign* (Washington: War Department, 1945).

23. Kippihut, "Theater Missile Defense Reflections for the Future."

24. Nicolai Timenes Jr., *Defense against Kamikaze Attacks in World War 2 and Its Relevance to Anti-Ship Missile Defense*, vol. 1 (Washington: Center for Naval Analysis, 1970). Volumes 1 and 2 were likely used to undergird the analytic requirements necessary to support the nascent AEGIS program's capabilities to assist senior US Navy leaders in determining fleet design and range of capability in countering aerial ship attack.

25. Brian Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (McLean, VA: Northrop Grumman, 2009)—a report prepared for the US-China Economic and Security Review Commission. While specific architectural studies are classified, this source is a well-written illustration of the computer network warfare challenges facing a large network which can be accessed by sophisticated cyberspace attackers.

26. Steven Noel, "Combinatorial Analysis Utilizing Logical Dependencies Residing on Networks (CAULDRON)," presentation at 9th Annual Air Force Intelligence, Surveillance, and Reconnaissance Agency and Communications Conference," San Antonio, TX, January 2010. That large portions of the global information grid are vulnerable to determined, sophisticated cyberspace attacks is not new, nor is it necessarily new knowledge that much of the computer capacity of civilian logistics providers to the DoD have computing capacity within the global information grid and thus it too is vulnerable. An interesting project that speaks to cyberspace attack and how it can be mitigated can be found in George Mason University's CAULDRON program and the work of Noel.

27. It was assumed that if the Cold War ever turned hot between the superpowers, US air, naval, and land forces would likely be confronted wherever they encountered Soviet forces. Since

the end of the Cold War, space to a greater degree and, for the first time, cyberspace, conceivably increased the number of domains where crisis and conflict may occur from three to five. Factor in the EMS as a venue for militarized effects, and the number of hostile domains could increase to six.

28. On 11 January 2007, the PRC detonated a defunct FY-1C weather satellite at an altitude of 536 miles. The resulting explosion produced more than 10,000 pieces of debris.

29. Forrest Morgan, "Escalation," unpublished RAND monograph, November 2011, 23.

30. Forrest Morgan et al., *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, CA: RAND, 2008), 168–69.

31. Ibid., 171.

32. T. V. Paul and Patrick M. Morgan, "Deterrence among Great Powers in an Era of Globalization," in *Complex Deterrence: Strategy in the Global Age*, eds. Paul, Morgan, and James J. Wirtz (New Delhi: Cambridge University Press, 2009), 265.

33. Ibid.

34. Alexander L. George, "A Provisional Theory of Crisis Management," in *Avoiding War: Problems of Crisis Management,* eds. George and Yaacov Bar-Siman-Tov (Boulder, CO: Westview Press, 1991).

35. Gen Norton Schwartz and ADM Jonathan Greenert, "Air-Sea Battle," *American Interest*, http://www.the-american-interest.com/article.cfm?piece=1212.

36. "Press Briefing by Press Secretary Jay Carney, Deptuy [*sic*] National Security Advisor for Strategic Communications Ben Rhodes and NSC Senior Director for Asia Danny Russel," Parliament House, Canberra, Australia, 16 November 2011, http://www.whitehouse.gov/the-press-office/2011/11/16/press-briefing-press-secretary-jay-carney-deptuy-national-security-advis.

Technology, Qualitative Superiority, and the Overstretched American Military

Daniel R. Lake

Why did the wars in Afghanistan and Iraq put so much strain on the US military? During the 1990s, the question was whether US forces should be prepared to fight two "major regional conflicts" or just one. No one thought that smaller operations would cause problems. Nonetheless, by 2006–07, operations in Iraq involving less than one-third the forces deployed for Desert Storm were stressing the US Army so much there was open debate over how close it was to breaking. The proximate cause is obvious—the Army lacked the assets it needed for operations in Iraq. The real question is why that would be the case. How is it the United States requires roughly half of the world's military spending to support a military too small to comfortably sustain moderate-intensity operations? I argue that the strain on the US military is the direct result of focusing on technological solutions to tactical and strategic problems. This practice is rooted in American culture, which is particularly prone to technological optimism. The focus on leveraging technology to gain qualitative superiority over US foes has resulted, due to escalating procurement costs and increased logistic needs, in a military that is too small where it needs to be: on the battlefield.

For more than a decade now, we have been hearing that the US military is "overstretched" and "at the breaking point." This is not simply an exercise in hyperbole. Rather, it reflects real problems the military was already facing even before the war in Iraq. For example, the intervention in Kosovo escalated to include seven out of 20 Air Force combat wings and required the call-up of reservists to conduct air refueling.[1] The high demand on reconnaissance and electronic-warfare aircraft for Kosovo also forced the Air Force to cut back on monitoring the "no-fly" zones in Iraq. This is indicative of the wider issue, which is that the US military in general was arguably understaffed and overstretched by the end of the 1990s.[2]

Daniel R. Lake, PhD, is an assistant professor in the Political Science Department of the State University of New York College at Plattsburgh. He previously taught at Denison University, Sweet Briar College, and Wayne State University. He has also been published in the journal *International Security* on coercive airpower.

It was evident by late 2003 that due to the force cutbacks of the 1990s, the need for troops in Iraq would strain the US military.[3] As the Iraq war dragged on, it became clear those projections were on the mark, and sustained operations in Afghanistan and Iraq risked breaking the Army.[4]

Why did these operations strain the US military so much? The United States has the largest defense budget in the world, the second-largest active duty military, and the seventh-largest military when reserves are included.[5] If any state should be able to handle operations like Afghanistan and Iraq with ease, it is the United States. Nevertheless, even with a $670 billion defense budget, the United States found it challenging to sustain a deployment of 200,000 troops.[6] This is particularly interesting because the much larger forces deployed for Operation Desert Storm did not cause any such problems.

A partial explanation is the mismatch between US military capabilities and needs. The bulk of the forces in Afghanistan and Iraq were ground forces, so most of the burden of these operations was borne by the Army and Marines. Such was the case with Desert Storm, but its much shorter duration made that larger deployment easier on the military. During 2005–06, the United States averaged 175,000 to 200,000 ground forces deployed to Afghanistan and Iraq, according to the Congressional Budget Office (CBO).[7] The CBO considered this an unsustainable level of deployment, based on the current availability of active duty and reserve forces. By January 2006, virtually all the available combat units in the Army, Marine Corps, and National Guard had been deployed to Afghanistan or Iraq at least once.[8] Many were already on their second or third tour. Many National Guard and reserve units had already hit their legal limit of two years deployed in a five-year period, shifting almost the full burden of operations onto active duty forces. The US Army and Marine Corps are simply too small to sustain such a level of operations.[9] To sustain an all-volunteer professional army, the rule of thumb is a three-to-one rotation ratio, meaning you have two units at home for every one deployed.[10] Higher deployment rates make it more likely that service members will decide against a military career, reducing retention and making it harder to sustain the overall force. Sustaining a deployment of 175,000 to 200,000 troops thus requires about 525,000 to 600,000 personnel. This is perilously close to the total active strength of US ground forces (around 700,000). When you take into account other deployments outside the continental United States (South Korea, Okinawa, Europe, etc.) and their

personnel needs, the Iraq and Afghanistan operations overstretch available ground forces. In essence, the US military has a manpower deficiency that is likely to get worse in the future if not addressed.[11] The drawdown in Iraq has temporarily mitigated this problem, and the situation will further improve as forces are pulled out of Afghanistan, but the potential for military overstretch remains.

This is not just a problem affecting US ground forces. The challenges created by the Kosovo intervention demonstrate how the Air Force can be overstretched. The Navy could also easily be overstretched by current obligations (much less a new operation) because it has too few warships.[12] While each warship is individually very capable, it cannot be in two places at once. As such, the decline in fleet size since the end of the Cold War is already causing problems.[13] For example, the Navy is currently unable to provide enough warships to control piracy off the coast of Somalia.[14] Dealing with that problem would take several times the 30 or so warships that various navies have deployed to the area. In the future, the small size of the Navy could also cause problems in a confrontation with China, which may already have a larger navy than the United States.[15]

The US military is even at risk of running out of critical types of ammunition. This has already happened at least once. Operations over Kosovo depleted the supply of air-launched cruise missiles to the point the Air Force had to cut back on their use.[16] Government stocks of the most expensive precision-guided munitions (PGM) are inherently limited due to their higher cost,[17] so every time there is a high demand on them there is a risk of running out. For example, a military strike against Iran's nuclear program would probably rely heavily on the new Massive Ordinance Penetrator, a 15-ton "bunker buster" bomb, but the Pentagon is only buying 20 of them.[18]

Why does the United States, with the largest defense budget by far, have inadequate land, air, and naval forces to carry out sustained operations at even a moderate tempo? The immediate cause is the shrinking military, which is the smallest it has been since the late 1940s. This has been exacerbated by a change in the distribution of forces within the military away from combat forces (the "tooth") toward an ever larger support network (the "tail"). While defense budgets are higher now than they have been in 60 years, the military is smaller in absolute terms, and the combat forces necessary to carry out missions make up a relatively smaller share of this smaller military.

These changes are mainly due to an increasing reliance on technology. While advanced technology does make the military more effective in many ways, it comes at an ever increasing cost. This is exacerbated by the US military's cultural bias toward technological solutions, which results in intensive use of cutting-edge technologies for maintaining qualitative superiority. The high cost of these efforts under conditions of relatively flat budgets has led to cuts in personnel and equipment. In addition, the increasingly sophisticated weaponry requires more logistical support. This has caused both a shift of troops from combat to support roles and an increased reliance on contractors for support. Ultimately, the overstretch has been due to the technological sophistication of the US military.

The US military's bias toward technological solutions to military problems explains its cultural basis and shows how it has manifested since World War II. Thus the focus on advanced technology has affected the size and composition of the US military. This begs the question whether (and how) the experience of military strain will affect US defense policy and how other states and nonstate actors are reacting to US technological superiority. In the end one must consider what this means in terms of the basic dynamics of providing for US national defense.

Technology and the American Way of War

The "American way of war" has a couple of basic characteristics that have implications for military organization and procurement.[19] The first is a bias toward waging war for unlimited political objectives and a concomitant focus on annihilating its foes.[20] US military leaders traditionally have rejected Clausewitz's maxim that war is merely the continuation of policy through other means,[21] hence the American way of war can be thought of more as a way of battle than of war.[22] American generals typically resisted the "meddling" of politicians in their conduct of war (and still resent it), and civilians were largely content to leave war to the professionals.

The second characteristic is strategic materialism, which developed due to the extensive resources available to American armies by the Civil War era.[23] This entails a preference for defeating the foe through the use of firepower and material superiority rather than through technique.[24] Material superiority has been seen as a way to avoid casualties, which American elites see as desirable because they perceive the public to be casualty averse.[25] Therefore, in each major war, starting with the Civil War, American armies

(except the South during the Civil War) have been lavishly equipped compared to their European counterparts.

These two main characteristics manifested repeatedly from the Civil War through the Korean War. In each major conflict during this period, the United States entered the war with a military inadequate for the current struggle. It responded by massively mobilizing the population and the economy and sought to completely defeat its foe. While not always successful, the victories of the North in the Civil War and the Allies in World War II—combined with the way that failure to completely defeat Germany in World War I led to World War II—reinforced American prejudices regarding how war should be fought.

The Korean War broke the pattern in two ways. First, after China's intervention it was not possible for the United States to achieve a decisive victory without resorting to massive use of nuclear weapons. Second, combined with the Berlin crisis, it clearly indicated that the Cold War had begun, which led the United States to maintain a large peacetime military for the first time.

The establishment of a large peacetime military allowed American culture[26] to express itself through the structure and equipment of the military in ways that had previously not been possible due to the small military budgets typical of interwar periods.[27] Culture is important because it affects how war is fought and thus how a nation prepares for war.[28] Most relevant here is a cultural bias where the application of technology is seen as the best way to solve a problem.[29] While an openness to technology is characteristic of Western cultures and helps explain how Europe was able to become so dominant by the nineteenth century,[30] American culture is unique in containing a strain of "technological utopianism" that sees technology as a panacea.[31] This focus on technological solutions is a logical extension of military materialism, though with particular consequences described below.

Technology has been seen as the solution for several tactical and strategic problems since the beginning of the Cold War, including avoiding American casualties, limiting collateral damage, and countering the quantitative superiority of America's foes.[32] In addition, America's political culture has developed to the point that having the most advanced military is an end in itself.[33]

The preference for technological solutions manifested repeatedly during the Cold War. The Eisenhower administration proposed to deal with the

threat posed by large Soviet conventional forces in Europe by threatening nuclear retaliation (the "New Look"). This involved general cuts in the military and an emphasis on strategic nuclear forces, mostly air forces. Since there were massive cuts in conventional forces, all three services (Army, Navy, and Air Force) pursued their own independent nuclear programs.[34]

By the end of the Eisenhower presidency, it was becoming apparent that the United States could no longer rely on nuclear deterrence to protect Europe from the Soviets. The development of Soviet strategic nuclear forces, including the first intercontinental ballistic missiles, was inaugurating the era of "mutually assured destruction." Since both sides now had the ability to destroy the other using strategic nuclear forces, US nuclear deterrence was no longer seen as credible for preventing a conventional assault in Europe. In response, the Kennedy administration developed the doctrine of "flexible response" to deal with the new strategic reality.[35] Civilian specialists in military strategy and business, led by Robert McNamara, sought to make force more adaptable by creating options short of nuclear Armageddon.[36] While this included a conventional buildup, the United States mainly sought to counter Soviet quantitative superiority with NATO qualitative superiority.[37] This included introducing a whole new generation of equipment, including the M-60 main battle tank, new tactical aircraft like the F-111 Aardvark and the F-4 Phantom II fighter, and new naval capabilities in antisubmarine warfare.

The way the United States conducted the Vietnam War also demonstrates its cultural predisposition toward technological problem solving, as well as the limits of that approach.[38] To deal with North Vietnamese air defenses, the Air Force and Navy began extensive deployment of electronic countermeasure (ECM)–equipped aircraft and antiradiation missiles.[39] To provide the mobility needed to effectively fight the guerrillas, the Army deployed the first airmobile division and used helicopters extensively throughout the war.[40] To interdict North Vietnamese supply routes through Laos and Cambodia, the US military developed and deployed new sensors that remotely provided targeting data.[41] The Vietnam War also saw the development of the first remotely piloted aircraft (RPA), or drones, and the first widespread use of PGMs.[42] Ultimately, all this technological innovation was unable to compensate for the failure to develop a political strategy for winning the war.[43]

Efforts to gain and maintain qualitative superiority increased with the end of the draft and the switch to an all-volunteer military in 1974, in part

because of increased casualty aversion after Vietnam.[44] Called the "offset strategy," it involved a systematic attempt to leverage new technologies (such as information technology) and develop new equipment to counter Soviet numerical superiority, particularly after the Soviets engaged in a major modernization effort during the 1970s.[45] This resulted in another new generation of military equipment including the M-1 Abrams main battle tank, the M-2/3 Bradley infantry fighting vehicle, the F-15 and F-16 fighters, the F/A-18 fighter/attack plane, the F-117 stealth fighter, the B-2 bomber, the *Ticonderoga*-class guided missile cruisers, and the Patriot surface-to-air missile system.

The astonishingly effective performance of the US military in the Persian Gulf War seemed to validate the focus on technological solutions.[46] New equipment developed since Vietnam—including PGMs, global positioning system (GPS) satellites, the joint surveillance and target attack radar system (JSTARS), stealth aircraft, and more prosaic hardware developed as part of the offset strategy—was given credit for the lopsided victory achieved.[47] During the 1990s the American military began to increasingly focus on PGMs as a way to avoid US and civilian casualties[48] and accomplish what Leslie Gelb referred to as "immaculate destruction."[49] The technological advances involved were seen as allowing the United States to use military coercion more freely,[50] as in Bosnia and Kosovo.

When Donald Rumsfeld became secretary of defense in 2001, he entered office firmly believing in the virtue of technology as a solution for myriad tactical and strategic problems. He set out to transform the culture of the military away from its risk- and casualty-averse preference for overwhelming force in favor of precise application of force—Gelb's "immaculate destruction.[51] This included a focus on reducing or eliminating Clausewitz's "fog of war" through better reconnaissance and communications capabilities as well as increased use of PGMs to make warfare more predictable and allow the military to do more with less.[52] In particular, Rumsfeld sought to make the military more efficient through the "super-empowerment of the individual" and by automating war through tools such as drones.[53] The success of the invasion of Iraq in 2003 seemed to validate this approach.[54]

While technological optimism has been a feature of US defense planning for several decades now, each service has its own culture which persists and manifests itself in its attitude toward technology.[55] The Air Force is the most technology-oriented branch, since it is defined by technology

and emphasized its core technologies when building its identity after its creation in 1947.[56] The Navy is also very technology oriented, but as an old service it has traditions that constrain and channel its technological enthusiasm.[57] The Army is fairly accepting of technology, seeing it as a means to gain an advantage over foes.[58] The Marines value technology the least, due to their warrior ethic and a history of tight budgets that created an institutional culture focusing on personnel rather than equipment.[59] In a broad sense, a key difference in service culture comes down to the difference between "manning equipment" (Air Force and Navy) and "equipping the man" (Army and Marines).

Technology and the Incredible Shrinking US Military

As a general rule, the cost of military equipment tends to rise faster than the inflation rate due to technological change.[60] This is true especially for modern weapons, which rely heavily on computing power for their effectiveness. Military computers do not rapidly decline in cost, per Moore's Law,[61] since they lack the massive economies of scale afforded to consumer electronics—much military hardware and software is custom designed and must constantly be upgraded to remain secure.[62]

Seeking to maximize performance also maximizes costs, particularly when developing multirole equipment.[63] Multirole systems, by their very nature, are going to be more complicated to develop and more costly to field.[64] Research and development costs increase rapidly as the technology incorporated increases and becomes more recent.[65] As a result, new weapon systems almost always cost more than expected, usually more than double the original estimate.[66]

Rapid technological change, which has been the norm for several decades, exacerbates these problems. First, anticipation of future improvements leads to smaller production runs.[67] This increases the unit cost of equipment because the research and development (R&D) costs get amortized over fewer units.[68] The large-scale production necessary to generate economies of scale (and reduce per-unit R&D costs) is constantly deferred.[69] Second, there is always an incentive to wait a little longer to incorporate a little more advanced technology.[70] This serves both to delay the introduction of new weapon systems and to keep costs high. Third, there is a constant desire to modernize existing equipment to take advantage

of technological advances, which also makes it harder to realize economies of scale.[71]

The combined effects of intergenerational cost growth, incorporation of the latest technologies, and smaller production runs have made the latest US weapon systems extremely expensive.[72] For example, the "flyaway cost" (excluding R&D) of a new F-35 fighter increased from $69 million in 2001 (current $) to $133 million in 2011 due to cost overruns and production delays.[73] This is more than four times the inflation-adjusted flyaway cost of the aircraft it is replacing, the F-16 ($30 million in 1985).[74] R&D costs add at least another $23 million per plane.[75] The cost is so much higher in part because the F-35 incorporates cutting-edge technologies, such as stealth, developed since the F-16. These planes are also very expensive because they are multirole aircraft meant to perform both air superiority and ground attack missions.

The impact of smaller production runs is particularly visible in the case of the B-2 bomber. The original production run was supposed to be 132 planes, but only 21 were actually purchased. As originally proposed (in 1986), the Air Force would acquire 132 B-2 bombers for a total program cost of $58.3 billion.[76] After cutting the production run to 21 and spending an extra $10 billion in R&D, the total program cost (in 1997) was $44.3 billion.[77] While the original estimated cost per plane of $442 million was undoubtedly inaccurate, cutting the production run from 132 to 21 certainly more than doubled the program unit cost based on the 1997 flyaway cost per bomber of $737 million. Even with no production economies of scale to realize, if the entire original planned production run had occurred, the total program unit cost would have been less than $1 billion ($737 million flyaway cost and $227 million per plane in R&D costs) instead of more than $2.1 billion. Another example played out with the F-22 fighter, the Air Force's top-of-the-line air superiority fighter, meant to replace the F-15. The original plan was to purchase 750 F-22s. When the production run was cut to 183, the unit cost went from $149 million to $342 million.[78]

This pattern of rising equipment costs is found across the US armed services. The Navy's new *Zumwalt*-class destroyer (DDG-1000) is the most recent class of surface warship developed. Its average procurement unit cost (not including R&D) is estimated at $4.3 billion per ship in 2010 dollars.[79] This compares to the $2.2 billion procurement unit cost of an *Arleigh Burke*–class destroyer (DDG-51), which originally entered service

in 1991. The increased unit cost is due to the inclusion of more advanced technologies, such as much greater automation, as well as its larger size (almost 15,500 tons vs. 9,500 tons). Because of the high unit cost, *Zumwalt* production was stopped after the third ship in the class was begun. As a result, the $9.3 billion in program R&D costs increased the total program cost per ship to $7.4 billion.[80] In comparison, the production of *Arleigh Burke*–class destroyers continues with 63 currently in service or on order, so the R&D costs have been spread across a much larger production run.

The nature of rising unit costs over time is shown on figure 1. As you can see, intergenerational unit costs go up exponentially for combat aircraft, and the same basic pattern (albeit more slowly) holds for other types of equipment such as ships.[81]

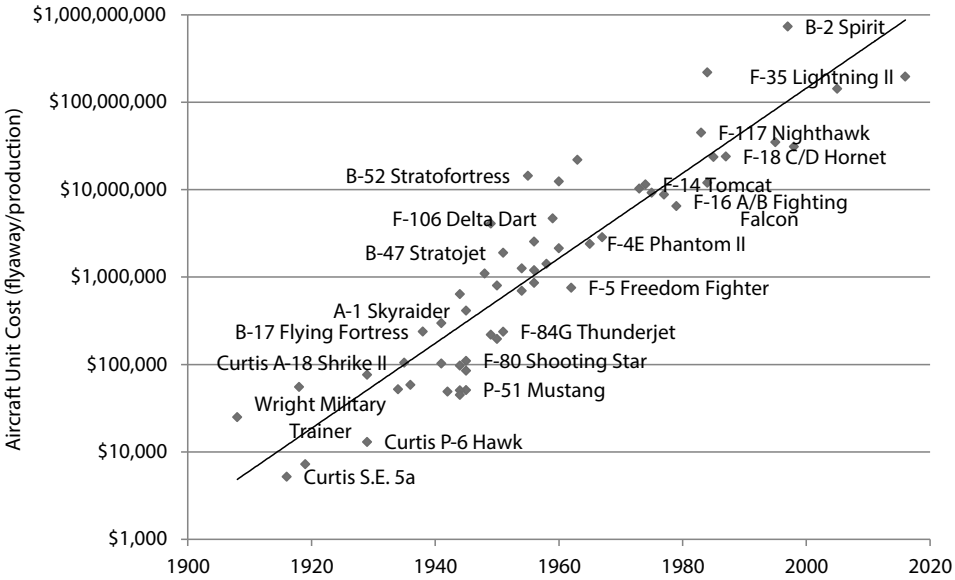


Figure 1. The rapidly increasing costs of US combat aircraft

Equipment that pushes the limit of what is technically possible also tends to be less reliable.[82] While component reliability tends to improve over time, the benefits are undermined by a tendency to improve capabilities by cramming more components into each system.[83] The net result has been rapidly increasing operations and maintenance (O&M) costs over the last several decades. For example, Air Force O&M costs increased

in real terms by 20 percent between the late 1980s and the late 1990s.[84] This is directly related to fielding more-sophisticated equipment. For example, the F-35 is estimated to cost a third more to keep flying than the F-16 it is replacing.[85] The B-2 bomber (an extreme example) requires 60 man-hours of maintenance for every hour of flight time.[86] When you include all O&M costs (personnel, equipment, fuel, maintenance, etc.), the average flight-hour cost went from about $4,800 in 1970, to $11,000 in 1985, to about $23,000 today (in constant dollars).[87]

Increasing the technological sophistication of military equipment also has important implications for personnel policy. While it reduces the relative importance of numbers, it puts a premium on high troop quality.[88] This is because to effectively use more-advanced equipment requires more training,[89] and the ability to successfully complete such training is a function of base troop quality in terms of intelligence and education. High-quality, smart, and well-trained troops are simply not available in large numbers, while low-quality recruits are less able to use complex weapons correctly.[90]

The switch to the all-volunteer military in 1974 made staffing more difficult and costly.[91] While conscripts can simply be required to serve, volunteers need to be enticed.[92] This requires investment in marketing, recruiting, higher salaries, and better benefits. Personnel costs have rapidly increased since 9/11, with total pay and benefit costs increasing from $73,300 to $126,800 per person in real terms (a 73-percent increase) between 2000 and 2011.[93] Fully a third of that increase is due to expanding costs of health care for retirees, an expense that is likely to continue to grow for the foreseeable future.[94] Recruiting and training costs have also risen. During 2008, it was estimated that recruiting and training 10,000 soldiers cost $1.2 billion a year.[95]

Critical for understanding the impact of technological change on the US military is the budget environment. As shown in figure 2, the US defense budget has been fairly stable in constant dollar terms since the Korean War. During this period, it never drops below $343 billion FY-2009 dollars (the 1955 low) and—except for the Reagan defense buildup—never exceeds $450 billion FY-2009 dollars during peacetime.

The result of dramatic increases in equipment and personnel costs within a fairly stable budget is evident on the table. While defense spending for 2009 is artificially inflated by costs associated with the Afghanistan and Iraq missions, even after deducting that expense (about $155 billion, ac-

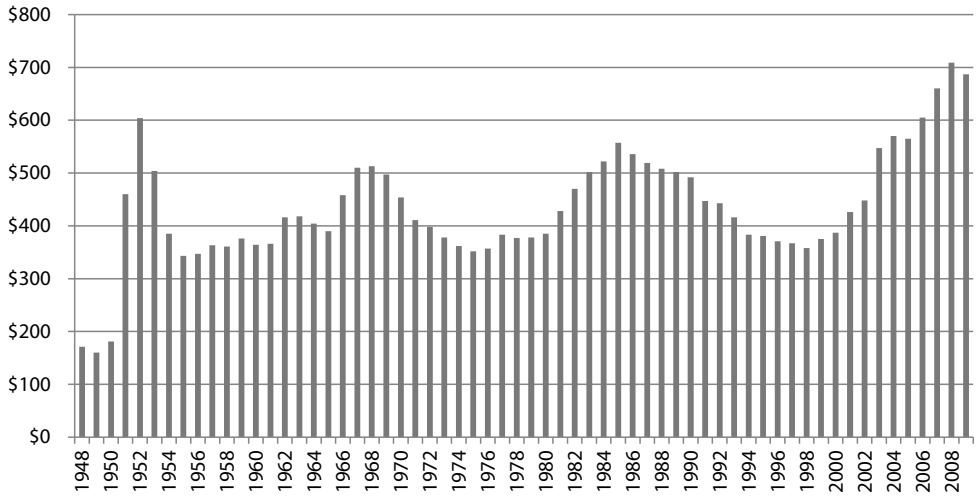


Figure 2. US defense budget authority in FY-2009 billions of dollars

Data from the Center for Arms Control and Nonproliferation.

cording to the Center for Defense Information) the United States still spent 38 percent more for almost 50 percent fewer combat assets compared with 1980. As discussed above, this trend is largely driven by increasing equipment costs resulting from technological change and the extensive use of cutting-edge new technology. In the case of the Navy, it is exacerbated by the decision to keep so many aircraft carriers, which forces the sacrifice of larger numbers of smaller vessels.[96] To save money, most navies have shifted to smaller ships, but the United States is bucking that trend at a high price.

The incredible shrinking US military

Item	1980	2009	Change
Total budget authority (2009 constant)	$385 billion	$687 billion	+78 percent
Navy ships (active)	530	285	-46 percent
Air Force fighter/attack planes (active)	2,769	1,493	-46 percent
Army divisions (active)	19	10	-47 percent

Data from the Center for Arms Control and Nonproliferation; the Naval History and Heritage Command; Ruehrmund and Bowie, *Arsenal of Airpower*; and Defense Business Board, "Task Group Report on Tooth-to-Tail Analysis."

Technology and the Changing Tooth-to-Tail Ratio

The focus on high technology has also shifted the US military's "tooth-to-tail" ratio toward a smaller tooth (combat assets) and a larger tail (support).

Technologically sophisticated weapon systems generally require more support, in part because (as noted above) they are less reliable than simpler systems.[97] The general rule is the more that is spent on an item, the more maintenance hours it will require to keep it operational.[98] Because of this, the increasing reliance on technologically sophisticated equipment since World War II has resulted in larger overall support requirements for the US military.[99]

Currently, the US tooth-to-tail ratio is very low, especially for the Air Force.[100] Only 16 percent of US military personnel have combat specialties (such as armor, infantry, reconnaissance, combat aviation, and surface warfare), which is lower than any of our NATO allies (except France and Poland), as well as China, India, Russia, Saudi Arabia, Singapore, South Korea, and Kuwait.[101] It is somewhat astonishing how few combat personnel are in uniform. For example, in 2003–04, the US military included only about 71,000 infantry,[102] which is a mere 10 percent of the combined Army and Marines or roughly 5 percent of the entire US military.

To some extent, the larger tail of the US military is the result of its global projection capabilities,[103] but most of it is related to increases in the logistical support required by combat forces.[104] This has increased over the last 100 years as the military has become more technologically sophisticated and is a direct result of that process. Basically, each generation of equipment requires more support than the previous one.

The impact of technological change is visible in the declining tooth-to-tail ratio for wars fought during the last 100 years.[105] While more than 50 percent of US troops deployed to France in World War I were combat forces, following the mechanization of the Army (during World War II), the share of combat forces in theater has never exceeded 40 percent. Since World War II, the trend is generally downward, though it appeared to reverse itself during the Iraq war, where 40 percent of the troops in theater during 2005 were combat forces. This was an artifact of two practices: an unprecedented use of contractors to support the troops and the location of many support forces in neighboring Kuwait. When support troops in Kuwait and contractors are taken into account, only 25 percent of the personnel in theater were combat forces.[106]

Note that there is a mismatch between the percentage of troops in Iraq that are combat forces (40 percent) and the share of the Army and Marines that is combat forces (about 25 percent). The burden of the Iraq and Afghanistan operations fell mostly on the Army and Marines and in particular

on combat forces and certain types of support troops (such as civil affairs and psychological operations). The strain on the military (both active duty and reserve components) resulting from post–Cold War demands has led to increased outsourcing of noncombat roles (and sometimes, but rarely, combat roles) to contractors.[107]

Contractors are increasingly important for providing support for US forces. This is due to the force cuts after the Cold War, the desire to keep as many combat units as possible on active duty, and high demands on the available troops.[108] It is easier to outsource logistical/support functions than combat functions, so that is where most of the activity has been.[109] In particular, contractors are heavily used for providing maintenance for our most advanced weapon systems such as the B-2 bomber and Navy vessels.[110] Very large numbers of contractors have been used to support US operations in Iraq, totaling more than the troops provided by US allies.[111] They perform a critical function, since replacing the 113,000 security and logistics contractors deployed in Iraq would require more than 250,000 additional military personnel to allow for normal personnel rotations.[112] That is simply not possible, as shown by the way the Army struggled to increase its numbers by 65,000 to support the "surge" in Iraq.[113]

The net impact of all this is a military that increasingly fields fewer, yet more-advanced, weapon systems and which contains a shrinking share of combat forces but still relies heavily on outsourcing support to contractors. The end of operations in Iraq has reduced some of the pressure, and things will continue to improve as operations in Afghanistan draw down. However, if the United States needs to use military force in the future, the same overstretch that characterized the last decade is likely to recur unless something changes the structure of the force. Even routine operations may cause strain on limited assets.

Implications

The United States

Right now the US military is vulnerable to overstretch by virtually any sustained operation, and even routine operations may cause problems. There are really only two ways to reduce the potential for overstretch. One is to increase the size of the military.[114] For example, another 100,000 to 200,000 ground troops are necessary to deal with existing security

threats.[115] Since the baseline defense budget (excluding Iraq and Afghanistan) is not a particularly large share of GDP,[116] in principle it could be increased enough to expand the military. This is not a good solution to the problem. Larger budgets increase the likelihood that equipment will be built to the limit of available technology,[117] rather than alleviating the problem of military overstretch. In fact, they may make conditions worse due to the increased support associated with maximizing equipment technology. Recall that the baseline defense budget has increased by almost 40 percent in real terms since 1980 (see table) while the military has shrunk by about one-third and combat assets by nearly half. Simply throwing more money at the military is not likely to reverse this trend. Regardless, since the baseline US defense budget is projected to remain stable for the next few years,[118] this is probably a moot point. If anything, budgets will likely be cut in the short term.[119]

Another possibility is to reduce costs within the existing budget to allow funds to be shifted toward expanding the military. For example, cutting unnecessary weapon programs could free up funds.[120] In reality, this would be extremely difficult due to the politics of US defense contracting which result in strong constituencies for existing programs.[121] When weapon programs are cut, the normal practice is to replace them with new programs or some other form of equipment-related compensation.[122] This practice seriously reduces the net benefit of program cuts. In addition, any savings from eliminating weapon systems tends to be very small since the spending is spread over several budget years and the contracts frequently include cancellation fees.[123]

Even if some funds could be freed up, high personnel costs make increasing the size of the US military very expensive.[124] In fact, the Pentagon has requested that Congress stop spending so much money on the troops, but it is politically unpopular (if not impossible) to do so.[125] Congress raises pay and benefits to signal its appreciation for service members and their families, and any attempt to rein in these costs faces opposition from powerful lobbying groups.[126] This is a long-term problem, because rising personnel costs (particularly health care) threaten to cut into procurement and maintenance budgets.[127] In fact, to cut personnel costs (thus protecting procurement and maintenance budgets), the Army is shedding personnel,[128] even though that makes future overstretch more likely.

A more promising approach would be to change the procurement process so military equipment is not at (or beyond) the limits of available

technology and does not try to do everything.[129] This would drive down costs since, as a rule of thumb, the last 10 percent of capability results in one-third of the costs and two-thirds of the problems.[130] It would also reduce logistical support and maintenance requirements, allowing a shift of troops from the tail to the tooth. This would be a very efficient way to address the problem. For example, if the military could reduce its requirements for support personnel by only 2 percent from the current level, it would be able to transfer nearly 30,000 personnel to combat functions. That dwarfs the impact of increasing the military by 100,000 personnel, which would only add about 16,000 combat personnel if current staffing patterns are followed. It would also free up money from the equipment budget because the equipment would require less R&D and be cheaper. One suggestion along this line is for the United States to develop light attack turboprops instead of relying only on jets like the F-35 and drones like the Predator for air support.[131] This would result in an air support platform that is cheaper to procure and operate and much easier to maintain. While it would not be able to operate in the same range of threat environments, it might provide a viable option for wars like the United States has found itself fighting in recent decades.

But this shift in procurement procedures is unlikely to happen. Perhaps unfortunately, the only times the US military has been willing to accept less than cutting-edge equipment has been when starved for funds (such as the peacetime before the Cold War) or during emergencies. Wartime demands tend to shift procurement toward large quantities at the lowest possible cost, which favors simple and cheap designs.[132] For example, during World War II neither the Liberty ship nor the M4 Sherman tank were very technologically sophisticated, but they were cheap to produce in volume, and that is what was needed at the time.[133] None of the wars the United States has been involved in since WWII has been big enough to cause a broad shift to wartime procurement patterns, which is just as well, since in this case the cure really is worse than the disease.

The rest of the time, the dominant trend is to generate "99-percent solutions," because that is how our procurement system is set up.[134] This is a function of the combination of entrenched interests (the defense industry and Congress) and a military culture of technological optimism. As such, shifting US procurement practices will be very difficult. There is some potential for change in the form of the Sustainable Defense Task Force, which has recommended cutting military spending and shrinking some

programs.[135] However, this would not actually alleviate the potential for overstretch since the proposals involve cutting US forces. The task force recommendations are also unlikely to be implemented because they face strong opposition from defense industry lobbyists and congressional districts with large defense industries.[136]

As a result, the United States is at the top end of the "cost/quality spectrum," using very high quality equipment but at a very high cost,[137] and, if anything, appears to be reemphasizing advanced technology.[138] The Air Force and Navy have persisted in purchasing expensive multirole aircraft even though their main role since Vietnam has been ground attack.[139] This practice continues with the F-35 program, though it is being delayed slightly.[140] The Air Force is also developing a new long-range bomber that is being fully funded, at least so far,[141] a new "space plane" (the X-37B Orbital Test Vehicle) to replace damaged military satellites and possibly attack enemy satellites, and the Hypersonic Technology Vehicle-2, which (if it works) will allow for very fast and long-range strikes anywhere on the globe.[142] The Navy is keeping all 11 of its aircraft carriers[143] and continues to procure highly sophisticated (and thus expensive and complicated) ships like the DDG-1000 and the littoral combat ship (LCS).[144] The Army is testing a new personal weapon (the XM25) that shoots projectiles that explode at a set distance.[145] The cost per rifle is around $35,000, and the cost per bullet will be around $25 after mass production begins. This is far more expensive than the M-4 rifle, the current standard personal weapon, and will require far more support. All the services are experimenting with electromagnetic weapons that may disable enemy equipment and missiles.[146]

The one new technology that seems to have some potential to alleviate the pressure on the budget and generate a more efficient force is remotely piloted aircraft, or drones. There have been dramatic increases in the use of RPAs in the last decade, to the point that they now fly more total hours than US manned strike aircraft.[147] Predator drones cost much less than the aircraft they can replace, like the F-16 for ground support, and can be more freely deployed in dangerous situations because their pilot is safely on the ground and they have a lower replacement cost.[148] In particular, RPAs have already proved useful as reconnaissance and fire-support platforms.[149] In the future, we are likely to see increased automation of combat systems on land and sea as well.[150] RPAs are simpler than the aircraft they replace and thus should require less maintenance and support.[151]

However, RPAs are not actually going to materially affect the potential for overstretch, at least not in the short term. Because 75 percent of the support for RPAs has been outsourced to contractors, it is quite difficult to assess what impact their deployment has on the US military.[152] As with outsourcing support in general, this serves to mask the real support required by the military without actually reducing it. In fact, armed drones require *more* support than the aircraft they replace, at least so far.[153] Their potential cost-effectiveness may also be compromised by a higher loss rate due to the lack of redundant systems (part of the reason they are cheaper to build) and the perception they are more expendable than manned aircraft.

Other States and Nonstate Actors

To some extent, the success of the United States at leveraging technology to gain military superiority is causing emulation by those states which can afford it.[154] None can fully emulate the United States at present, so different states maintain different capabilities. Britain and France have largely stopped including capital ships in their navies.[155] Other NATO states have completely abandoned certain weapon systems or capabilities, such as the Dutch (maritime reconnaissance) and the Danes (submarines).[156] This may have something to do with why our NATO allies tend to have a larger proportion of combat forces but still required US support to intervene in Libya.[157] Rivals, including Russia and China, are engaged in modernization programs which include weapon systems that approach the capabilities of US systems.[158] In Russia, this is deliberately aimed at countering US conventional superiority through professionalizing its military and upgrading its equipment.[159]

Two main barriers face other states that seek to emulate the United States: individual weapon systems are too costly, and operating high-tech equipment requires highly trained and educated, long-service professionals that most states lack.[160] This can be thought of as a function of the financial intensity of the technologies involved and the organizational capital necessary to adopt the technologies. *Financial intensity* simply refers to the resource mobilization required to adopt a particular military innovation in terms of the unit cost of new equipment compared to that of the item being replaced.[161] *Organizational capital* refers to the ability of personnel to master new tasks and the willingness to fundamentally transform the way the institution operates (cultural flexibility). The financial intensity of the US way of waging war is very high due to the high unit costs associated

with key technologies, such as PGMs and stealth technology. By itself, this limits the ability of many states to emulate the United States because they lack the financial resources. As costs fall we should see more countries adopt these technologies, since the organizational capital to incorporate them is relatively low. Cyber warfare may require less financial intensity to adopt because of the extensive use of related technologies by commercial enterprises, but it will probably require a high organizational capacity because it constitutes a fundamentally different way of waging war. This may limit the ability of states like China to exploit this technology, even though they are trying to develop this capability.[162] It may also explain why the Soviet Union was unable to emulate the US military when the Soviets realized the revolutionary implications of US advances in electronics and precision guidance before the United States did.[163]

One area with real potential for other states to compete with the United States is in RPAs.[164] The technology itself is new enough and potentially revolutionary enough that it could render much of America's existing conventional inventory obsolescent, much like the development of aircraft carriers rendered battleships obsolescent during World War II. RPAs are also relatively cheap to operate, so financial intensity does not prevent adoption.[165] The similarity of operating an RPA to playing video games also reduces the organizational capacity necessary for adoption, since potential "pilots" are readily available.

The main way potential opponents have responded to US technological superiority so far is through asymmetric approaches.[166] The intensive use of technology by the United States has resulted in conventional superiority but also creates opportunities for foes to employ asymmetric counters to top-of-the-line US weapons.[167] These include missiles which can threaten US tanks, ships, and planes for a fraction of their price; submarines to undermine US naval superiority; and cyber warfare capabilities to degrade US communications and intelligence systems.[168] They also include weapons of mass destruction (WMD), particularly nuclear weapons.[169] Asymmetric tactics, such as attacking US bases or using irregular forces (who are also becoming more effective due to technological change) rather than directly confronting the United States with conventional forces, are another option.[170] Much of the conventional superiority of the US military can also be countered by operating in urban environments or other congested terrain.[171]

Conventional asymmetric approaches that have the greatest potential to degrade US military superiority tend to focus on air defense, missiles, and

submarines. Rod Thornton suggests that antiaircraft artillery and man-portable air-defense systems (MANPADS) are particularly problematic for US aircraft because both can use passive sensors which make them harder for US forces to suppress. This could force the United States to either carry out airstrikes from a higher altitude (which reduces effectiveness) or place very expensive aircraft at risk from relatively cheap air defenses.[172] While the potential for these weapons to threaten near-future US aircraft like the F-35 is probably overstated, in general it is cheaper to build extensive air defenses than it is to acquire the capability to suppress them. In a similar way, sea-skimming cruise missiles offer a cost-effective counter to US naval superiority by either forcing the ships to stay far offshore (where carrier-based aircraft are no longer useful) or risk destruction by much cheaper missiles.[173] Submarines are another cost-effective counter to US naval superiority, because cheap diesel-electric submarines are difficult to detect in littoral waters where US ships will need to go if they are to be of use during a conflict.[174] The net impact of these developments is that US conventional superiority is increasingly under threat in key regions like the South China Sea.

Conclusion

The strain on the US military resulting from Afghanistan and Iraq is related to the age-old tradeoff between quantity and quality, which is driven by inherent limitations on the resources that can be allocated to national defense.[175] Military power is a function of both, so excessive focus on either will compromise the whole. Quantity is particularly important for long wars,[176] which is exactly why operations in Afghanistan and Iraq put the Army and Marines under so much strain. Therefore, as former secretary of defense Robert Gates notes, the United States may have reached the point of diminishing returns for focus on qualitative superiority.[177]

The lack of sufficient forces in Iraq led directly to the post-invasion problems the United States experienced there.[178] We are seeing a similar dynamic take hold in Afghanistan, because even with the extra surge forces, the United States and its NATO allies lack enough troops on the ground to adequately police the entire country. Relying on Afghan forces is not a solution, because their level of training is much lower and the threat of Taliban infiltration is too high. This is an example of how technologies reduce personnel requirements for some missions but not for all. In

effect, the attempt to take advantage of the "revolution in military affairs" has resulted in a US military largely unprepared for missions other than high-intensity interstate war.[179] Firepower lethality can be decisive in wars that are "enemy-centric" but not in wars that are "population-centric," because the latter require spreading troops throughout the population.[180] Population-centric wars are precisely what the United States has found itself involved in over the last decade. Failing to better balance US military capabilities with the types of conflict it is likely to get involved in will probably result in similar problems in the future.[181] While it lacks a true peer competitor, the consensus position is that the United States needs to retain the full spectrum of military capabilities so it can carry out any type of mission.[182] Of course, that still leaves the question of priorities, since it is unlikely the United States will be able to excel at every type of conflict at the same time.[183] Unconventional approaches such as insurgency and terrorism are particularly difficult for the United States.[184] Counterinsurgency requires large numbers of costly ground troops, so it puts a large burden on a scarce resource. Terrorism offers US foes the chance to carry out damaging attacks at low cost and is challenging to combat because of the international scope of terrorist networks.[185] It is likely that the United States will find itself in further irregular conflicts,[186] but it still needs to be able to fight a high-intensity conflict against a major foe.

It would be easier to balance these demands if military forces were fungible, but most are not.[187] One possible solution is to establish two separate militaries, one for fighting conventional wars and one for unconventional conflicts and state-building,[188] though it seems unlikely any such plan would be implemented.[189] Barring such a radical step, the next best solution would be to place greater emphasis on factors like cost effectiveness and support requirements when new equipment is evaluated. Doing so offers the greatest potential for expanding US combat forces without increasing the defense budget, as discussed above. This approach may actually enhance US capabilities to fight a major war, if necessary, since it will provide more combat forces, and US technological advantages are already so large that cutting-edge equipment is probably not necessary to maintain conventional superiority.

The United States is a great power with interests around the globe and a tendency toward liberal interventionism.[190] It has a military quite capable of defending against any conventional threat that is likely to manifest for decades to come. However, barring a fundamental change in the way the

US military is staffed and equipped, periods of military overstretch are likely to recur whenever there is an increase in the operational tempo. As technological change continues, overstretch may even become the normal state of affairs. On the plus side, the conventional dominance of the United States and the inability of any other state to challenge it may help keep the international system relatively peaceful. If so, that may be an unexpectedly good side effect of American technological optimism. SSQ

Notes

1. Paul Richter, "As Campaign Intensifies, U.S. Feels Strain," *Los Angeles Times*, 14 April 1999.
2. Frederick W. Kagan, "The U.S. Military's Manpower Crisis," *Foreign Affairs* 85, no. 4 (2006).
3. Jeffrey Record, *Bounding the Global War on Terrorism* (Carlisle, PA: Strategic Studies Institute, 2003), 39–40; Max Boot, "The New American Way of War," *Foreign Affairs* 82, no. 4 (2003); and Phillip Carter, "Hollow Force," *Slate.com* (2004), http://www.slate.com/articles/news_and_politics/war_stories/2004/04/hollow_force.html.
4. Defense Business Board, "Task Group Report on Tooth-to-Tail Analysis," 2008; David Isenberg, "Budgeting for Empire: The Effect of Iraq and Afghanistan on Military Forces, Budgets, and Plans," in *Independent Policy Reports* (Oakland, CA: Independent Institute, 2007); Kagan, "U.S. Military's Manpower Crisis"; and Robert Haddick, "This Week at War: General Casey's Doubts," *ForeignPolicy.com*, 2009, http://www.foreignpolicy.com/articles/2009/10/23/general_caseys_doubts.
5. James Hackett, ed., *The Military Balance 2010* (London: Routledge, 2010).
6. Defense Business Board, "Task Group Report."
7. Isenberg, "Budgeting for Empire," 12.
8. Ibid., 13.
9. Kagan, "U.S. Military's Manpower Crisis."
10. Isenberg, "Budgeting for Empire," 13.
11. Lawrence J. Korb and Peter Ogden, "The Army You Have," *Foreign Affairs* 85, no. 6 (2006); and Kagan, "U.S. Military's Manpower Crisis."
12. Robert D. Kaplan, "Center Stage for the Twenty-first Century," *Foreign Affairs* 88, no. 2 (2009).
13. Ibid., 26.
14. "Piracy: No Stopping Them," *Economist*, 3 February 2011; and James Kraska and Brian Wilson, "Somali Piracy: A Nasty Problem, a Web of Responses," *Current History* 108, no. 718 (2009).
15. "Defence Spending in a Time of Austerity," *Economist*, 26 August 2010; and Kaplan, "Center Stage for the Twenty-first Century."
16. Richter, "As Campaign Intensifies."
17. Michael Handel, "Numbers Do Count: The Question of Quality versus Quantity," *Journal of Strategic Studies* 4, no. 3 (1981): 235.
18. Tony Capaccio, "Pentagon's New Bunker-Busters Not for Iran or 'Any One Country,'" *Businessweek*, 21 November 2011.
19. Max Boot describes another "American Way of War" that deals with fighting small wars, though in many of these, the materialist approach to annihilating foes also was present. Boot, *The Savage Wars of Peace: Small Wars and the Rise of American Power* (New York: Basic Books, 2003).
20. F. G. Hoffman, *Decisive Force: The New American Way of War* (Westport, CT: Praeger, 1996), 9; Russell Frank Weigley, *The American Way of War; A History of United States Military*

Strategy and Policy, The Wars of the United States (New York: Macmillan, 1973); Thomas G. Mahnken, *Technology and the American Way of War* (New York: Columbia University Press, 2008), 4; Reuben E. Brigety, *Ethics, Technology, and the American Way of War: Cruise Missiles and US Security Policy*, Contemporary Security Studies (London; New York: Routledge, 2007), 37–38; and Benjamin Buley, *The New American Way of War: Military Culture and the Political Utility of Force*, LSE International Studies (New York: Routledge, 2007), 2. This has been described more broadly as the "Western way of war," though the United States has generally been understood as adopting an extreme form of this preference for decisive battle. Victor Davis Hanson, *The Western Way Of War: Infantry Battle in Classical Greece* (Berkeley: University of California Press, 2000); Hanson, *Carnage and Culture: Landmark Battles in the Rise of Western Power* (New York: Doubleday, 2001); and John Keegan, *A History of Warfare* (New York: Knopf/Random House, 1993).

21. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 77.

22. Antulio Joseph Echevarria, "Toward an American Way of War," (Carlisle, PA: Strategic Studies Institute, 2004).

23. Weigley, *American Way of War*; and Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford, CA: Stanford University Press, 2010), 78–79.

24. Buley, *New American Way of War*, chap 1; and Hoffman, *Decisive Force*, 5.

25. Buley, *New American Way of War,* 49–50.

26. "Culture" can be thought of as "a general state or habit of mind," quoted from Raymond Williams, "Culture and Society," in *Technological Utopianism in American Culture*, ed. Howard P. Segal (Chicago: University of Chicago Press, 1985), 14.

27. Buley, *New American Way of War,* 46–47; and Mahnken, *Technology and the American Way of War*, 5.

28. Keegan, *History of Warfare*, 387; John A. Lynn, *Battle: A History of Combat and Culture* (Boulder, CO: Westview Press, 2003); Hanson, *Western Way of War*; and Hanson, *Carnage and Culture*.

29. Buley, *New American Way of* War; Adamsky, *Culture of Military Innovation*, 68; Mahnken, *Technology and the American Way of War*, 5; and Robert H. Scales Jr., "Culture-Centric WARFARE," *US Naval Institute Proceedings* 130, no. 10 (2004).

30. Geoffrey Parker, *The Military Revolution: Military Innovation and the Rise of the West, 1500–1800* (Cambridge; New York: Cambridge University Press, 1996).

31. Segal, *Technological Utopianism in American Culture*; Buley, *New American Way of War*, 47; Handel, "Numbers Do Count," 227; Adamsky, *Culture of Military Innovation*, 61, 82, 85–87, 91; and Mahnken, *Technology and the American Way of War*, 5.

32. Lawrence Freedman, *The Revolution in Strategic Affairs*, Adelphi paper, (London; New York: Oxford University Press, 1998), 15–16; Keith L. Shimko, *The Iraq Wars and America's Military Revolution* (New York: Cambridge University Press, 2010), 32–35; Handel, "Numbers Do Count," 227–28; Brigety, *Ethics, Technology, and the American Way of War*, 1–4, 38–39, 52; Adamsky, *Culture of Military Innovation*, 86; Mahnken, *Technology and the American Way of War*, 5, 9, 63, 65–67, 123–24; and Rod Thornton, *Asymmetric Warfare: Threat And Response in the Twenty-First Century* (Cambridge; Malden, MA: Polity Press, 2007), 9.

33. Christian Caryl, "Life by a Thousand Cuts," *ForeignPolicy.com*, 7 July 2010, www.foreignpolicy.com/articles/2010/07/07/life_by_a_thousand_cuts; and Adamsky, *Culture of Military Innovation*, 91.

34. Mahnken, *Technology and the American Way of War*, 27–50.

35. Ibid., 62–88.

36. Buley, *New American Way of War*, 41, 54–58.

37. Mahnken, *Technology and the American Way of War*, 65–72.
38. Ibid., 89.
39. Ibid., 91–93.
40. Ibid., 102–3.
41. Ibid., 107–10.
42. Ibid., 113–17.
43. Ibid., 118; and Hoffman, *Decisive Force*, xi.
44. Buley, *New American Way of War*, 72–73, 77; and Shimko, *Iraq Wars and America's Military Revolution*, 32–33.
45. Mahnken, *Technology and the American Way of War*, 122–24; Adamsky, *Culture of Military Innovation*; and Shimko, *Iraq Wars and America's Military Revolution*, 35–36.
46. Mahnken, *Technology and the American Way of War*, 157, 75; Adamsky, *Culture of Military Innovation*, 74–75; and Shimko, *Iraq Wars and America's Military Revolution*, 171.
47. Mahnken, *Technology and the American Way of War*, 157–73; and Shimko, *Iraq Wars and America's Military Revolution,* 40–45, 108.
48. Mahnken, *Technology and the American Way of War*, 179–88.
49. Quoted in Buley, *New American Way of War,* 3.
50. Ibid., 96.
51. Ibid., 85; and Shimko, *Iraq Wars and America's Military Revolution*, 134.
52. Buley, *New American Way of War*, 85–88, 97.
53. Ibid., 107–10.
54. See Boot, "New American Way of War."
55. Mahnken, *Technology and the American Way of War*, 6–7; and Adamsky, *Culture of Military Innovation*, 86.
56. Mahnken, *Technology and the American Way of War*, 9; and Adamsky, *Culture of Military Innovation*, 86.
57. Ibid.
58. Mahnken, *Technology and the American Way of War*, 8.
59. Ibid; and Adamsky, *Culture of Military Innovation*, 86.
60. Handel, "Numbers Do Count," 229; Philip Pugh, *The Cost of Seapower: The Influence of Money on Naval Affairs From 1815 to the Present Day* (London: Conway Maritime Press, 1986), 31, 143; Norman R. Augustine, *Augustine's Laws and Major System Development Programs*, rev. & enl. ed. (New York: American Institute of Aeronautics and Astronautics, 1983), 53–59; and Shaun Waterman, "Why the U.S. Can't Afford Its military," *UPI.com,* 2009, http://www.upi.com/Top_News/Special/2009/02/11/Why-the-US-cant-afford-its-military/UPI-27741234368622/.
61. Moore's Law states that the number of integrated circuits that can be put on a single chip doubles about every two years, which makes computers more powerful and, more to the point, cheaper over time.
62. "Defence Spending in a Time of Austerity."
63. Handel, "Numbers Do Count," 228; Pugh, *Cost of Seapower*, 143, 258; Augustine, *Augustine's Laws*, 44; and Waterman, "Why the U.S. Can't Afford Its Military."
64. Pugh, *Cost of Seapower,* 144.
65. Kagan, "U.S. Military's Manpower Crisis."
66. Augustine, *Augustine's Laws*, 14, 23.
67. Handel, "Numbers Do Count," 228.
68. Pugh, *Cost of Seapower*, 252.
69. Handel, "Numbers Do Count," 229.
70. Augustine, *Augustine's Laws*, 43–44.

71. Kagan, "U.S. Military's Manpower Crisis."
72. Waterman, "Why the U.S. Can't Afford Its Military."
73. "The Last Manned Fighter," *Economist*, 14 July 2011.
74. Waterman, "Why the U.S. Can't Afford Its Military."
75. "Last Manned Fighter."
76. "The Gold-Plated Hangar Queen Survives," *StrategyPage*, 14 June 2010, http://www.strategypage.com/htmw/htairfo/articles/20100614.aspx.
77. *B-2 Bomber: Cost and Operational Issues* (Washington: General Accounting Office, 1997).
78. "Last Manned Fighter."
79. Ronald O'Rourke, *Navy DDG-51 and DDG-1000 Destroyer Programs: Background and Issues for Congress* (Washington: Congressional Research Service [CRS], 2011), 29.
80. Ibid., 1.
81. Pugh, *Cost of Seapower*, 143–44; and Augustine, *Augustine's Laws*, 53–59.
82. Handel, "Numbers Do Count," 232; "Defence Spending in a Time of Austerity"; and Augustine, *Augustine's Laws*, 44–47, 68–70. Since equipment that is not available for battle has no value, this may reduce the advantage that sophisticated technology provides over simpler but more robust equipment. Handel, "Numbers Do Count," 231.
83. Augustine, *Augustine's Laws*, 70.
84. Carl Conetta and Charles Knight, *The Readiness Crisis of the U.S. Air Force: A Review and Diagnosis* (Cambridge, MA: Commonwealth Institute, 1999).
85. "Last Manned Fighter."
86. "Gold-Plated Hangar Queen Survives."
87. Col James C. Ruehrmund Jr., USAF, retired, and Christopher J. Bowie, *Arsenal of Airpower: USAF Aircraft Inventory 1950–2000* (Washington: Mitchell Institute for Airpower Studies, 2010).
88. Freedman, *Revolution in Strategic Affairs*, 5.
89. Shimko, *Iraq Wars and America's Military Revolution*, 38.
90. Handel, "Numbers Do Count," 229, 44–45; Boot, *War Made New: Technology, Warfare, and the Course of History, 1500 to Today* (New York: Gotham Books, 2006), 431; and Fred Kaplan, "Dumb and Dumber: The U.S. Army Lowers Recruitment Standards . . . Again," *Slate.com*, 2008, http://www.slate.com/articles/news_and_politics/war_stories/2008/01/dumb_and_dumber.html.
91. Shimko, *Iraq Wars and America's Military Revolution*, 32.
92. Craig Whitlock, "Pentagon Asking Congress to Hold Back on Generous Increases in Troop Pay," *Washington Post*, 2010.
93. Robert Haddick, "This Week at War: The Pentagon's Own Private Welfare State," *ForeignPolicy.com*, 2010, http://www.foreignpolicy.com/articles/2010/07/02/this_week_at_war_the_pentagons_own_private_welfare_state.
94. Waterman, "Why the U.S. Can't Afford Its Military."
95. John T. Bennett, "$40B Price Tag for Larger Army," *Defense News*, 15 December 2008.
96. Pugh, *Cost of Seapower*, 285.
97. Handel, "Numbers Do Count," 230–32; and Augustine, *Augustine's Laws*, 44–47, 68–70.
98. Augustine, *Augustine's Laws*, 73.
99. John J. McGrath, *The Other End of the Spear: The Tooth-To-Tail Ratio (T3R) in Modern Military Operations*, Long War Series Occasional Paper (Fort Leavenworth, KS: Combat Studies Institute Press, 2007).
100. Boot, *War Made New*.
101. Scott Gebicke and Samuel Magid, *Lessons from around the World: Benchmarking Performance in Defense* (Pittsburgh, PA: McKinsey and Co., Spring 2010). According to the Defense Manpower Center, the combat troop share of the Army and Marines is approximately 25 percent.

102. Max Boot, "The Struggle to Transform the Military," *Foreign Affairs* 84, no. 2 (2005): 107.

103. Gebicke and Magid, *Lessons from around the World*, 12.

104. McGrath, *Other End of the Spear*.

105. Ibid.

106. Ibid., 64, 81.

107. Buley, *New American Way of War*, 104–5; and P. W. Singer, "Outsourcing War," *Foreign Affairs* 84, no. 2 (2005).

108. Mark Cancian, "Contractors: The New Element of Military Force Structure," *Parameters* 38, no. 3 (2008): 61; and P. W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry*, Cornell Studies in Security Affairs (Ithaca: Cornell University Press, 2003), 16. Many support functions were also shifted to the reserves.

109. Singer, "Outsourcing War," 122–23.

110. Singer, *Corporate Warriors*, 15.

111. Moshe Schwartz, *Department of Defense Contractors in Iraq and Afghanistan: Background and Analysis* (Washington: CRS, 2009); Singer, "Outsourcing War," 122; and Cancian, "Contractors."

112. The real total would be more like 400,000 when the training pipeline is included. Cancian, "Contractors," 73.

113. Ibid.; and Isenberg, "Budgeting for Empire," 17–18. This inability to increase the size of the military and the high demand for particular specialties also led to the use of "stop-loss" to prevent over 50,000 troops from leaving the service by the end of 2005.

114. Martin Feldstein, "The Underfunded Pentagon," *Foreign Affairs* 86, no. 2 (2007); and Kagan, "U.S. Military's Manpower Crisis." Former secretary of defense Robert Gates does not think this is a solution to the problem. Robert M. Gates, "A Balanced Strategy: Reprogramming the Pentagon for a New Age," *Foreign Affairs* 88, no. 1 (2009).

115. Kagan, "U.S. Military's Manpower Crisis"; and Feldstein, "Underfunded Pentagon."

116. Feldstein, "Underfunded Pentagon."

117. Pugh, *Cost of Seapower*, 258.

118. Office of the Undersecretary of Defense (Comptroller), "National Defense Budget Estimates for FY-2012," (Washington: DoD, 2011), 217.

119. David W. Barno, Nora Bensahel, and Travis Sharp, "You Can't Have It All," *ForeignPolicy.com*, 2012, www.foreignpolicy.com/articles/2012/01/06/you_cant_have_it_all; Gordon Adams, "Winning the Battle, Losing the War," *ForeignPolicy.com*, 2011, www.foreignpolicy.com/articles/2011/02/15/winning_the_battle_losing_the_war; Fred Kaplan, "Obama's Pentagon Budget Cuts: Panetta's Defense Department Cuts Are Surprisingly Modest," *Slate.com* 2012, http://www.slate.com/articles/news_and_politics/war_stories/2012/01/obama_s_pentagon_budget_cuts_panetta_s_defense_department_cuts_are_surprisingly_modest_.html; and Robert Haddick, "This Week at War: Winners and Losers of the Defense Budget," *ForeignPolicy.com*, 2012, http://www.foreignpolicy.com/articles/2012/01/27/this_week_at_war_winners_and_losers_of_the_defense_budget?page=0,1.

120. Korb and Ogden, "Army You Have"; and Gordon Adams and Matthew Leatherman, "A Leaner and Meaner Defense," *Foreign Affairs* 90, no. 1 (2011).

121. Caryl, "Life by a Thousand Cuts."

122. Fred Kaplan, "2013 Pentagon Budget: Why So Much Spending on Big-War Weapons?" *Slate.com*, 2012, http://www.slate.com/articles/news_and_politics/war_stories/2012/02/_2013_pentagon_budget_why_so_much_spending_on_big_war_weapons_.html.

123. Fred Kaplan, "The Army's Next Big Fight," *Slate.com*, 2011, http://www.slate.com/articles/news_and_politics/war_stories/2011/07/the_armys_next_big_fight.html.

124. Kagan, "U.S. Military's Manpower Crisis"; and Mark Thompson, "How to Save a Trillion Dollars," *Time*, 14 April 2011.

125. Whitlock, "Pentagon Asking Congress to Hold Back"; and Haddick, "Pentagon's Own Private Welfare State."

126. Whitlock, "Pentagon Asking Congress to Hold Back."

127. Waterman, "Why the U.S. Can't Afford Its Military"; Whitlock, "Pentagon Asking Congress to Hold Back"; Haddick, "Pentagon's Own Private Welfare State"; and Isenberg, "Budgeting for Empire," 14, 16.

128. Kaplan, "2013 Pentagon Budget"; Kaplan, "Obama's Pentagon Budget Cuts"; and Haddick, "Winners and Losers."

129. Gates, "Balanced Strategy."

130. Augustine, *Augustine's Laws*.

131. "Air Power on the Cheap," *Economist*, 20 September 2010.

132. Pugh, *Cost of Seapower*, 328.

133. Buley, *New American Way of War*, 50.

134. Gates, "Balanced Strategy."

135. Caryl, "Life by a Thousand Cuts."

136. Ibid; and Thompson, "How to Save a Trillion Dollars."

137. Gebicke and Magid, "Lessons from around the World," 10.

138. Haddick, "Winners and Losers."

139. Boot, "New American Way of War."

140. Kaplan, "2013 Pentagon Budget"; and Haddick, "Winners and Losers."

141. Haddick, "Winners and Losers."

142. Robert Haddick, "This Week at War: Star Wars in the Age of Obama," *ForeignPolicy.com* (2010), http://www.foreignpolicy.com/articles/2010/04/30/this_week_at_war_star_wars_in_the_age_of_obama?hidecomments=yes.

143. Haddick, "Winners and Losers."

144. O'Rourke, "Navy DDG-51 and DDG-1000 Destroyer Programs"; David Axe, "How the Navy's Warship of the Future Ran Aground," *Wired Danger Room*, 3 August 2011; and Nathan Hodge, "Navy Weighs Ship's Design, along with its Own Future," *Wall Street Journal–Eastern Edition*, 2010.

145. "Magic Bullets," *Economist*, 14 January 2012.

146. "Frying Tonight," *Economist*, 15 October 2011.

147. "Unmanned Aerial Warfare: Flight of the Drones," *Economist*. 6 October 2011.

148. P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (New York: Penguin Press, 2009), 33; and Brian Mockenhaupt, "We've Seen the Future, and It's Un-Manned," *Esquire* 152, no. 5 (2009).

149. Singer, *Wired for War*, 33–37; and Mockenhaupt, "We've Seen the Future."

150. Singer, *Wired for War*, 109–22; and P. W. Singer, "We, Robot," *Slate.com*, 2010, http://www.slate.com/articles/news_and_politics/war_stories/2010/05/we_robot.html.

151. Mockenhaupt, "We've Seen the Future."

152. Singer, "We, Robot."

153. Micah Zenko, "10 Things You Didn't Know About Drones," *Foreign Policy* 192 (27 February 2012).

154. Shimko, *Iraq Wars and America's Military Revolution*, 220–21.

155. "Defence Spending in a Time of Austerity."

156. Ibid.

157. Gebicke and Magid, "Lessons from around the World."

158. Gates, "Balanced Strategy."

159. Vladimir Putin, "Being Strong," *ForeignPolicy.com* (2012), http://www.foreignpolicy.com/articles/2012/02/21/being_strong; and Fred Weir, "With Russia's $650 Billion Rearmament Plan, the Bear Sharpens its Teeth," *Christian Science Monitor*, 28 February 2011.

160. Boot, *War Made New*.

161. Michael Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, NJ: Princeton University Press, 2010), 30–39.

162. Neither of these technologies fundamentally changes the nature of warfare, but they still require skilled personnel to use effectively. Ibid., 218–20.

163. See Shimko, *Iraq Wars and America's Military Revolution*.

164. William Wan and Peter Finn, "Global Race on to Match U.S. Drone Capabilities," *Washington Post*, 4 July 2011.

165. Horowitz, *Diffusion of Military Power*, 222.

166. Shimko, *Iraq Wars and America's Military Revolution*, 218–19, 21; Gates, "Balanced Strategy"; Thornton, *Asymmetric Warfare*; Simon Murden, *The Problem of Force: Grappling with the Global Battlefield* (Boulder, CO: Lynne Rienner Publishers, 2009), 15; and Horowitz, *Diffusion of Military Power*, 222.

167. Boot, *War Made New*, 431; and Thomas L. McNaugher, "The Real Meaning of Military Transformation," *Foreign Affairs* 86, no. 1 (2007).

168. Andrew F. Krepinevich, "Get Ready for the Democratization of Destruction," *Foreign Policy* 188 (2011); Boot, *War Made New*; Gates, "Balanced Strategy"; Thornton, *Asymmetric Warfare*, 53–77; and Krepinevich, "The Pentagon's Wasting Assets," *Foreign Affairs* 88, no. 4 (2009).

169. Gates, "Balanced Strategy"; Thornton, *Asymmetric Warfare*, 15; Krepinevich, "Get Ready"; and Feldstein, "Underfunded Pentagon."

170. Boot, *War Made New*, 431–34; David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford; New York: Oxford University Press, 2009), 22–23; Thornton, *Asymmetric Warfare*, 29–33; Krepinevich, "Pentagon's Wasting Assets," 24; and Krepinevich, "Get Ready."

171. Thornton, *Asymmetric Warfare*, 128–33, 37–40.

172. Ibid., 80–83.

173. Ibid., 107–9; Krepinevich, "Pentagon's Wasting Assets," 20–21; and Krepinevich, "Get Ready."

174. Thornton, *Asymmetric Warfare*, 111–13; and Krepinevich, "Pentagon's Wasting Assets," 20–21.

175. Handel, "Numbers Do Count"; and Michael Moodie, *The Dreadful Fury: Advanced Military Technology and the Atlantic Alliance* (New York: Praeger, 1989), 38.

176. Ibid., 226–27.

177. Gates, "Balanced Strategy."

178. Shimko, *Iraq Wars and America's Military Revolution*, 200; Buley, *New American Way of War*, 123–24; Kagan, "U.S. Military's Manpower Crisis"; and Feldstein, "Underfunded Pentagon."

179. Shimko, *Iraq Wars and America's Military Revolution*, 201, 203.

180. Ibid., 209; Buley, *New American Way of War*, 128–29; Boot, "Struggle to Transform the Military," 104; and Korb and Ogden, "Army You Have."

181. Shimko, *Iraq Wars and America's Military Revolution*, 224–25.

182. Ibid., 223; Gates, "Balanced Strategy"; and Andrew F. Krepinevich, "The Future of U.S. Ground Forces," Testimony before Senate Armed Services Committee, 26 March 2009.

183. Shimko, *Iraq Wars and America's Military Revolution,* 224–26.

184. Kilcullen, *Accidental Guerrilla*.

185. Martin Van Creveld, *The Transformation of War* (New York: Free Press, 1991); Moises Naim, "The Five Wars of Globalization," *Foreign Policy* 134 (2003); Kilcullen, *Accidental Guerrilla*, 25–26; Stephen D. Krasner, "Sharing Sovereignty," *International Security* 29, no. 2 (2004); Rupert

Smith, *The Utility Of Force: The Art Of War in the Modern World* (New York: Knopf, 2007); and Thornton, *Asymmetric Warfare*, 29–33.

186. Smith, *Utility Of Force*; Buley, *New American Way of War*, 143–44; Van Creveld, *Transformation of War*; Boot, "Struggle to Transform the Military"; and Krepinevich, "Future of U.S. Ground Forces."

187. Shimko, *Iraq Wars and America's Military Revolution*, 226–29.

188. Thomas P. M. Barnett, *The Pentagon's New Map: War and Peace in the Twenty-First Century* (New York: G. P. Putnam's Sons, 2004); and Shimko, *Iraq Wars and America's Military Revolution*, 230–31.

189. In July 2006, Undersecretary of Defense for Personnel and Readiness David S. C. Chu suggested another alternative which amounted to establishing an American foreign legion that would gain recruits by offering a path to citizenship. Isenberg, "Budgeting for Empire," 19.

190. Murden, *Problem of Force*, 11–12.

Virtual Patriots and a New American Cyber Strategy

Changing the Zero-Sum Game

Matthew Crosston

Most analyses on cyber deterrence draw a sharp distinction between the operational philosophy of the United States and that of authoritarian states like China and Russia. On the whole, they describe the difficulty of US efforts to maintain an effective cyber defense against brazenly offensive Chinese and Russian threats. This analysis takes an important contrarian position on this issue which has been relatively ignored: the cyber philosophy of China might offer the United States some useful insights. China's approach is more effective in ways that, for now, are apparently antithetical to the United States—amoral, overt, and proactive.

Whether Russian cyber nationalists or the Chinese Honkers Union, their guiding principles are clear: they are willing to defend their homeland through assertive and invasive techniques and will not limit their focus to defensive capabilities that only unevenly deter attacks. When defending the state from any perceived enemies—whether state, substate, or nonstate—establishing an offensive capability that instills fear is clearly a main agenda item within Russia and China. Part of this is based on their insecurities about a perceived kinetic imbalance with the United States and a willingness to be morally flexible when it comes to cyber-war norms. Arguably, the United States does not adopt a similar approach because of an apparent reluctance to mimic the policy of such distasteful regimes and an arrogance that does not concern itself with asymmetry. These stances undermine US national security.

First, for clarification, it is necessary to parse out the so-called rogue cyber behavior of China and Russia. There are significant differences in the manner and philosophy with which the two states approach their

---

Dr. Matthew Crosston is the Miller Endowed Chair for Industrial and International Security and founder and director of the International Security and Intelligence Studies (ISIS) program at Bellevue University. He has authored two books, several book chapters, and nearly a dozen peer-reviewed articles on counterterrorism, corruption, democratization, radical Islam, and cyber deterrence.

cyber activities. China is seen as having a more "learnable" model that should creatively inspire the United States to alter and evolve its own cyber strategy to a level that would subsequently surpass the Chinese approach. Importantly, the purpose is not to copy Chinese cyber policy exactly, but rather to transform the characteristic of overt transparency into a US strategy of proactive cyber capability. This would infuse US security with a complex but capable new influence calculus where strategically overt means are used to further positive deterrence ends.

Ideally, this overt cyber strategy would create credibility in virtual weapons which employ disruptive cascading effects so powerful as to negate their use. The key would be in establishing plausible fear in the adversary. Some might argue there is limited utility in this approach because of the possibility that both China and Russia would fail to recognize the power of such a posture. Such logic subsequently declares virtual weapons do not have the same credibility as, say, nuclear weapons because the former have not achieved that level of credibility through actual usage or even testing. The efficacy evolution in cyber weaponry, however, helps support the main argument here. Given the recent revelations about Stuxnet and the effectiveness of the Duqu and Flame viruses—which quite possibly moved beyond the capabilities of Stuxnet—cyber weapons are rapidly obtaining that fearful reputation, and thus, deterrence via overt cyber strategy can no longer be considered pure fantasy.

This influence calculus turns current conventional wisdom on constraining norms within *jus in cyber bello* on its head. To date these constraints have shunned an overtly proactive US cyber strategy. A greater likelihood for peace across the global virtual commons is possible by using a strategy of facilitating restraint through fear. Please note, however, that *amoral* and *unethical* are not freely interchangeable in this analysis. For example, the Chinese may not view their cyber stances as unethical, while the United States does. The classically Machiavellian argument is that deep reflective discussions about morals and ethics should be suspended from the cyber domain if effective deterrence is to be achieved through overt strategy.

Finally, a cautious caveat: this is not an entreaty to abandon covert activities or secrecy. Rather, it is an important balancing argument for developing a fully encompassing strategy that allows both covert *and* overt US cyber power—an important evolution. It is not an argument against the need for classified operations. Simply, cyber strategy must be decoupled from a de facto zero-sum game. The building and elevating of

overt cyber preemption does not take away from the relevance and reach of US covert cyber reactionary powers.

China and Russia: Cyber Cousins—Not Cyber Brothers

There seems to be a strong divergence in perception regarding China's desire to command cyberspace offensively. On the one hand is the assumption that this is a natural manifestation of its growing desire to achieve global superpower status. On the other hand is the counterargument that emphasizes China's own perception of its inability to operate effectively against the United States in a conventional military confrontation. Indeed, many Chinese writings suggest cyber warfare is considered an obvious asymmetric instrument for balancing overwhelming US power.[1] This latter argument is more compelling based on these stark military realities:

- In overall military spending, the United States spends between five and 10 times as much per year as China.
- Chinese forces are only now beginning to modernize. Just one-quarter of its naval surface fleet is considered modern in electronics, engines, and weaponry.
- In certain categories of weaponry, the Chinese do not compete. For instance, the US Navy has 11 nuclear-powered aircraft carrier battle groups. The Chinese navy only recently launched its first carrier, a refurbished Russian ship used solely for training.[2]
- In terms of military effectiveness (i.e., logistics, training, readiness), the difference between Chinese and US standards is not a gap but a chasm. The Chinese military took days to reach survivors after the devastating Sichuan earthquake in May of 2008 because it had so few helicopters and emergency vehicles.[3]

With this state of military affairs, China's perception of insecurity is not surprising. Even more logical is the Chinese resolve to grow its asymmetric cyber capabilities: such attacks are usually inexpensive and exceedingly difficult to precisely attribute. Attribution becomes even more complex for states where cyber attacks can be "launched" from neutral or allied countries.[4]

Given an authoritarian state's capacity for paranoia, it is illogical for China not to develop its offensive cyber capabilities. In this case, the weak conventional military strength is quite real. To that end, the People's

Republic has endeavored to create its own set of lopsided military advantages in the cyber domain. To wit:

- The Pentagon's annual assessment of Chinese military strength determined in 2009 that the People's Liberation Army (PLA) had established information warfare units to develop viruses to attack enemy computer systems and networks.
- The PLA has created a number of uniformed cyber warfare units, including the Technology Reconnaissance Department and the Electronic Countermeasures and Radar Department. These cyber units are engaged on a daily basis in developing and deploying a range of offensive cyber and information weapons.
- China is believed to be engaged in lacing the network-dependent US infrastructure with malicious code known as "logic bombs."[5]

The official newspaper of the PRC, the *Liberation Army Daily*, confirmed China's insecurity about potential confrontation with the United States in June 2011. The Chinese government proclaimed that "the US military is hastening to seize the commanding military heights on the Internet. . . . Their actions remind us that to protect the nation's Internet security we must accelerate Internet defense development and accelerate steps to make a strong Internet Army."[6] Clearly, the Chinese have sought to maximize their technological capacity in response to kinetic realities. This is not to say the United States is therefore guaranteed to be in an inferior position (information about US virtual capabilities at the moment remains largely classified), but the overt investment, recruitment, and development of Chinese virtual capabilities presents opportunities the United States should also be willing to entertain.

How does all of this compare and contrast with the Russian approach to the cyber domain? Anyone studying cyber conflict over the last five years is well aware of Russia's apparent willingness to engage in cyber offensives. The 2007 incident in which the Estonian government was attacked and the 2008 war with Georgia are universally considered examples of Russian cyber technology as the tip of their military spear. While it is true Russia actively encourages what has come to be known as "hacktivism" and lauds "patriotic nationalist" cyber vigilantism as part of one's "civic duty," there are still distinct differences with China.[7]

Much of Russia's cyber activity, when not in an open conflict, seems to be of the criminal variety and not necessarily tied directly into the state.

Indeed, Russia seems to utilize organized crime groups as a cyber conduit when necessary and then backs away, allowing said groups continued commercial domination. Russia, therefore, almost acts as a rentier state with criminal groups: cyber weapons are the natural resource, and the Russian government is the number one consumer. This produces a different structure, style, and governance model when compared to China.

Table 1. Parsing cyber rogues

Category Breakdown	China	Russia
Purpose	Protectionist	Predatory
Psychology	Long-term/Rational	Short-term/Cynical
Style	Strategic	Anarchic
Governance Model	State-centric	Crimino-Bureaucratic

Purpose

China's purpose in developing its cyber capability seems motivated by protectionist instincts based largely on the perception that it is not able to defend itself against the United States in a straight conventional military conflict. Russia's purpose seems utterly predatory. This is no doubt influenced by the fact that most of the power dominating cyber capability in the Russian Federation is organized and controlled by criminal groups, sometimes independently and sometimes in conjunction with governmental oversight.

Psychology

The operational mind-set of China seems to be both long-term and rational. Its strategies are based on future strategic objectives and its position within the global community. Most if not all of China's goals in the cyber domain can be clearly understood in terms of rational self-interest. Russia's cyber mind-set is dominated by short-term thinking, largely motivated by the pursuit of massive profit and wielding of inequitable political power. Analyzing just how much of Russian cyber activity is in fact controlled by the desire for wealth leads to an overall impression of state cynicism.

Style

Chinese cyber activity is strategic in style. The state strives to control the cyber environment and maintain influence over all groups in the interest

of the state. The Russian cyber atmosphere, unfortunately, resembles anarchy. The state engages criminal groups through an authority structure that is blurred if even existent. Consequently, there is little confidence that the Russian government exclusively controls its cyber environment.

Governance Model

It is clear that China's cyber governance model is state-centric. This may not be ideal for democracy, but it shows China does not allow competing authorities or shadow power structures to interfere with its national interests. Russia's cyber governance model is crimino-bureaucratic. It is not so much that the state is completely absent from the cyber domain in Russia, but rather the ambiguity of power and authority define the cyber domain. Russia may enjoy claiming the allegiance of its patriotic nationalist hackers, but it does not in fact tightly control its own cyber netizens, at least not in comparison to China.

While neither Russia nor China is afraid to use offensive cyber weapons, there are dramatic structural, motivational, strategic, and philosophical differences. Russia seems to embody a criminal-governmental fusion that has permeated the entire state apparatus. The cyber domain there is used for temporary forays to achieve state objectives and then returns to more permanent criminal projects. As such, it is not truly state-controlled, is relatively anarchic, and cannot establish any deterring equilibrium. China, on the other hand, may be the first state to truly embrace the importance of tech-war; it has realistically assessed its own kinetic shortcomings and looked to cyber for compensation. In short, it has fused Sun Tzu with Machiavelli—better to quietly overcome an adversary's plans than to try to loudly overcome his armies.

This analysis paints Russia in a relatively stark strategic light. While these differences do not give rise to a trusted alliance with China, the manner in which it approaches its cyber domain presents interesting new ideas about how the United States should approach the global cyber commons. These ideas would be in contrast to both academic literature and journalism, as they offer two completely divergent responses. On the one hand, the United States is not appropriately meeting this challenge, and on the other hand, it remains second-to-none in cyber offense.

The United States invests heavily in cyber security, and members of the intelligence community work to create cyber weapons meant to preserve US military predominance. However, there are still missed opportunities

and weaknesses that have not been addressed or overcome by covert strategy. Namely, emphasizing covert and opaque cyber initiatives hinders the emergence of a global cyber strategy that could compel constraint without actually engaging in cyber attacks. Recall this is not about developing overt at the expense of covert. Rather, it is about ending the zero-sum cyber game to the strategic benefit of the United States. Up to now American virtual patriots have not been used for maximum impact and effectiveness. It would be wise to position offensive cyber capabilities for strategic, overt, preemptive purposes rather than as solely logistical, covert, reactionary weapons. This is a dramatic shift in strategic mind-set, arguing for a yin-yang approach toward the covert and overt aspects of cyber rather than the present view as a zero-sum game.

New Technology but not New Thinking

In 2004, the Congressional Research Service (CRS) issued a report on information warfare and cyber war. It discussed public policy oversight issues Congress should consider, including whether the United States should

- encourage or discourage international arms control for cyberweapons, as other nations increase their cyber capabilities;
- modify US cyber-crime legislation to conform to international agreements that make it easier to track and find cyber attackers;
- engage in covert psychological operations affecting audiences within friendly nations;
- encourage or discourage the US military to rely on the civilian commercial infrastructure to support part of its communications, despite vulnerabilities to threats from possible high-altitude electromagnetic pulse (HEMP) or cyber attack;
- create new regulation to hasten improvements to computer security for the nation's privately-owned critical infrastructure; or
- prepare for possible legal issues should the effects of offensive US military cyberweapons or electromagnetic pulse weapons spread to accidentally disable critical civilian computer systems or disrupt systems located in other non-combatant countries.[8]

The CRS analysis focused on existing physical infrastructure and capacity. It did not explore new theoretical concepts that might achieve national interest more effectively. Most striking is the apparent assumption that the cyber domain will worsen in terms of political environment, as seen by the overreliance on cyber defensive systems. Such emphasis renders the US position reactive and late. The argument made here is for also pushing overt strategies based on devastating offensive capabilies that shift the US position into being more proactive, like China. Reactive policy simply *responds* to cyber attacks. Overt policy seeks to *deter* them.

The same CRS report highlighted the need for the Department of Defense (DoD) to achieve both decision and information superiority. This means a competitive advantage in the cognitive realm and one that enables the military to surprise an enemy.[9] Both of these advantages are best achieved with added frontend capability and not solely accomplished by reactionary policies. In short, there can be no dominant operational transfiguration without first a profound strategic transformation. An overt cyber strategy upfront makes proactive deterrence through fear more probable and gives the perception of decision and information superiority. Broadening the discussion to embrace a change in strategic mind-set greatly expands new potential deployment and deterrence options.

Many agencies within the US government have come close to espousing this transformation, only to fall short by demanding that US cyber capabilities remain exclusively covert. The National Security Agency has argued to better defend information networks by openly engaging both allies and adversaries in an open forum.[10] The Pentagon believes strongly in "active defense," which is quite simply, cyber offense. The problem is that both remain strategically focused on *responding* to a major cyber attack through covert means. In other words, the same flaw found in the CRS report nearly a decade earlier still applies; the limited innovation remains reactive. If the United States continues to view the overt and covert aspects of cyber strategy as a zero-sum game rather than as yin-yang symmetry, then it will fail to realize its true cyber dominance.

A more disconcerting aspect of the discussion—at least for those who envision the cyber domain as a venue for instigating deterrence, not provocation—is that a capability used exclusively for covert activity becomes just another weapon among weapons. The point of maintaining total secrecy is due to the lethality of actual deployment. Any preemptive deterring power, therefore, is lost when kept covert. Remember, the argument

here is not to abandon secrecy altogether; it is not about showing all the cards but voluntarily revealing some cards for strategic purposes. If the desire is to expand a capability's impact, not just in terms of winning wars but in preventing them, then overt strategy is a valuable tool.

Recall where Chinese cyber policy found its fundamental motivation: China's original intent was to deter other nations from pursuing more-traditional coercive policies. It also wanted to develop an advanced cyber warfare capacity that would allow it to asymmetrically challenge any potential adversary.[11] One must see Chinese cyber offensive strategy as a rational solution that is not simply cheap, but potentially capable of giving the United States pause before a large-scale conventional military engagement.[12] This kind of policy in US hands, focused by an overt offensive strategy, could transcend national interests and provide a framework for achieving greater cyber restraint at the global level. Keeping the aforementioned influence calculus in mind, it elevates above Chinese parochialism for the greater, more responsible global good of overt US cyber dominance.

Note this is not an entreaty to copy or mimic Chinese cyber policy. China itself does not formally admit to an explicitly overt strategic policy over the cyber domain. It is, however, undoubtedly proactive and offensive. By strategically allowing general knowledge about the existence of an offensive program and spreading the perception that it is willing to proactively use it, the United States has the opportunity to increase the fear-hesitancy of potential adversaries beforehand. In other words, adopting China's proactive policy and mutating it into something more overt and explicit (combined with superior US technological innovation and rule of law) can expand US cyber capability beyond its current covert, reactive roles. This is not an argument to disband covert action or remove reactive capacity. Rather, it is an admission that these two latter spheres simply do not equip the United States with an effective deterring cyber capability. Adding a proactive, offensive, overt "third strategic wheel" to this domain might do so.

The importance of this issue was confirmed by the head of US Cyber Command, Gen Keith Alexander, testifying before the House Armed Services Committee's Subcommittee on Emerging Threats and Capabilities in 2011:

> We believe that state actors have developed cyber weapons to cripple infrastructure targets in ways tantamount to kinetic assaults; some of these weapons could potentially destroy hardware as well as data and software. The possibilities for

> destructive cyber effects, having long been mostly theoretical, have now been produced outside of the lab and are proliferating into national arsenals and possibly beyond. . . . Segments of our nation's critical infrastructure are not prepared to handle this kind of threat.[13]

For those aware of the innate difficulty of cyber deterrence reactively keeping ahead of cyber attacks, this confession from General Alexander only makes it more compelling to allow discussion of a new overt mind-set in US cyber strategy that strives to prevent these deadly new weapons from being used. In some ways Alexander is close to this very conclusion but misses the final connection:

> We see frequent media reports on nations contemplating the creation of their own cyber commands. . . . *There is a rough, de facto deterrence at the strategic level of cyberspace. Although no one knows how a cyberwar would play out, even the most capable state actors seem to recognize that it is in no one's interest to find out the hard way.* This concern has led to a certain degree of restraint by states that we deem capable of causing very serious cyber effects (emphasis added).[14]

In developing offensive cyber weapons for overt strategic use, states make it known how devastating and cost-punitive a potential cyber strike would be. In essence, it is simply adjusting the general's vision—by making the costs of cyber war overtly explicit, it becomes every state's self-interest to engage in cyber restraint. Alexander intimates that such restraint has already developed to a certain degree because of the unknown fear (but clearly perceived assumption) that an all-out cyber war would be disastrous. As such, the most logical path is to try to intensify that perception through overt cyber strategy and thus raise restraint even more. The argument here seeks to answer the "why it matters" question and begin changing the original strategic mind-set. With such an argument in place, it will then be appropriate to broaden and deepen the project into blazing potential "how to" trails. This in fact makes analytical sense; namely, there can be no relevant "game planning" if the strategic state mind-set remains unaltered.

Is US Cyber Command already blazing that trail on its own? When considering the five strategic initiatives below, as detailed by General Alexander, it seems clear that it is not:

1. Treat cyberspace as a domain for the purposes of organizing, training, and equipping, so the DoD can take full advantage of its potential in military, intelligence, and business operations;
2. Employ new defense operating concepts to protect DoD networks and systems;

3. Partner closely with other US governmental departments and agencies and the private sector to enable a whole-of-government strategy and an integrated national approach to cybersecurity;
4. Build robust relationships with US allies and international partners to enable information sharing and strengthen collective security; and
5. Leverage the nation's ingenuity by recruiting and retaining an exceptional cyber work force and enable rapid technological innovation.[15]

There is nothing faulty or inappropriate with the above strategies. The issue is that the United States is not fully considering all the strategies available. US cyber policy remains too wedded to reactive defensive measures. When it considers proactive offensive measures more akin to Chinese strategy, they remain within covert operations. This is fine to facilitate the two goals of USCYBERCOM—to protect US freedom of action in cyberspace and to deny freedom of action in cyberspace to all adversaries—but it is not enough as a holistic strategy to achieve the desired change in the global cyber mind-set, where the use of cyber weapons becomes as abhorrent as using nuclear weapons.

The focus on possible cyber improvements should be strategic. Not all cyber initiatives must be reacted to in kind. Theoretically, it will always be possible to react to a cyber attack with, for example, a drone strike. Logistically, however, such reactions might be worse than the initial action. As such, while answering cyber with cyber should not be considered inevitable and exclusive, it could be the best strategic response in the end. This would be a loose inspiration from the Chinese example, where cyber often seems a preferred initiative over direct military maneuvers.

Perhaps partial explanation for this strategic flaw is that the United States does not have a healthy fear of kinetic asymmetry like China and Russia. Viewing kinetic asymmetry as "everyone else's problem," the United States could actually fall behind other states in terms of innovative cyber strategy. China's concern over conventional asymmetry clearly led to greater investment in proactive and offensive cyber measures. Since the United States does not worry about such asymmetry, it seems stuck on measures that are reactive, covert, and defensive. This overconfidence limits the potential reach and deterrent impact of a new US overt cyber strategy.

Leading cyber states excel at increasing the effectiveness of covert virtual weapons. The United States in fact is the prime leader. But it remains a poor representative in pushing forward an agenda of overt strategic cyber

transparency where cyber becomes more about preemption and deterrence rather than inferior surprise and reaction.

Zero-Sum Game, Part I
The Strategic Power of Overt Transparency

The potential risks in cyberspace have always been on policymakers' minds. The stakes were made clear in the president's *National Cyberspace Policy Review*:

> With the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations . . . and individual rights. The government has a responsibility to address the strategic vulnerabilities to ensure that the US . . . together with the larger community of nations, can realize the full potential of the information technology revolution.[16]

Clearly, a constructive cyber environment—globally expansive in its positive conformity while limiting free riders and violators—is essential. Alas, the drive to create such an environment seems based on idealistic beliefs that do not conform to the real world. As stated by Mikko Hypponen at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn in 2009, "in the end, it is just about good versus evil." The United States will not co-opt through paramilitary structures, like China, nor will it coerce through shadowy criminal networks, like Russia. So how does it motivate global cyber netizens to positive behavior? Apparently, this seems to rest on creating enough trust in states "doing the right thing."[17] Given the counterculture ethos of the cyber domain, this goal seems hyper-idealistic, if not outright irresponsible.

If the choice is between a system of deterrence based on idealistic governmental altruism or on a realist fear of retaliatory punishment and strategic first-strike restraint, the latter (again, loosely inspired by Chinese strategic thinking) is not only more easily achievable but also more effective. It would appear, however, that contemporary conventional wisdom does not agree. This is partially based on an attempt to force just war theory unchanged into the cyber domain and to misread what the rules of strategic cyber deterrence ought to be, as Randall Dipert notes:

> It is also true that Just War Theory, having been endorsed by most industrial democracies and in international law, has acquired the status of damage-minimizing convention. However, the increasing number of nations, especially non-Western ones, who show no serious effort to endorse or follow this convention—and the

> unwillingness of other nations to force compliance—means that the advantage of a widely accepted convention is lost; it merely handicaps nations with the developed public sense of morality and prevents them from moral intervention.[18]

This public sense of morality handicaps well-meaning nations, because they are trying to create compliance on the backend of a process, reactively and covertly, when such compliance is more likely when accompanied by an equal strategy on the frontend, proactively and overtly. Focusing on ethics, morals, and trust to motivate compliance in the cyber domain is irrational at the very least because of how easy it is to attack anonymously. Flipping this process and inverting the motivational stimuli produces a system of compliance independent of goodwill and ethical behavior: not purely defense, but offense; not purely covert, but overt; not purely reactive, but proactive; not hoping to inspire trust, but forcibly compelling fear. The cyber domain is not so different that the guiding principle of international relations cannot apply—fear plus self-interest equals peace. It is simply about realizing that covert and overt cyber activity function best not as zero-sum, but as yin-yang.

This idealistic normative thinking is even more dubious when the limitations of a so-called cyber cold war are supposedly elaborated:

> It is relatively clear what the reasonable (and thus moral) constraints on Cyber Cold War would be. There should be little targeting of strictly defensive computer control systems. There should be no attacks that disable or panic global financial or economic systems. There should be no power interference in the vital economic and security interests of a major power.[19]

These proposed behavioral rules about *jus in cyber bello* are paradoxical: with so many constraints on allowable action, the underlying motivational framework of fear—so essential in the original Cold War in moderating behavior—becomes nonexistent. Indeed, if the above parameters were observed, then a state could arguably be *more* motivated to attack. Remove the civilian population and domestic infrastructure from cyber attack, and you have sanitized cyber war to a point where there is no fear of engagement.

> A Cyber Cold War would be multilateral rather than bilateral: it would involve many nations, with different interests and not allied by treaty. Furthermore, the parties would include major non-governmental players such as private companies or even individuals or groups of individual hackers, perhaps with political interests. It is unlikely, in the more capitalistic and constitutionally free countries, which national governments can easily rein in these potential corporate and individual cyber attackers.[20]

The problem with this formulation is that it envisions a so-called cyber cold war beholden to apparently *voluntary* parameters of constraint. The parameters elaborated, however, do not honor but corrupt the true deterring force that existed in the Cold War. If an overt strategy of credible cyber debilitation were allowed to openly develop, then most of the problems mentioned above would be inconsequential to the proper functioning of the virtual global commons—multilateral or bilateral, individuals or groups, national governments or private corporations, clearly defined adversaries or anonymous, nonattributable attacks. A system that does not rely on arbitrary good behavior and instead proactively establishes overt cyber-weaponization strategies alongside continued covert capabilities creates an environment where the futility of first-strike efficacy and perceived retaliatory devastation reigns in behavior globally.

The United States tends to be obsessive about keeping its technological capabilities classified. This is partially explained by the need to maintain effective surprise in retaliation to an attack rather than striving to prevent an attack initially. Yet, it is also explained by the US attempt to be the leading voice for liberally idealistic global cyber norms. This was confirmed in 2008 when former intelligence official Suzanne Spaulding testified before the House Cybersecurity Subcommittee.

> My concern is that (the Department of Defense) has been so vocal about the development and deployment of [classified] cyber-warfare capabilities that it will be very difficult for that department *to develop and sustain the trust necessary to undertake essential collaboration on defensive cybersecurity efforts* with the private sector and with international stakeholders. . . . There is significant risk that these vital partners will suspect that the collaboration is really aimed at strengthening our offensive arsenal (emphasis added).[21]

There are two problems with the above quote. On the one hand, policymakers continue to focus on apparent voluntary trust in a domain that is not typified by such behavior. On the other hand, the DoD remains steadfast in its worship of clandestine capability and thus loses the preemptive deterrence of overt strategy which can compel cooperation as opposed to just hoping for it. These are not small problems, as trust and collaboration between dangerous actors work when there is an element of consequence to poor action. An overt strategy of offensive cyber capability—revealing some cards while not revealing all, with no nod to ethical considerations that demand targeting constraints and a focus purely on the efficacy of preemptive deterrence—arguably has a chance to shine a light of consequence

into the shadowy anarchy of cyber. This is how the United States, as mentioned at the beginning of this article, could be inspired by the essence of Chinese cyber strategy, but it must ultimately elevate to a higher capability and competence.

Further hindering this evolution, the academic community has remained too enamored with trying to connect ethical theories into the cyber domain to create a liberal, idealistic governing code. Many scholars have acknowledged that these theories, whether utilitarianism, Kantian theory, or natural rights theory, have cast relatively little new light into the cyber domain.[22] Despite such sincere if misguided efforts, the best possibility for preemptive cyber deterrence might be old-school strategic realism and not new-school ethical liberalism.

As awkward as it may be to admit publicly, the Chinese might have something for the United States to truly consider. A fusion of Sun Tzu's pragmatism with Machiavelli's overt strategic amorality carries the potential to deter negative cyber action before it ever begins. As Sun Tzu asserted, the highest realization of warfare is to attack the enemy's plans; next is to attack its alliances; next to attack the army; and the lowest is to attack its fortified cities. Machiavelli made it clear that if an injury has to be done to a man, it should be so severe that his vengeance need not be feared. This overt, amoral offensive fusion has one purpose: not to *logistically* conduct war but to *strategically* avoid it. At the present time there is no current discussion of US cyber strategy broaching these subjects, and subsequently, the zero-sum cyber game remains unchanged.

Zero-Sum Game, Part II
Cyber Domain and International Law: Can Fear Be the Duty to Assist?

Unlike cyber crime, the international community has not achieved an agreed-upon consensus for cyber rules. This leaves existing international law no choice but to try to apply by analogy. While the application is not perfect, there are at least three general prescriptions to state conduct in cyberspace, according to law professor Duncan Hollis.

1. States must not launch a cyber attack that qualifies as a use of force absent UN Security Council authorization or pursuant to a state's inherent right to self-defense.

2. States must not employ cyber attacks within armed conflicts that violate the laws of war. States must avoid cyber attacks that target civilian objects, cause indiscriminate harm, or violate the rights of neutral states.
3. States must respect the sovereignty of other states in responding to any cyber attacks that do not constitute a use of force. . . . States cannot respond to cyber attacks directly if it would interfere with the sovereignty of another state.[23]

The most controversial argument here is the idea to purposely and openly violate the above three precepts, or at least create believability that such violation will occur, to instill the compelling credibility of fear. Such overt strategy can create compliance improvement when considering the duty to assist (DTA), as Hollis suggests, using a rescue-at-sea analogy.

> International law needs a new norm for cybersecurity: a duty to assist, or DTA. . . . As yet, there is no DTA for the Internet. But an SOS for cyberspace, an e-SOS, could both regulate *and* deter the most severe cyber threats. Unlike proscriptive approaches, a DTA would not require attribution to function effectively; those facing harm would not need to know if it came from a cyber-attack, let alone who launched it. A DTA would seek to redress unwanted harms directly, whatever their cause. It would do so by marshaling sufficient resources to avoid or at least mitigate that harm. If it does so effectively, attackers may think twice about whether it is worth the effort to attack at all (emphasis in original).[24]

The overall purpose of the DTA is correct: to deter the worst potential cyber behavior. It is by no means a false deterrence ploy; it is the rightful obligation of states to assist in an investigation not only to help, but also to improve their own trustworthiness and remove suspicion of complicity. The flaw, once again, comes in focusing on the backend of the process, seeking to reactively reduce harm. It uses the terms *deter* and *avoid*, but in actuality the DTA is truly centered on the terms *redress* and *mitigate*. An overt proactive cyber strategy is about deterrence and avoidance, which would make issues of redress and mitigation less necessary.

Hollis wanted to legally establish an e-SOS that would better deter cyber attacks by rendering states more resilient in the face of threats.[25] He is accurate in diagnosing the problem but is unable to connect to truly new strategy because of moralistic hand-wringing that restricts discussion to reactive and defensive measures of mitigation. In other words, the intellectual community has focused so exclusively on the aftermath of an attack that it

basically does not consider the potential promise in overt, proactive strategies that might preempt attacks.

This becomes obvious when considering two concepts used in the law of armed conflict, reflecting the fundamental differentiation between principles that govern the legal decision to use force in international relations (*jus ad bellum*) and conduct/behavior during times of war (*jus in bello*).[26] Trying to seamlessly apply these principles to the cyber domain has proven consistently thorny.

> Both traditional elements of deterrence seem to be considered unsatisfactory for the purposes of cyber deterrence. . . . *Whilst cyber deterrence does not abandon the approach based on influencing potential adversaries' mind-sets, it will most likely have to rely on different methods to achieve this desired effect* (emphasis added).[27]

Changing the strategic mind-set of cyber thinkers requires one to recognize it is easier to leverage influence *before* conflict takes place than *after* hostilities have begun. The flaw is in the failure to connect higher-purpose ethical considerations to a harder strategic core; the argument is not that the United States must *never* consider the parameters and limitations in cyber war once underway. Rather it is about the need to address these concerns by enacting an overt strategy that can prevent cyber attacks. Perhaps one other reason this bridge-building has not been attempted is because of the general consensus that cyber weapons cannot be used for coercive purposes or do not instill fear as easily as nuclear weapons. But in reality, this might not matter.

Cyber Deterrence: Voodoo Magic or Simple Classic Realism?

Although the work of Martin Libicki is extremely well-known among cyber experts, a relatively little-emphasized point in a recent article that discussed the ability (or inability) of cyber war to have strategic impact is crucial here:

> If cyber war is going to assume strategic importance, it must be able to generate effects that are at least comparable to, and preferably more impressive than, those available from conventional warfare. . . . More to the point, for cyber to be a strategic weapon for coercive purposes, it has to be frightening to the population at large, or at least to the leaders—so frightening that the aggressors can actually read some gains from the reaction or concession of their targets. . . . It follows that if the use of cyber weapons is unimpressive at the strategic level, the fear that might come from the *threat* to use cyber weapons may be similarly unimpressive. . . . Nuclear

> arms fostered fear, but there was not a great deal of doubt or uncertainty in their applications. Cyber may be the opposite—incapable of inducing real fear directly, but putatively capable of raising the specter of doubt and uncertainty (emphasis in original).[28]

Libicki is right in how the fundamental debate is framed. So how can a new strategic line of thinking answer some of his concerns? Perhaps the inability of cyber to achieve true strategic importance is not based on its inability to instill fear, but rather the policy community's reluctance to cross the ethical Rubicon and consider a system whose aim is to achieve credibility in using real-time cyber lethality overtly. The goal is not to turn cyber weapons into some sort of voodoo magic. Rather, it is to fuse cyber weapons with classical realism, whether through propaganda or public testing. If the perception of a first cyber strike becomes irrational because of a "proven" retaliatory capability, then Libicki's legitimate concern about the credibility of cyber lethality will be surmounted. Overcoming this concern is essential, as it brings the deterring equilibrium of fear without having to engage in actual cyber war.

With a system that can at times overtly advertise these requisite skills, the United States would no longer need to convince adversaries of its omniscience or magic. Adversaries would only need to believe in rational self-interest that good behavior will avoid debilitation and bad behavior carries severe consequences. Ironic as it may seem, perhaps the key to developing this overt cyber strategy of preemptive deterrence, ensuring more reliable behavior across the virtual commons, comes about by being creatively inspired by an authoritarian state like China and adopting more strategically amoral rules of conduct in cyber war that so far have been relatively forbidden by the American scholarly community.

This is not to say the United States should do away with defensive efforts or covert weapons or cyber spies. Rather, it is an entreaty to allow American virtual patriots to employ offensive cyber capabilities for strategically overt preemptive purposes rather than solely as logistically covert reactionary weapons. This is not an argument against the relevance of the latter, but it is an explanation of how the former might lessen their need. The overt and covert aspects of US cyber strategy are better understood as yin and yang. They are not zero-sum. Change that strategic mind-set in the uniquely American ways discussed here, and US cyber dominance will be unchallenged for a long time to come. SSQ

Notes

1. Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4, no. 2 (Summer 2011): 1–24.
2. China's First Aircraft Carrier Enters Service," *BBC*, 25 September 2012, http://www.bbc.co.uk/news/world-asia-china-19710040.
3. James Fallows, "Cyber Warriors," *Atlantic* 305, no. 2 (March 2010).
4. Gunter Ollman, "Asymmetrical Warfare: Challenges and Strategies for Countering Botnets," in *Proceedings of ICIW 2010: The 5th International Conference on Information-Warfare & Security*, 509–14 (Reading, UK: Academic Conferences International, 2010).
5. George Patterson Manson, "Cyberwar: The United States and China Prepare for the Next Generation of Conflict, *Comparative Strategy* 30 (April–June 2011): 122–33.
6. Don Reisenger, "Chinese Military Warns of US Cyber Threat," *cnet.com*, 16 June 2011, http://news.cnet.com/8301-13506_3-20071553-17/chinese-military-warns-of-u.s-cyberwar-threat.
7. Scott D. Applegate, "Cyber Militias and Political Hackers—Use of Irregular Forces in Cyberwarfare," *Security & Privacy* 9, no. 5 (September/October 2011): 16–22, http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=6029351.
8. Clay Wilson, *Information Warfare and Cyberwar: Capabilities and Related Policy Issues* (Washington: CRS, 19 July 2004), "Summary."
9. Ibid., 3.
10. Fallows, "Cyber Warriors."
11. Manson, "Cyberwar."
12. Hjortdal, "China's Use of Cyber Warfare."
13. Gen Keith Alexander, "Building a New Command in Cyberspace," *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 5.
14. Ibid., 7.
15. Ibid., 8.
16. Quoted in Col James Cook, "Cyberation and Just War Doctrine: A Response to Randall Dipert," *Journal of Military Ethics* 9, no. 4 (December 2010): 411–23.
17. Alexander Klimburg, "Mobilising Cyber Power," *Survival* 53, no. 1 (February/March 2011): 41–60.
18. Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (December 2010): 394.
19. Ibid., 403.
20. Ibid.
21. Suzanne Spaulding, quoted in Shaun Waterman, "US Needs Cyber-offensive," *Space War*, 29 September 2008.
22. Giles Trendle, Cyberwars: The Coming Arab E-Jihad, *Middle East*, issue 322, April 2002.
23. Duncan B. Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal* 52, no. 2 (Summer 2011): 393–95.
24. Ibid., 378.
25. Ibid., 426–29.
26. Ulf Haeussler, "Cyber Strategy and the Law of Armed Conflict," in *Proceedings of ICIW 2011: The 6th International Conference on Information-Warfare & Security*, 99–105 (Reading, UK: Academic Conferences International, 2011).
27. Ibid.
28. Martin Libicki, "Cyberwar as Confidence Game," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 135–37.

Deterring North Korea from Using WMD in Future Conflicts and Crises

Bruce W. Bennett

For nearly 60 years, North Korea has determinedly pursued the development of weapons of mass destruction (WMD), usually defined as chemical, biological, radiological, and nuclear (CBRN) weapons. In recent years, it has used its nuclear weapons to deter threats and to coerce its neighbors during crisis. As the North Korean regime continues to suffer many failures, it may someday lash out and cause a major war in northeast Asia, or its government may collapse into civil war and anarchy. With almost no chance of winning a conflict limited to conventional weapons and having invested so much of their limited resources in WMD, North Korea's leaders are likely to use these weapons in conflicts or further crises. North Korean WMD could cause immense damage to the populations and economies in northeast Asia, potentially destabilizing the region for many years.

It is therefore incumbent on the United States and its allies to develop means to deter North Korea's use of WMD. But doing so is not easy. The United States and the Republic of Korea (ROK) have clearly failed to deter multiple North Korean provocations associated with WMD. Moreover, the North Korean leaders appear insensitive to the kind of "assured destruction" nuclear weapon retaliatory threats against cities and industry that formed the basis for Cold War deterrence. Instead, deterrence of North Korean WMD use needs to be based more on the ability to defeat that use and deny its objectives while still threatening retaliation that would undermine or destroy the North Korean regime.

This article describes such a deterrent approach, first by characterizing North Korea as a failing state—one which has used crises and may yet try to use conflict to strengthen the regime. It then addresses the nature of

---

Bruce W. Bennett, PhD, is a senior defense analyst at the RAND Corporation. He specializes in strategy formulation, force requirements, and responding to "asymmetric threats" such as weapons of mass destruction. He regularly works on Korean issues, having visited the region more than 80 times.

This article is adapted from a chapter that appeared in *Tailored Deterrence: Influencing States and Groups of Concern*, eds. Barry Schneider and Patrick Ellis (Maxwell AFB, AL: USAF Counterproliferation Center, 2011), 118–52.

North Korea's WMD threat, how that threat might be used, and the damage that could result. The study concludes by discussing how the United States and the ROK might deter North Korean WMD threats in conflict and crisis.

"Know Thy Enemy"

The ancient Chinese philosopher/strategist Sun Tzu urged, "Know thy self, know thy enemy. A thousand battles, a thousand victories." The situation inside North Korea is serious, complicating efforts to deter its use of WMD.

The Situation in North Korea

North Korea is a failing state with a failing economy and agricultural production usually much less than its subsistence food requirements.[1] As a result, many North Koreans starve to death, while the rest of the population survives in part because of substantial foreign aid and in part because of market activities. But the regime fears that North Korean merchants are beyond its control, especially given the extensive use of bribery. It therefore carried out a currency revaluation in late 2009 that allowed only minimal currency exchange and prohibited the use of foreign currency, seeking to wipe out the merchants' capital. This also took away the savings of many North Korean elites, caused hoarding of goods (especially food), and resulted in hyperinflation.

Despite North Korean efforts at authoritarian control, the regime sees a lot of rebellious behavior. This includes refugee flows into China,[2] major black market activities, graft, and corruption by North Korean authorities,[3] and even reported attacks on North Korean leaders.[4]

Social unrest appears to be spreading in North Korea. The regime there has tried to maintain control through heavy use of propaganda. But observers noted long prior to his death that "there is mounting evidence that Kim Jong-Il is losing the propaganda war inside North Korea, with more than half the population now listening to foreign news, grassroots cynicism undercutting state myths, and discontent rising even among elites."[5]

Recognizing that Kim Jong-Il's designated successor, his third son Kim Jong-Un, is young and inexperienced, the regime attempted to build his image in the waning days of his father's reign by crediting him with the December 2009 currency revaluation, in the end making him appear to

have caused a disaster. GEN Walter L. Sharp, then US commander in South Korea, summarized the situation in March 2010: "Combined with the country's disastrous centralized economy, dilapidated industrial sector, insufficient agricultural base, malnourished military and populace, and developing nuclear programs, the possibility of a sudden leadership change in the North could be destabilizing and unpredictable."[6] That prediction proved true, as "the suddenness of Kim Jong-Il's death has sparked fears of instability, with dangerous implications for the peninsula, East Asia, and the world." Nevertheless, North Korean "elites know that even a whisper against Kim Jong-Un (let alone actual coup attempts) would mean death for themselves and severe punishment for their families."[7]

How Is North Korea Coping?

The North Korean leadership has a culture of empowerment to justify its legitimacy. As the regime faced the many failures described above, it has used provocations to demonstrate it is still empowered and to create diversionary conflict effects. The regime seeks to unify its elites against common external adversaries, mainly the ROK and the United States, trying to steer their displeasure away from the regime.

For example, in 2006 North Korea faced serious US economic sanctions imposed because of illegal activities such as counterfeiting US currency and goods. It could have reversed these sanctions by admitting its illegal activities, apologizing, and promising to stop them. But in the culture of empowerment, such action would make the North Korean leadership appear weak and subject to overthrow. Instead, the regime prepared for, and carried out, a series of provocations, including missile launches on 4 July (US time) and escalating to a nuclear weapon test on 8 October (US time). Kim Jong-Il had demonstrated his empowerment, and by February 2007, had concluded an agreement with the United States and the other regional powers that reversed the economic sanctions and otherwise proved very advantageous to North Korea.

North Korea has continued its pattern of escalating brinksmanship to deal with its many challenges. It used missile launches and a nuclear test again in 2009 to demonstrate Kim Jong-Il's continued empowerment despite his very poor health, to support regime succession, to continue his use of diversionary conflict, and to achieve other objectives discussed below. In 2010 North Korea sank a ROK warship, escalating its pattern of provocations.

North Korean Asymmetric WMD Threats

As ROK and US conventional military superiority developed over several decades, the North Korean economy could not keep pace. Instead, North Korea opted to pursue various asymmetric threats, especially WMD. This was a natural evolution from Kim Il-Sung's emphasis on special operations forces in World War II.

How Much WMD Might North Korea Have?

Most experts in the United States assume North Korea has developed its nuclear weapon capabilities independently. For example, the CIA said North Korea produced enough plutonium by 1994 for one to two weapons,[8] and did not produce any more plutonium until 2003. Experts typically argue North Korea could have roughly 5–10 nuclear weapons today,[9] although, given the limited testing both of the weapons and their delivery means, only 2–6 of these would likely be deliverable and reliable.

A number of reports suggest North Korea has had external help. For example, in 1999 Dr. A. Q. Khan of Pakistan said he went to North Korea and was shown three plutonium weapons that could be assembled for use on ballistic missiles in one hour.[10] If he was right, North Korea must have had an external source of plutonium. Moreover, it would not likely have put all of its weapons in one place at one time and shown them to a foreigner, as a security failure could have led to US preemption. It may thus have had at least five or six nuclear weapons in 1999, consistent with what the defector Hwang Jong Yup said he was told in 1996.[11]

If these reports are correct, North Korea may have developed more than 10 nuclear weapons. In particular, Russian intelligence claimed that in 1992, North Korea got 56 kilograms of plutonium from the former Soviet Union.[12] If so, it could have enough fissile material today for perhaps 20 weapons. And if some organizations risked giving North Korea fissile material, they may also have provided the technical expertise necessary to make ballistic missile warheads, as Dr. Khan asserted.

Many reports address North Korean chemical and biological weapons. "We also assess Pyongyang has an active biological weapons research program, with an inventory that may include anthrax, botulism, cholera, hemorrhagic fever, plague, smallpox, typhoid and yellow fever. . . . North Korea has an assessed significant chemical agent stockpile that includes blood, blister, choking and nerve agents."[13] "In the assessment of US intelligence services, their reserves, accommodated in perhaps half a dozen

major storage sites and as many as 170 mountain tunnels, are at least 180 to 250 tons, with some estimates of chemical stockpiles run as high as 2,500–5,000 tons."[14] "In May 1996 ROK Foreign Minister Yu Chong-ha reported to the National Assembly that it was estimated that North Korea possessed approximately 5,000 tons of biological and chemical weapons. Given the extensive production facilities, this later estimate may constitute the low end of the actual stockpile."[15]

In terms of delivery systems, "chemical weapons can be delivered by virtually all DPRK [Democratic People's Republic of Korea] fire support systems. This includes most artillery, multiple rocket launchers (including those mounted on CHAHO-type boats), mortars, FROG and SCUD missiles, and some bombs."[16] "The North has about 600 SCUD missiles capable of hitting targets in South Korea, and possibly also of reaching Japanese territory. There are also 200 Nodong-1 missiles which could reach Tokyo."[17] North Korea would likely use its special operations forces (SOF) to deliver biological weapons. "Military authorities in Seoul estimate that North Korea's special operations forces currently exceed 200,000 soldiers. . . . North Korea has recently deployed about 50,000 special forces along its border with South Korea."[18]

Potential North Korean Uses of WMD

In peacetime, North Korea regularly uses its nuclear weapons to threaten neighbors, hoping to coerce them and/or deter their actions. It has used nuclear weapon possession and tests mainly for internal purposes to illustrate the strength or formidability of its regime and to claim North Korea is one of the most powerful (and respected) countries in the world. It has also used nuclear weapons as a bargaining chip to secure goods and agreements from other countries. It generally does not use chemical and biological weapons for such strategic purposes.

It is less clear how North Korea might use WMD in wartime. It has threatened to use nuclear weapons against the cities and military facilities of neighbors. An "unofficial spokesman" talked of North Korea using nuclear weapons to (1) create electromagnetic pulse (EMP) effects to disable electronic systems, (2) attack nuclear power plants (causing widespread nuclear fallout), and (3) attack cities in various ways.[19]

While the use of nuclear weapons against cities would be horrific, the United States planned a similar strategy during the Cold War with its so-called assured destruction concept of threatening Soviet cities. As early as

1945, the Joint Chiefs of Staff explained the concept of targeting Soviet cities: "The atomic bomb, in the foreseeable future, will be primarily a strategic weapon of destruction against concentrated industrial areas vital to the war effort of an enemy nation. In addition, it may be employed against centers of population with a view to forcing an enemy state to yield through terror and disintegration of national morale."[20]

North Korea is likely to view the survivability of its nuclear forces as limited, pushing it to use them relatively early in a conflict. This attitude would be strengthened by a belief that the United States will use nuclear weapons early and nuclear weapons would provide greater, potentially conflict-winning leverage if used early on.[21] For example, North Korea might hope appropriate nuclear weapon use would convince Japan not to become involved in the conflict and thereby deny the use of its territory to support US deployments and operations.[22]

Alternatively, North Korea might wait until an invasion of the South fails and the ROK/United States start a counteroffensive before using its nuclear weapons. The regime would know it had to stop the counteroffensive to survive and would be prepared to take very risky actions, including nuclear attacks on cities. Many analysts argue this would be the most likely use of North Korean nuclear weapons.

North Korea is more likely to use its chemical and biological weapons to achieve specific operational objectives such as causing breakthroughs on the battlefield, disrupting airfield and port operations, and disrupting the flow of US forces into Korea. Such attacks would best support North Korean objectives if done very early in a conflict. Given the potency of biological weapons, North Korea may prefer to use them at some significant distance from the Korean peninsula, such as in Japan or the United States.

Nuclear Effects on People and Things

The table below evaluates the expected effectiveness of North Korean nuclear attacks delivered by ballistic missiles against ROK ground forces, airfields, and population centers. This analysis assumes an airburst weapon to maximize prompt effects and eliminate most fallout. The Republic of Korea today, in peacetime, has 47 army divisions, 15 major military airfields, and a population of 48,500,000.

Thus, if North Korea uses one 10-kiloton (Kt) weapon against a ground force division (the second to last row), prompt effects would cause an expected 7 percent attrition, whereas the same weapon would cause an

Approximate North Korean nuclear weapon effects on ROK targets

Weapon Performance (60% delivery)	Weapons Launched per Target	Army Divisions Lost to Prompt Casualties	Airfields Lost to Prompt Casualties	ROK City Prompt Casualties*
10 Kt, 1.5 km CEP	20	1.40 of 47	5.7 of 15	3,100,000
10 Kt, 1.5 km CEP	15	1.05 of 47	4.7 of 15	2,400,000
10 Kt, 1.5 km CEP	10	0.70 of 47	3.1 of 15	1,700,000
10 Kt, 1.5 km CEP	6	0.42 of 47	1.9 of 15	1,100,000
10 Kt, 1.5 km CEP	3	0.21 of 47	0.93 of 15	600,000
10 Kt, 1.5 km CEP	1	0.07 of 47	0.31 of 15	200,000
50 Kt, 0.5 km CEP	1	0.25 of 47	0.70 of 15	850,000

*Expected casualties, including reliability/delivery probability. Thus a 10 Kt weapon launched at a city like Seoul will cause an expected 200,000 fatalities and serious casualties (assuming a baseline reliability/delivery probability of 60 percent); if it actually detonates in the middle of the city, it will cause an expected 340,000 fatalities and serious casualties.

expected attrition of 31 percent at a typical airfield or nearly 200,000 expected casualties in a city like Seoul. A high-effectiveness warhead (the last row) with higher explosive yield (50 Kt), accuracy (0.5 km CEP), and delivery probability (70 percent) would cause several times as much damage, depending upon the target type, suggesting the value North Korea might place on improving nuclear weapon capabilities.

The earlier rows of the table above show multiple nuclear weapons would do even more damage. For example, if North Korea uses (launches) three nuclear weapons against ground forces, 21 percent of a division would be damaged, while three weapons (spread across three airfields) would create an expected damage of 31 percent at each of three airfields, or casualties equivalent to 93 percent for a single airfield. At the extreme, 20 nominal North Korean nuclear weapons launched against these targets would affect about 3 percent of the ROK ground forces, or almost six ROK major air bases, or about 3 million ROK civilians. The very high potential damage to the civilian population suggests why North Korea might focus its attacks on cities as targets.

The Effects of Chemical and Biological Weapons

Chemical and biological weapons (CBW) can also affect large areas. Consider that a 12.5-Kt nuclear airburst will cause fatalities over perhaps 8 square kilometers (km^2), a large area of a city. In contrast, chemical and

biological weapons are carried by the wind; their effects are a function of the original dispersal pattern, wind direction and speed, and atmospheric conditions. If dispersed across a wide base, 1,000 kg of sarin might cause lethal effects over 0.7 to 8 km^2, depending upon these various factors. Similar dispersal of 10 kg of anthrax might cause lethal effects over 5 to 30 km^2.[23] These estimates suggest that possible quantities of CBWs could affect similar areas to those shown for nuclear weapons in the table.

The other key difference between CBWs and nuclear weapons is the number of people in these areas most likely affected. With an airburst nuclear weapon, most people in the lethal area would be affected. Even those inside buildings would see their buildings collapsed or seriously damaged, contributing to the injuries. With CBWs, the buildings may provide some degree of shelter from weapon effects. This would be especially true of multistory buildings without central air conditioning, as is typical in Seoul. Thus, only a fraction of the people in these areas would be affected, depending upon the time of year and building ventilation, leading to somewhat fewer casualties within a similar area. Still, even if the casualties are only half or a quarter as great as with nuclear weapons over a similar amount of area, these quantities of CBWs could cause tens of thousands of casualties or more in ROK cities.

Against military targets, chemical and biological weapons would tend to cause far less damage than is shown for nuclear weapons in the table. Military personnel tend to have protective clothing, medicines, and other counters to CBWs—protections that would significantly reduce casualties. Still, they would need timely warning to apply many of these protections, and thus warning of WMD use would become a key determinant of the damage North Korean CBWs could do to military forces.

Deterrence Theory

Deterrence occurs when an adversary expects the benefits of an action to be less than the costs and acts accordingly in a rational manner. The *Deterrence Operations Joint Operating Concept* (*DO JOC*) is the official Defense Department statement on deterrence. It says: "Deterrence operations convince adversaries not to take actions that threaten US vital interests by means of decisive influence over their decision-making. Decisive influence is achieved by credibly threatening to deny benefits and/

or impose costs, while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome."[24]

Basic Deterrence Concepts

The *DO JOC* uses a rational deterrence theory framework.[25] This theory examines the adversary's perception of the net benefits (benefits minus costs) of any action as well as the probabilities of these net benefits to determine the utility of the action. It then compares the utilities of the alternative actions—if the utility of restraint (the status quo) is greatest, deterrence is achieved.[26] This assessment does not require an adversary to find an action that is clearly beneficial. In some situations, all of its choices (even the status quo) may have negative utility, as appears to be the case with North Korea. In such cases, the adversary looks for the "least miserable option." Said differently, noted deterrence expert Robert Jervis has argued, "It is rational to start a war one does not expect to win . . . if it is believed that the likely consequences of not fighting are even worse."[27]

Rational deterrence theory assumes the adversary is risk neutral—its decision is based solely upon expected value calculations, not the taking or avoiding of risks.[28] The alternative theory considered by the *DO JOC* is called prospect theory, which assesses risk differently. It argues that when facing serious losses, as in the North Korean conditions described above, the adversary becomes a risk taker, ready to try actions that avoid or reduce its losses even if there is serious risk in those actions. Deterrence of risk takers is a much more difficult effort, as US experience with North Korea has illustrated.

Understanding Deterrence Leverage

As suggested, deterrence is achieved by affecting the benefits and costs perceived by an adversary as well as the adversary's perceptions of the probabilities it will experience these costs and benefits. The literature talks about two kinds of deterrence efforts: deterrence by threat of punishment and deterrence by threat of denial.[29]

Deterrence by threat of punishment usually seeks to increase the costs an adversary will suffer from an unwanted action, while deterrence by threat of denial seeks to reduce the benefits the adversary hopes to achieve. For example, if the United States wants to deter a North Korean missile test, it could threaten economic sanctions if North Korea proceeds with

the test (punishment) or it could threaten to preemptively destroy the missile on the launch pad (denial).

Deterrence is in the eye of the adversary. What does it perceive to be the benefits and costs of particular actions, and what does it believe are the probabilities of each outcome? Those perceptions are in turn based on US capabilities for denial and punishment and its will to impose those capabilities. When adversaries perceive the United States lacks will (e.g., it fails to act against the bad behavior of an adversary), they may discount other US denial and punishment threats (they perceive lower probabilities of costly outcomes and higher probabilities of beneficial outcomes).

Each US deterrent action has consequences for both sides. For example, a preemptive attack on a missile launch pad could destroy the missile and potentially embarrass the North Korean leadership, contributing to deterrence. But this would likely lead to further escalation, something the United States would usually prefer to avoid but which North Korea may be prepared to accept to rally its military and other elites around a failing regime. North Korea's escalation might be an artillery attack on the ROK, something the ROK would want to avoid. Thus, the ROK might pressure the United States not to carry out a preemptive attack to avoid escalation.

Many in the international community would also likely communicate their view that US preemptive action was unnecessary and inappropriate, hence reducing the probability of such action. If the United States has strong incentives not to carry out a preemptive attack, the adversary may conclude that the probability of such action, despite US capabilities, is extremely low.

If the United States cannot fully prove bad behavior by an adversary, it will normally be reluctant to take action. For example, despite assertions by President Bush in 2006 that he would hold North Korea accountable for nuclear proliferation, no serious action was taken when North Korean assistance in building a Syrian nuclear reactor was discovered the following year, assistance the United States could not prove beyond a reasonable doubt.

To the extent that its adversaries can keep their WMD activities covert, the United States will have difficulty responding against them. Adversaries may thus feel undeterred from pursuing covert WMD development and proliferation efforts.

Finally, there is a difference between US efforts to deter an attack upon the United States and efforts to deter attacks on its allies. Most adversaries will perceive the United States would respond very seriously to an

attack on its territory. But deterrence that supports US allies—so-called extended deterrence—often appears less likely to draw a serious response, given the lower level of US interest. To counter this concern, the US/ROK Presidential Summit in June 2009 declared a "Joint Vision for the Alliance of the United States of America and the Republic of Korea." This statement said in part, "The Alliance is adapting to changes in the 21st century security environment. We will maintain a robust defense posture, backed by allied capabilities that support both nations' security interests. The continuing commitment of extended deterrence, including the US nuclear umbrella, reinforces this assurance."[30]

Applying the Theory

In practice, few decision makers explicitly calculate the costs and benefits of each possible outcome, estimate the probability of that outcome, and calculate the preferred action based on precise calculations. Instead, consideration of these factors is more subjective and approximate. Moreover, it is difficult to estimate these factors for the North Korean regime, given how it strives to deny information on its attitudes and decision making to the outside world. Nevertheless, North Korean behavior does give some baselines against which to examine this framework and at least try to understand the tradeoffs its regime might perceive.

Consider the April 2009 North Korean missile test provocation.[31] Why did Kim Jong-Il select this action? To keep this example simple, assume there were three alternative courses of action at that time: (1) restraint (the status quo), (2) the use of artillery to fire into the ROK, and (3) the missile test.

The long-range missile launched on 5 April 2009 was likely seen as Kim's best course of action for creating the appearance of regime empowerment without much chance of retaliatory actions that could threaten regime survival, while avoiding the appearance of weakness to his internal or external enemies. Doing nothing in his regime's deteriorating position was likely seen as unhelpful, and doing too much—such as an artillery attack on Seoul—was likely viewed as unleashing a concatenation of escalation responses that could destroy the Pyongyang regime.

With the missile test, Kim Jong-Il probably hoped to counter the appearance of regime weakness associated with its many failures and his recent illnesses. He likely also hoped to create a "diversionary conflict" where his military and other elites would focus on the United States and the ROK

as their enemies, responsible for North Korea's problems, thereby creating an environment where his son had the best chance to succeed him. While his past provocations have invariably led to the United States and the ROK imposing some form of costs in return, usually economic sanctions, Kim Jong-Il has turned those costs to political benefit by unifying his military and other elites against their external enemies and in support of the regime.

Kim's missile test in April 2009 might have backfired if the United States had shot it down during the boost phase, preventing him from demonstrating his missile capability.[32] Alternatively, an artillery fire provocation could have failed due to effective ROK counterbattery fire that quickly silenced the artillery, indicating North Korean weakness rather than strength. Further, North Korean artillery fire into the ROK was clearly too escalatory and dangerous, and thus an unacceptable action.

The United States might have deterred a second North Korean missile launch if it had prepared to intercept the missile. It could have announced that it would not allow North Korea to launch another intercontinental-range ballistic missile.[33] The US announcement might have said, "If North Korea launches, the United States will use the opportunity to test its missile defenses against the target missile kindly provided by North Korea." Of course, since this would be an initial ballistic missile defense (BMD) test against this kind of threat, there would be a significant potential that the intercept would fail. But even then, the United States would gain significant experience in, and data about, intercepting real North Korean missiles.[34]

Kim Jong-Il might have viewed such a BMD threat as posing a good probability of making the regime look weak (by successfully intercepting the missile), plus some chance the launch episode could have escalated out of control toward full-scale war if the United States were prepared to be so aggressive. Under those conditions, he could have preferred the status quo to the outcome of a second missile launch.[35]

This simple example illustrates many of the characteristics of deterrence. In particular, it suggests the North Koreans might be deterred by US efforts to deny their provocations. Historically, much of the deterrence literature, and especially the nuclear deterrence literature, has focused on deterrence by the threat of punishment: an adversary could be deterred from taking an action because of the punishment threatened if it takes that action. But the United States and the ROK also need to apply denial

threats and find punishments that deter North Korean provocations such as missile launches.[36]

Deterring WMD Use

What is the relative utility of deterrence by denial and deterrence by punishment in the case of North Korea? Is there sufficient leverage in these two approaches combined to somehow control or prevent North Korean WMD use?

Options for Deterrence by Punishment and Deterrence by Denial

During the Cold War, the United States focused its deterrence of the Soviet Union on punishment. Deterrence by the threat of punishment can be achieved by threatening various assets of an adversary. Early in the Cold War the United States recognized nuclear weapon attacks against adversary cities were a serious deterrent threat (as noted above). US strategists also discussed targeting adversary military forces and/or leadership to achieve deterrence by threat of punishment (and also a significant level of deterrence by denial).

There are four basic actions that support deterrence by denial: counterforce, active defense, passive defense, and consequence management. *Counterforce attacks* seek to destroy adversary WMD forces (both weapons and delivery means) to prevent their use, and may also target command and control capabilities as well as adversary leaders to prevent WMD launch. *Active defenses* seek to intercept WMD en route to targets, and include air and missile defenses as well as border control against special operations forces or terrorists. *Passive defenses* seek to protect people and assets from WMD effects once the weapons detonate or are otherwise released. *Consequence management* seeks to deal with the effects of WMD after people/assets have been exposed, providing medical care and other kinds of damage recovery.

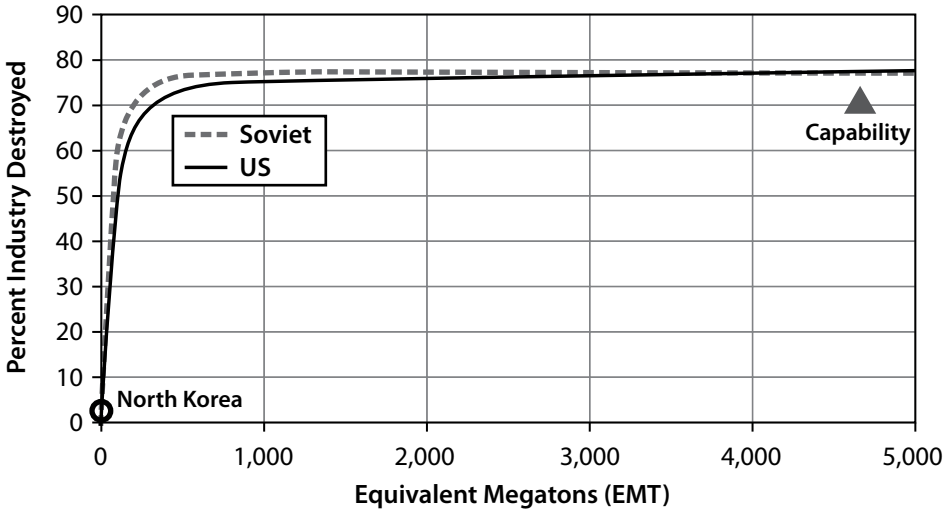
These denial means provide different levels of leverage against WMD use. Counterforce can be powerful if preemptive action is possible and the locations of the WMD forces are known. Active defense can be technologically challenging but potentially very effective as technologies mature. Passive defenses are relatively more effective against chemical, biological, and radiological weapons, having a more limited role against nuclear weapons (though sheltering and evacuation/dispersal can still be

important). And consequence management is important for dealing with WMD effects, but its capabilities have generally not been considered very effective in achieving deterrence of WMD use.

The Historical Approach to Deterrence by Punishment

Nuclear deterrence was a major international issue during the Cold War. For much of the period, the United States talked about strategic nuclear deterrence almost interchangeably with the concept of assured destruction. It deterred Soviet nuclear attacks by threatening to destroy Soviet cities with their associated populations and industry (imposing a high punishment cost). Many in the United States felt that if the Soviet cities were destroyed, most of their society would also be destroyed and the risk-averse Soviet leadership would not take that chance since their power flowed from the talents and productivity of their people.

In the 1970s, the ability of the United States and the Soviet Union to destroy each other's cities was assessed in the terms shown in the figure below. At the time, both the United States and the Soviets had thousands of equivalent megatons (EMT) of nuclear weapons,[37] as suggested by the "capability" mark at the right.



Deterring nuclear weapon use: Cold War vs. North Korea

The Soviet cities curve is derived from Alain C. Enthoven and K. Wayne Smith, *How Much Is Enough?* (New York: Harper and Row 1971), 207. The US cities curve is derived from US manufacturing value-added data of the same era.

The figure indicates even if the Soviets could have somehow destroyed most of the US nuclear forces, the United States could still have destroyed most of the Soviet industrial capacity,[38] since even a "small" city attack (a few hundred EMTs) would have been devastating.[39] And the same was true for the Soviets; they also deterred US nuclear attacks by threatening US cities. Moreover, the cost of adding one more warhead to the attack to ensure damage would always be much less than the adversary's cost of destroying one more warhead. Thus, little leverage was achieved by the capability for counterforce attacks or active defenses—not enough of the opposing threat could be denied to make a difference.

But the North Korean nuclear threat is a different problem, because it is on the part of the curve with steep returns. A North Korean force of 5–20 nuclear weapons of 10-Kt yield each would amount to about 0.25 to 1 EMT. Because North Korea has relatively few nuclear weapons, serious US/ROK efforts to destroy those weapons, combined with effective active defenses, could significantly reduce the damage North Korea could cause against its possible targets in ROK and Japanese cities or elsewhere.

Deterring of Chemical and Biological Weapon Use

During the Cold War, the US approach to deterring chemical and biological weapon use was less clear. The United States carried out a serious CBW defense program (passive defenses), seeking protection against the use of these weapons and deterrence of their use by denying their effects. US counterforce and active defense capabilities would also have helped deny CBW effects and thereby had some role in deterrence.

Early in the Cold War, the United States developed its own chemical and biological weapons to retaliate in kind against any Soviet CBW attack. Effectively, the United States was prepared to use these weapons to deny the Soviets any advantage from having employed similar weapons; in addition, research on offensive CBW capabilities significantly aided passive defense efforts against those threats.

Eventually, the United States joined the Biological and Toxin Weapons Convention (BTWC) in 1972 and the Chemical Weapons Convention in 1993 in the hope of precluding these weapons from future conflicts. But toward the end of the Cold War, the United States learned that the Soviet Union had not given up its biological weapons efforts despite having joined the BTWC. Lacking biological weapons at that point, the United

States implied it would employ nuclear retaliation against the use of these weapons.

But in the 2010 *Nuclear Policy Review Report*, the United States declared, "With the advent of US conventional military preeminence and continued improvements in US missile defenses and capabilities to counter and mitigate the effects of CBW, the role of US nuclear weapons in deterring nonnuclear attacks—conventional, biological or chemical—has declined significantly. The United States will continue to reduce the role of nuclear weapons in deterring non-nuclear attacks."[40] This statement does not preclude a nuclear response to adversary CBW use, but it makes such a response unlikely (a low probability), potentially reducing the deterrence of such attacks unless highly effective conventional force responses are guaranteed.

Deterring North Korean Use of WMD in a War

Deterrence of North Korean WMD use in war requires understanding what its leaders might think they could gain from war and from using WMD. Given North Korea's circumstances, an invasion of the ROK would most likely be an act of desperation for a regime losing control, a "diversionary war" used to secure support from the North Korean military for a near-failed regime.

At that point, there may even be some evidence of military plotting to overthrow the regime. Facing serious survival risks if it does nothing, the North Korean regime may decide that a general war will restore military support for the regime and give it a chance for survival, despite all the other risks.

Such a decision to invade the ROK would not be easy. North Korea has been deterred from invading since 1953, suggesting that its leadership already doubts its prospects in a major war. Indeed, the former US commander in South Korea, GEN Walter Sharp, has said, "I'm absolutely confident that if they [North Korea] came south, the ROK-US Alliance would be able to defeat them."[41] Thus, if the North Korean regime concludes that war is necessary for political reasons, it must also find a way to win or achieve some kind of "draw" in the conflict.

North Korean asymmetric means—its WMD—likely provides the only option for a favorable outcome. By using WMD, North Korea may feel there is some chance it could break Japanese support of the United States and also overcome US and ROK technological advantages. It has

put considerable investments into WMD capabilities—investments that could have been spent on other weaponry had North Korea not truly valued WMD. This is especially true for CBWs. It has paid the price to develop these weapons almost entirely for wartime utility.

Moreover, if the regime expects US nuclear weapon use in a war regardless of North Korean actions, it may view WMD use as just part of a war with the United States. While North Korea's prospects for success in such a war would be poor, in challenging circumstances the regime may perceive the prospects of war would be better than the prospects of outright regime failure. Thus, the key to deterring North Korean WMD use is to deter an invasion of the ROK in the first place—to convince the North Korean regime that war is not an alternative for handling its internal problems.

Deterring North Korean WMD Attacks by Punishment

Some military analysts argue that if North Korea ever uses a nuclear weapon (or perhaps other forms of WMD), the United States will launch a large nuclear weapon response to massively damage North Korea. Some even talk of turning North Korea into a "sea of glass," reminiscent of the Cold War assured destruction logic. Would such a threat against mainly innocent civilians deter the North Korean regime's use of WMD?

The regime has shown little value for the North Korean common people, allowing the starvation of at least hundreds of thousands and the massive societal disruption associated with a failing economy. It is unlikely to perceive significant cost to a Cold War–like assured destruction threat.

It is unlikely that either the ROK or the United States would want to devastate North Korean society with nuclear weapons. The ROK government wants the unification of Korea, a unification that would be immensely complicated by extensive nuclear damage. Moreover, the American public would find such destruction morally repugnant. The 2010 *Nuclear Posture Review Report* said the United States, "would only consider the use of nuclear weapons in extreme circumstances to defend the vital interests of the United States or its allies and partners."[42] Massive societal damage to North Korea would do relatively little to defend US and allied vital interests.

Retaliation against the North Korean military or political leadership would be alternative punishment approaches. These targets would also provide denial effects. But a North Korean leadership worried about

instability might welcome attacks on its military, which would likely increase military support for the political leadership.

Thus, the best punishment approach would be to threaten the North Korean political leaders themselves. Kim Jong-Un and the other leaders must come to feel their prospects for surviving a war are much less than their prospects of surviving a failing regime. A threat to target those leaders could provide much of the leverage needed to deter an invasion if the North Korean leaders believe that (1) US/ROK forces can effectively target them and (2) the United States and the ROK have the will to execute such an attack.

The greatest difficulty in effectively targeting the North Korean leadership is in locating that leadership. Indeed, Kim Jong-Il regularly "disappeared" from public view when he committed provocations,[43] likely hoping to avoid the possibility of being targeted. The North Korean leaders may therefore perceive they can avoid damage even from nuclear attacks, undermining deterrence of their actions. In addition, they would likely locate underground in a conflict situation, making it difficult to cause them damage. The United States must demonstrate to the North Korean leaders that it does regularly find them when they are "hiding" and can cause destruction, even against underground facilities, seeking to erase any perception that they could survive a retaliatory attack.

Kim Jong-Un may also wonder, "Would the United States have the will to attack me personally?" Many in the United States talk about avoiding such targeting of adversary leaders, which may give the North Korean regime hope. The United States needs to dissuade the regime of this notion through clear strategic communications. In particular, it should consider practicing attacks on the North Korean leaders as part of its exercises in the ROK, demonstrating that a decision to pursue them has already been made.

The quotes above from the 2010 *Nuclear Posture Review Report* raise the question of whether punishment for North Korean WMD use, and nuclear weapon use in particular, should be done with conventional or nuclear weapons. There are several reasons for preferring the use of nuclear weapons in such punishment:

- North Korean leaders will likely have much greater fear of US nuclear weapon use. According to an East German report in 1986, "Comrade Kim Il Sung affirmed that the Democratic People's Republic of Korea

(D.P.R.K.) does not intend to attack South Korea, nor could it. More than 1,000 US nuclear warheads are stored in South Korea, ostensibly for defense, and it would take only two of them to destroy the D.P.R.K."[44] To the extent that such a view persists in North Korea, US nuclear weapon threats will be far more effective in deterring its leaders' use of WMD and invasion of the ROK.

- If North Korea uses nuclear weapons early in a conflict and the United States does not answer in kind, the North Korean leaders will likely conclude that they can continue to use nuclear weapons without a US nuclear weapon response. This would effectively reinforce their peacetime impression of US threats lacking substance, thereby undermining transwar deterrence.
- The United States has promised a nuclear umbrella to both the ROK and Japan, which is a commitment of an in-kind response to North Korean nuclear weapon use. But the purpose of the nuclear umbrella is to deter adversary nuclear weapon use. Once an adversary has used nuclear weapons, the US nuclear umbrella has failed and may be questioned globally. The United States would therefore need to re-establish (or abandon) the credibility of its global nuclear umbrella commitments, commitments that many would not perceive as being met by a conventional weapon response. The US nuclear umbrella commitments are intended to persuade both adversaries and allies not to pursue nuclear weapon development. A failure to act consistently with these commitments could spur both adversaries and allies to develop their own nuclear forces, something not in the US interest.

In summary, the United States should threaten nuclear attacks against the North Korean leaders as punishment for nuclear weapon use and prepare to employ those threats. The North Korean leaders need to be convinced there is no chance they would survive an invasion of the ROK and associated WMD use. Other punishment threats are much less likely to deter North Korean WMD use, while punishment threats against the North Korean military may actually aid the diversionary strategy of the regime.

Deterring North Korea by Threat of Denial

As argued above, deterrence by denial involves primarily possessing effective capabilities for counterforce attacks, active defenses, and passive defenses.

Counterforce. In wartime, US and ROK counterforce efforts would attempt to destroy the North Korean WMD forces (both weapons and delivery means) and potentially the associated command and control. While the United States and the ROK have many capabilities to destroy such targets, they must first identify each target's location. Since they do not even know how much WMD North Korea possesses, they likely do not know all of the locations that must be attacked to destroy that WMD and associated delivery means.

The ROK minister of national defense has indicated that, "There are about 100 sites related to the nuclear program in North Korea."[45] Many of these are likely underground, and destroying them could require a large force, much more than would likely be available early in a conflict when other targets would also need to be struck and when standoff attack forces would be limited. Still, whatever North Korean WMD is destroyed by counterforce attacks reduces the burden on active and passive defenses. Unfortunately, incomplete destruction could push North Korean leaders into a "use them or lose them" approach, prompting WMD attacks on the ROK and/or Japan, an unwanted consequence.

Better intelligence on North Korean WMD, delivery means, and leaders would help facilitate counterforce efforts. Defectors could provide such intelligence, much as Soviet defectors from its biological program provided critical intelligence toward the end of the Cold War. Dissatisfaction among the North Korean elites may make such defections more possible now than ever before.[46]

Active Defenses. Active defenses seek to destroy WMD after launch but before it arrives on target and detonates or is dispersed. US, ROK, and Japanese air defenses would likely deny effective attacks by aircraft, thus few experts expect North Korea to deliver WMD bombs. But ballistic missile defenses provide only limited protection in Japan and especially in the ROK today. This means some North Korean missiles could leak through, and the missile defenses could be exhausted by initial North Korean strikes.

Broader deployment of missile defenses around potential targets plus the addition of more broad area defenses (like the US Navy SM-3 interceptor and the US Army THAAD system) could increase the effectiveness of the defenses and, to the degree that North Korean leaders appreciate these capabilities, thereby enhance deterrence of North Korea's aggressive actions. In addition, enhanced control of immigration into Korea and surveillance of ROK coastal

areas could reduce the ability of North Korean special operations forces (potentially carrying biological weapons) to infiltrate the ROK.[47]

Passive Defenses. Passive defenses seek to protect people and assets from the effects of WMD once those weapons detonate or are dispersed. Because nuclear weapons are so powerful, the best passive defenses against them involve evacuation of likely target and fallout areas and dispersal of assets to safer areas. The hardening of some target areas can also be helpful, using blast-protected shelters and underground facilities to avoid fallout casualties. The Soviets attempted such an approach to overcome US assured destruction during the Cold War, and the North Koreans have made similar efforts with vast numbers of underground facilities. But building such shelters would be prohibitively expensive in the ROK, Japan, or the United States for all but modest-sized groups. And evacuation would also prove challenging and difficult to sustain.

As noted earlier, passive defenses would be far more powerful against North Korean chemical and biological weapons. The United States and the ROK should use strategic communications to convey the level of passive defenses they have developed, including advanced medical measures, to convince North Korea that these weapons will not yield the leverage the North would seek in a war. Such US and ROK efforts should describe the level of protection afforded by these defenses without divulging the details of the defenses to avoid North Korean work on counters.

Conclusions on Deterring North Korean WMD Use. Deterrence of WMD use would clearly be very difficult when the North Korean leaders become desperate. The United States and its allies would need to convince the leaders that they are more likely to survive with peace (facing rebellion) than with war (facing destruction)—peace is still the least miserable option.

The denial component of deterrence would be key—prevent North Korea from perceiving any chance of achieving victory. Focusing punishment on its leaders would also be important: they must be convinced they will not survive a war, even if they use WMD for leverage. In short, the United States and the ROK should focus on deterring North Korea from invading the ROK and thereby deter North Korean WMD use.

Deterring North Korean WMD Crises/Provocations

From February through July 2009, North Korea created a number of serious crises with WMD-related provocations. These were apparently

motivated by the conditions inside North Korea described at the beginning of this article, some rising to the crisis level even before the provocation. Such crises jeopardize regime control and could eventually imperil the regime.

The provocations appear to reflect the regime's view of its jeopardy—serious enough to take modest risks with provocations, but not so serious as to justify an invasion or major attacks on the ROK. The sinking of the ROK warship *Cheonan* and the artillery shelling of Yeonpyeong Island in 2010 escalated this pattern to unprovoked, limited attacks. This escalation makes North Korea appear even more dangerous.

Can the United States and the ROK deter such provocations? Thus far, the United States has failed to deter a number of North Korean provocations, but it has likely deterred others. It is important to recognize while little is known for certain about North Korea, such uncertainty should not prevent purposeful US/ROK action.

Understanding the North Korean Provocations

The underlying instability in North Korea in 2009 was Kim Jong-Il's bad health. He apparently suffered a stroke in August 2008 and was slow to recover. This serious illness undermined his appearance of empowerment needed for leadership in North Korea. Reports of his bad health had started even before the reported stroke, with claims that he had heart surgery in May 2007. By the spring of 2009, there were many reports of North Korea speeding succession efforts for his third son because Kim Jong-Il's health was so serious;[48] by September 2010, Kim Jong-Il had put his son in positions that made his succession appear likely. His son's previous lack of such positions and his mid-20s age made him an unlikely ruler by North Korean leadership standards.

To solve his appearance of weakness and support potential succession, Kim Jong-Il needed to create an image that the regime is powerful, and he and his son are responsible for that power. His 2009 provocations showed North Korea as close to acquiring a space launch capability and intercontinental ballistic missiles, and it has produced nuclear weapons—capabilities few other countries possess.

While the North Korean regime likely anticipated US efforts to implement sanctions in response, the United States made no specific sanction threats, failing to reinforce deterrence. And the previous UN sanctions

had not been particularly harmful to North Korea because they were largely unimplemented.[49]

Indeed, the regime likely planned to use any sanctions to once again claim that the United States and its allies are the enemies of the North Korean people and responsible for everything wrong in North Korea. Still, it apparently hoped to extort further aid and recognition from the United States and regional powers, using escalatory brinksmanship until rewarded for deescalating tensions.

North Korea's second nuclear test in late May 2009 was a major escalation. While many in the West had criticized the first test in 2006 as a likely failure, the second had a much higher yield (at least several kilotons), about 10 times the first. North Korea apparently had mastered the basics of nuclear weapons, increasing its appearance of empowerment as well as its ability to deter action by the United States and others. It had also increased its ability to market nuclear expertise; it had reached the threshold at which it may have hoped to be considered a nuclear power. "There was a sense that every North Korean escalation was intended as a bargaining chip. Now there's an alternative view taking hold: that Kim Jong-Il wants to force the world to acknowledge it as a nuclear power before he dies."[50]

Immediately after the North's nuclear test, the ROK announced it would join those nations supporting the Proliferation Security Initiative (PSI). But before the test, the ROK had refused to threaten to join the PSI in response to North Korean provocations, thus its joining likely had little impact on the North Korean decision to conduct a nuclear test. The UN also implemented fairly serious economic and military/nuclear test sanctions against North Korea in UN Security Council Resolution (UNSCR) 1874, but no specific sanctions threats were made seeking to deter the test.

Especially with a risk-taking state like North Korea, threats must be explicitly presented before the state takes an action or they will have little credibility and thus little deterrent value. The United States had already failed to take action against North Korea for its nuclear proliferation to Syria, as noted earlier; therefore, the regime likely felt there was little probability it would pay serious costs for a nuclear test. In summary, the United States and its allies did not use—or poorly used—the means they had for deterring the North Korean provocations.

This is not to say the United States totally failed in deterring North Korean provocations in 2009. Just after its second nuclear test, North Korea appears to have moved intercontinental-range missiles to both its east and

west coast launch facilities.[51] It appeared to be preparing for another ICBM/space launch test, similar to its April test. North Korea was likely trying to continue its escalating brinksmanship, as in 2006, hoping to achieve a major payoff from the United States.

Shortly after the second nuclear test, President Obama announced, "We are not intending to continue a policy of rewarding provocations. I don't think that there should be an assumption that we will simply continue down a path in which North Korea is constantly destabilizing the region and we just react in the same ways by, after they've done these things for a while, then we reward them."[52] He was joined in such comments by several other members of the US administration. The consistency and strength of these statements suggested North Korea's escalatory brinksmanship campaign would not pay off like its similar campaign did in 2006–07.

It is impossible to know whether these statements changed its plans, but North Korea did not launch an ICBM with its missile launches on 4 July 2009. It may have chosen to launch only short-to-medium-range missiles then, trying to stay below a provocation threshold that might have triggered a major US response. Within North Korea, the regime could still claim it had (1) violated the UN sanctions after its second nuclear weapon test, (2) defied the United States and the United Nations, and (3) deterred a significant US/UN response.

Former president Bill Clinton then went to Pyongyang to free a US woman jailed by North Korea. According to the North Korean secret police agency, "Thanks to Commander Kim Jong-Un's cleverness, former US President Clinton crossed the Pacific Ocean to apologize to the General [Kim Jong-Il]."[53] For North Korean audiences, this provided Kim Jong-Il the appearance that the United States had surrendered, and he was very much empowered; the Clinton visit also supported Kim Jong-Un's succession. The regime could accept such an outcome as a very adequate end state for the 2009 provocations.

US/ROK Options for Deterring North Korean Provocations

How should the United States and the ROK try to deter/counter future North Korean provocations? For example, how should they have acted to deter the sinking of the warship *Cheonan*? Threats of economic sanctions have generally proven inadequate, and US/ROK threats of military actions have very little likelihood of being carried out. Indeed, even with

fairly strong evidence of North Korean culpability in the *Cheonan* sinking, the United States and the ROK did not pursue military responses, in part because of the escalatory danger of such responses. There are two key parts of a strategy to deter North Korean provocations, corresponding to deterrence by threat of denial or threat of punishment through retaliation.

Deterrence by Denial. The ROK has already recognized that the *Cheonan* sinking reflects gaps in its military capabilities. President Lee has committed to "make sure such an incident does not occur again."[54] The ROK needs to fill the gaps in its military preparations against provocations and limited warfare threats, with US help, and appears to be proceeding to do so. This means not only developing capabilities to detect and counter North Korean submarines in ROK territorial waters, but also addressing North Korean missile, artillery, SOF, and other limited threats. Poor ROK defenses on Yeonpyeong Island undoubtedly contributed to North Korea feeling it could fire artillery at the island in November 2010; the ROK has greatly reinforced its marine forces on all of the northwest islands since then.

The ROK has singled out North Korean asymmetric threats as a particular area of focus, which includes WMD.[55] Thus, the earlier discussion of counterforce, active defense, and passive defense against WMD is equally relevant here. North Korea is unlikely to execute provocations which it anticipates will fail, causing the regime to look weak.

Deterrence by Punishment. As with major warfare, US/ROK efforts to punish North Korean provocations via limited attacks on its military would be unlikely to do immediate, significant damage to the North's military power but would likely drive the military to be more supportive of the regime, exactly the opposite of the desired response. Instead, punishment needs to focus more on the regime's political weaknesses, where it would likely perceive a major cost being imposed.

This approach needs to start by recognizing that North Korea is a failing state and that, sooner or later, its government will collapse. If a collapse were to occur today, the United States and the ROK are woefully unprepared to handle the consequences[56] (as is China, the other major player in such a collapse). This lack of preparation could be extraordinarily costly to all these countries if collapse were to occur in the short term. Thus, they need to prepare for a collapse and shape the North Koreans to reduce the potential negative outcomes.

Anything the United States or the ROK does to prepare for a government collapse would be offensive to the North Korean regime. These actions therefore become the perfect political threats that can be applied in trying to deter North Korean provocation. They would include simply talking about collapse and the subsequent ROK-led unification of Korea. Thus, the United States and the ROK should outline a unification strategy and plan and use some actions from that plan to punish North Korea for its provocations, while threatening other (stronger) actions to deter further provocations.[57] Any US/ROK actions to shape North Korea for unification would impose costs on the regime and directly undercut the benefits sought in its provocations (a denial outcome).

But to correct earlier weaknesses in US/ROK deterrence efforts, they would need to explicitly threaten North Korea with specific deterrent responses and then be prepared to execute them if necessary. Vagueness in making threats or showing little apparent will to follow through could thoroughly undermine the deterrence of North Korea, especially as the regime feels more threatened internally and thus more willing to take risks.

For example, in response to the shelling of Yeonpyeong Island, US and ROK leaders could have announced that North Korean internal instability led to the shelling, and such instability forces the ROK to prepare for a North Korean collapse. As a first step in these preparations, the ROK president could ask US and ROK Marines to train to deliver humanitarian aid (especially food and medicine) along the North Korean coastlines.

Such an effort is needed because food and medicine are already in short supply in North Korea and would largely disappear in the aftermath of a collapse, leading to a humanitarian disaster. The roads across the demilitarized zone (DMZ) would be inadequate to transport all of the needed humanitarian aid into North Korea, making across-the-beach deliveries one appropriate option. ROK and US Marines would need to perform this task, as opposed to international humanitarian organizations (IHO), because of the lack of security in a collapsed regime environment and the danger posed by the North Korean military and black market criminals. IHOs could take over once a secure environment in specific areas of North Korea is achieved.

The North Korean regime would clearly hate such declarations and actions by the United States and the ROK, as these would impose serious costs. The costs could be enhanced by training along the ROK coasts for humanitarian aid delivery, filming those exercises, and broadcasting those

films and pictures into North Korea. The message to the North Korean people and even the elites would be clear: the United States and the ROK are not your enemies and are instead preparing to help you when the North Korean regime allows. Directly countering the propaganda of regime leaders could impose a significant penalty on them.

North Korea is likely to respond unfavorably to these US/ROK actions and could escalate, seeking to retain the appearance of empowerment but also to deter further actions of this kind. The potential for escalation compels the United States and the ROK into planning deterrence against a range of North Korean escalations, as well as other provocations.

The US/ROK actions for deterring further North Korean provocations could also be used to prepare North Korea for an ROK-led unification. These measures could include demonstrating high-technology ROK military capabilities; actively seeking North Korean defectors, especially from its nuclear program and senior political/military leaders; a declaration that the United States will attempt to shoot down any North Korean missiles launched; development of counterfire plans against North Korean artillery use; pursuit of laser or other weapons to destroy North Korean artillery in flight;[58] selective amnesty for the elites; and a discussion of ROK plans for retirement payments to be offered to senior North Korean elites. The ROK and United States should prepare and then privately threaten to take some of these actions if the regime initiates further provocations.

Proper Terminology with Nuclear Powers

The United States and the ROK must also deny North Korean efforts to achieve its objective of becoming a recognized nuclear weapon power. Such a designation would be a major accomplishment for the regime, strengthening its ability to deter external threats and coerce its neighbors while demonstrating the empowerment of the regime and partially legitimizing its possession of nuclear weapons. Unfortunately, even Malcolm Moore, former "head of the United Nations nuclear agency, has said that North Korea is a fully fledged nuclear power."[59]

It is neither accurate nor in the interest of the world to so recognize North Korea or to reward its regime. Eight other countries currently possess nuclear weapons, and even the one with the smallest nuclear arsenal may have 10 times as many weapons as North Korea. In addition, each of these other countries has forces equipped to deliver nuclear weapons on targets. North Korea is just not in the same league. More importantly, the

Non-Proliferation Treaty (NPT) recognizes only five nuclear powers, and they are designated as the only states approved for possession of nuclear weapons.

To avoid rewarding North Korea and other aspiring nuclear weapon countries (like Iran or even Myanmar), the international community should develop new terminology associated with state possession of nuclear weapons. Appropriate terms might be:

- **A Compliant Nuclear Power**: One of the five countries recognized in the NPT as a nuclear power—the United States, Russia, China, Great Britain, and France.
- **A Noncompliant Nuclear Power**: Countries which have circumvented the NPT in fielding significant numbers of nuclear weapons and organized nuclear forces for the delivery of those weapons. Today, the states in this category apparently would be India, Pakistan, and Israel.
- **A Noncompliant Nuclear Experimenter**: Countries which have circumvented the NPT and begun testing nuclear weapons but still have few such weapons and little delivery capability. Today, North Korea is the sole state in this category.

The 2010 *Nuclear Posture Review Report* makes a big issue of compliance with the NPT and argues that global policy should follow that precedent. But it is also important to characterize even a "noncompliant nuclear power" as a country that has done much more than just test nuclear weapons. The nuclear power designation should be reserved for those responsible states that

- Field secure, transparent nuclear forces of a size appropriate for regional minimum deterrence;
- Establish nuclear weapon safety programs to prevent unauthorized use of nuclear weapons—these efforts would include weapon employment limits like the US permissive action link (PAL); and
- Limit nuclear testing and do not test nuclear weapons on delivery means like ballistic missiles.

A state unwilling to meet these standards is either a noncompliant nuclear experimenter or merits a designation like "noncompliant nuclear rogue."

Speaking of North Korea as a noncompliant nuclear experimenter more accurately captures its nuclear weapon capabilities. It downgrades the rec-

ognition North Korea wants, which is a good thing, and discourages other states from thinking they can quickly improve their international standing by testing a nuclear weapon. While North Korea appears determined to pursue further nuclear weapon tests to demonstrate its nuclear status, these terms would reduce the incentive it would have with further tests and leave it permanently designated as out of compliance with the Nuclear Non-Proliferation Treaty. This would reduce a major benefit North Korea has sought with its nuclear weapon tests (thereby increasing the disincentives for provocations in the future) and might dissuade other countries seeking to gain nuclear weapon capabilities.

Conclusions

North Korea appears to pose a serious WMD threat. In particular, its nuclear weapon threat is potentially greater than normally assumed. Because North Korea is a failing state, it will have considerable incentives to employ its WMD in crises and conflict.

The United States and the ROK need a deterrence strategy against this threat, addressing both North Korean provocations and potential WMD use. This strategy will differ from the Cold War nuclear deterrence strategy because of North Korea's risk-taking behavior and the nature of its WMD capability (especially the small number of its nuclear weapons). Thus, the US/ROK deterrence strategy must be based on a combination of their capabilities for denial and punishment, both of which need to be increased.

To prevent significant North Korean WMD use, the United States and the ROK need to focus on the internal threats the North Korean regime faces. They need to convince the regime it has no prospects of survival in war, and thus war is not an alternative for dealing with internal threats. Moreover, they need to convince North Korea its WMD use would often be thwarted by denial capabilities, reducing the incentives for its use.

To prevent North Korean provocations and limited attacks, potentially including WMD use, the United States and the ROK must first work to resolve the gaps in defenses against limited attacks. This is not just a naval issue after the sinking of the *Cheonan*, but rather a broader issue, including North Korean missile, artillery, and SOF attacks. The ability to deny North Korea success in these limited attacks will significantly strengthen deterrence against a regime wishing to avoid embarrassment and the appearance of weakness. The United States and the ROK should also

develop a strategy and plans for the ROK-led unification of Korea and use key elements of such a strategy to punish and deter North Korean provocations. The North Korean regime is likely to see that these actions impose serious costs, and these actions will generally be within the feasible set of actions available to the United States and the ROK, thereby strengthening deterrence. SSQ

Notes

1. North Korea needs about 5.4 million tons of grain to feed its people and produced only about 4.1 million tons in 2009. See, for example, "Food Shortage Worsens in N. Korea: Official," *Korea Herald*, 10 February 2010, http://www.koreaherald.com.kr/ NEWKHSITE/data/html_dir/2010/02/10/201002100069.asp.

2. "Tens of thousands of North Koreans have crossed the border seeking a better life. Some 15,000 have successfully defected to the South, while an estimated 100,000 to half a million are in China seeking asylum." Tae-hoon Lee, "NK Regards OPLAN 5029 as Declaration of Warfare," *Korea Times*, 8 November 2009, http://www.koreatimes.com.kr/www/news/nation/2009/11/116_55089.html.

3. "Survival of the Wickedest," *Strategypage.com*, 26 June 2008, http://www.strategypage.com/qnd/korea/articles/20080626.aspx.

4. Sang-hyun Um, "N. Korea: Kim Jong-Il's Distant Relative Tried to Kill Him with Chinese Blessing," *Shin-Dong-A* (S. Korean monthly), October 2004.

5. Blaine Harden, "Dear Leader Appears to be Losing N. Koreans' Hearts and Minds," *Washington Post*, 24 March 2010, 11. See also "Millions of N. Koreans Listen to Foreign Radio Broadcasts," *Chosun Ilbo*, 30 April 2010, http://english.chosun.com/site/data/html_dir/2010/04/30/2010043001070.html.

6. "USFK [US Forces Korea] Commander Warns of Possible N.K. Instability," *Korea Herald*, 26 March 2010, http://www.koreaherald.com.kr/NEWKHSITE/data/html_dir/2010/03/26/201003260041.asp.

7. Jennifer Lind, "Kim Jong-Un Takes the World's Worst Job: The Downside of Stability in North Korea," *Foreign Affairs*, 22 December 2011.

8. "North Korean Nuclear Weapons: CIA Estimate for Congress," 19 November 2002, http://www.fas.org/nuke/guide/dprk/nuke/cia111902.html.

9. See David Albright and Paul Brannan, "The North Korean Plutonium Stock," *Institute for Science and International Security*, 21 February 2007, http://www.isis-online.org/publications/dprk/DPRKplutoniumFEB.pdf.

10. Jeffrey Smith and Joby Warrick, "Pakistani Scientist Depicts More Advanced Nuclear Program in North Korea," *Washington Post*, 28 December 2009.

11. "Hwang Jang-Yop . . . said that Jong Pyong-Ho, a senior party official in charge of military matters, had told Hwang in 1996 that North Korea had five plutonium-based nuclear weapons." *North Korea's Weapons Programmes: A Net Assessment* (London: International Institute of Strategic Studies, January 2004), http://www.iiss.org/publications/ strategic-dossiers/north-korean-dossier/north-koreas-weapons-programmes-a-net-asses/north-koreas-nuclear-weapons-programme.

12. Larry A. Niksch, *North Korea's Nuclear Weapons Program*, Congressional Research Service, IB91141 (updated 27 August 2003), 9, http://fpc.state.gov/documents/ organization/24045.pdf.

13. Gen Leon J. LaPorte, "Statement before the Senate Armed Services Committee," 1 April 2004, 5, http://www.globalsecurity.org/military/library/congress/2004_hr/ 040401-laporte.pdf.

14. "North Korea: Chemical Weapons Program," *GlobalSecurity.org*, http://www.globalsecurity .org/wmd/world/dprk/cw.htm.

15. Federation of American Scientists, "North Korea: Chemical Weapons Program," http://www .fas.org/nuke/guide/dprk/cw/.

16. Defense Intelligence Agency, *North Korea Handbook*, PC-2600-6421-94, (1994), 3-15–16.

17. "Longer-Range Seoul Missiles in the Works," *Singapore Straits Times*, 9 October 2009, 38.

18. "N. Korea Believed to Have 200,000 Special Forces Troops," *Chosun Ilbo*, 11 October 2010, http://english.chosun.com/site/data/html_dir/2010/10/11/ 2010101101081.html.

19. Myong Chol Kim, "Nuclear War is Kim Jong-Il's Game Plan," *Asia Times*, 12 June 2009, http://www.atimes.com/atimes/Korea/KF12Dg01.html.

20. US Joint Chiefs of Staff, "Over-All Effect of Atomic Bomb on Warfare and Military Organization," J.C.S. 1477/1, 30 October 1945, US National Archives.

21. For example, "Korea cannot be unified in a peaceful way. [The North Koreans] are prepared for war. If a war occurs in Korea, it will be waged by nuclear weapons, rather than by conventional ones." This quote is from a report by a Hungarian foreign ministry staffer based on a 1976 conversation with a member of the staff of the North Korean Embassy in Hungary, in Balazs Szalontai and Sergey Radchenko, "North Korea's Efforts to Acquire Nuclear Technology and Nuclear Weapons: Evidence from Russian and Hungarian Archives," Woodrow Wilson International Center for Scholars, Cold War International History Project, Working Paper #53, August 2006, Document no. 28, 55, www.wilsoncenter.org/topics/pubs/WP53_web_final.pdf.

22. "North Korea threatened Thursday to turn Japan into a 'nuclear sea of fire' if the United States launches a nuclear war against the communist country." See "*Yonhap* Cites DPRK Warning to Japan on U.S. Cooperation Causing 'Nuclear Sea of Fire,' " *Seoul Yonhap in English,* Foreign Broadcast Information Service (FBIS) translation KPP20040923000069, 23 September 2004.

23. The areas compared here are from *Proliferation of Weapons of Mass Destruction: Assessing the Risks* (Washington: Congressional Office of Technology Assessment, August 1993), 53–54.

24. Department of Defense, *Deterrence Operations Joint Operating Concept*, Version 2.0, December 2006, 3.

25. "This is a stylized view of deterrence often associated with rational choice/expected utility deterrence models of the Cold War era. The *DO JOC* expands upon rational choice considerations and incorporates elements of prospect theory in its approach." Ibid., 20.

26. Mathematically, the adversary's utility (U) of each action (j) is assessed by combining the benefits (B) and costs (C) of each outcome (i) with the probability (P) of that outcome if the action is taken, thus: U(j) = S (Bji-Cji)*Pji.The utilities are then compared and "restraint" is chosen if: U(restraint) > max($U(j_1)$, $U(j_2)$, …, $U(j_n)$).

27. Robert Jervis, "The Political Effects of Nuclear Weapons," *International Security* 13, no. 2 (Fall 1988), 80–81.

28. By analogy, monetary gambling almost always involves a negative expected value payoff to the individual because the "house" takes a portion of the money bet. Gamblers are thus normally risk takers (unless they believe that they have a "system") because, while they may win a large amount of money, on average they will lose.

29. These concepts were introduced in Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, NJ: Princeton University Press, 1961), 14–16.

30. "Joint Vision for the Alliance of the United States of America and the Republic of Korea," 16 June 2009, http://www.whitehouse.gov/the_press_office/Joint-vision-for-the-alliance-of-the-United -States-of-America-and-the-Republic-of-Korea/.

31. On 5 April 2009, North Korea test-launched a long-range missile that it described as a space launch vehicle.

32. There is, however, a risk to the United States in trying to shoot down a North Korean missile. If it tries but fails to shoot down the missile, US missile defense capabilities would be discredited, and Kim Jong-Un would appear to be further strengthened and even more capable.

33. On 19 March 2009, ADM Timothy Keating, then commander of the US Pacific Command, "said the U.S. is 'fully prepared' to shoot down the missile and added that the U.S. military has the capability to do it." But Secretary of Defense Gates subsequently indicated that the United States would not attempt an intercept, likely fearing the escalatory implications and perhaps anticipating that the North Korean test would have likely failed. "Does Obama Have a N. Korea Policy?" *Chosun Ilbo* (31 March 2009), http://english.chosun.com/w21data/html/news/200903/200903310031.html.

34. Of course, North Korea would claim that such a missile launch was actually of a space launch vehicle, allowed by international law. Thus, the United States would have to carry out a strategic communications plan to preemptively discredit such a claim and focus on the destabilizing implications of operational North Korean ICBMs.

35. This is an extremely simple example for illustrative purposes. In practice, US strategic planners need to be developing more sophisticated assessments, including potential escalations, and also sensitivity testing the uncertain factors, seeking robust counters to North Korea's threats.

36. In trying to deal with the sinking of the South Korean warship *Cheonan*, "[US Secretary of Defense] Gates, who met counterparts from Japan and South Korea . . . admitted Washington and its allies had limited options." Dan De Luce, "Gates Warns of More N. Korea 'Provocations,' " *Agence France-Presse*, 6 June 2010.

37. An equivalent megaton (EMT) consists of the number of weapons of any given explosive yield needed to do the same damage as a single one-megaton weapon. Three 200-Kt weapons, seven 50-Kt weapons, or 21 10-Kt weapons would constitute 1 EMT.

38. In practice, the database used to make this assessment included only about 77 percent of Soviet industry. Thus, the fact that the lines quickly peak at 77 percent does not mean that 23 percent of Soviet industry would necessarily have survived, but rather that the information needed to determine the survivability of that 23 percent was not available.

39. This analysis was extremely simplistic and assumed, for example, that all nuclear weapons would be targeted on cities and that weapons destroyed by counterforce attacks would be replaced by surviving weapons in attacking each target.

40. *Nuclear Policy Review Report* (Washington: DoD, April 2010), viii.

41. "U.S. General Concerned by Threat to Seoul Posed by N. Korea's 800-Missile Arsenal," *East-Asia-Intel.com*, 17 October 2008. General Sharp's predecessor, GEN Burwell B. Bell III, said, "I also know with some certainty that if for some reason deterrence fails and North Korea attacks South Korea in any way, that we would quickly and decisively defeat the aggression." Anna Fifield, "U.S. General Warns of N Korean Nuclear Test," *Financial Times*, 30 October 2006.

42. *Nuclear Policy Review Report*, viii–ix.

43. See, for example, "Kim Jong-Il Vanishes From Public Eye," *Donga Ilbo*, 7 August 2006; and later, Ji-hyun Kim, "Kim Jong-Il Lying Low," *Korea Herald*, 2 June 2010, http://www.koreaherald.com/national/ Detail.jsp?newsMLId=20100602000180.

44. This quote is from a report on the visit of Erich Honecker to North Korea in 1986 and is included in Szalontai and Radchenko, Document no. 52, 74.

45. "Seoul Suspects about 100 Sites in N.K. Linked to Nuclear Program," *Korea Herald*, 5 October 2009, http://www.koreaherald.co.kr/NEWKHSITE/data/html_dir/2009/ 10/05/200910050098.asp.

46. The December 2009 North Korean currency revaluation took most of the wealth away from even the North Korean elites, leading to reports of social unrest that may open the door to defection for some.

47. The author has been told of North Korean SOF coming into the ROK on commercial airlines, using forged passports. This kind of activity could be largely eliminated by tying the passport databases together for the regional countries and dealing with anyone using a forged passport.

48. See, for example, "Kim's Failing Health Prompting N. Korean Power Transfer to Son: Seoul Minister," *Korea Herald*, 4 June 2009.

49. The North Korean leaders were likely surprised by the relative strength of the subsequent UN Security Council Resolution (UNSCR) 1874 and the sanctions it applied.

50. David E. Sanger, Mark Mazzetti, and Choe Sang-Hun, "North Korean Leader Is Said to Pick a Son as Heir," *New York Times*, 3 June 2009, 1.

51. "N. Korean Missile Train on the Move," *Chosun Ilbo*, 17 June 2009, http://english.chosun.com/site/data/html_dir/2009/06/17/2009061700282.html.

52. Jennifer Loven, "Obama Vows Tougher N. Korea Stance," *Arizona Daily Star*, 7 June 2009.

53. So-hyun Kim, "N. Korean Agency Uses Clinton's Visit to Praise Kim Jong-Un," *Korea Herald*, 10 August 2009, http://www.koreaherald.co.kr/NEWKHSITE/data/html_dir/2009/08/10/200908100042.asp.

54. Jeong-ju Na, "President Plans Stern Steps after Cause of Ship Sinking Revealed," *Korea Times*, 19 April 2010, http://www.koreatimes.co.kr/www/news/nation/2010/ 04/116_64442.html.

55. Sung-ki Jung, "Lee Directs W3 Tril. Rise in Arms Buying: Seoul Seeking to Counter NK's Asymmetrical Warfare," *Korea Times*, 16 May 2010, http://www.koreatimes.co.kr/www/news/nation/2010/05/205_65967.html.

56. See, for example, Victor Cha, "We Have No Plan," *Chosun Ilbo*, 9 June 2008, http://english.chosun.com/w21data/html/news/200806/200806090015.htm.

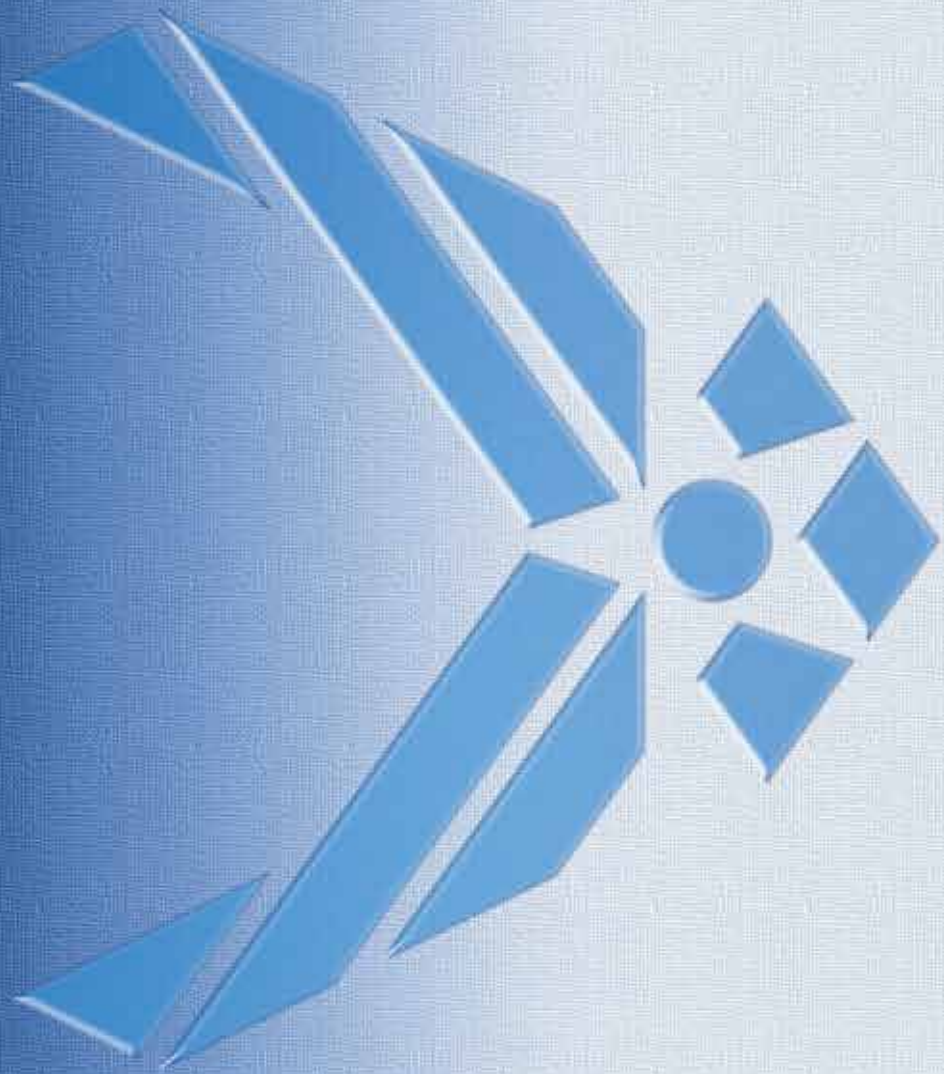
57. The United States and the ROK could make such threats privately to the North Korean regime to have the best chance at deterrence.

58. A laser weapon to shoot down artillery was developed years ago in the United States and could jumpstart ROK efforts.

59. Malcolm Moore, "North Korea now 'fully fledged nuclear power,'" *Telegraph* (UK), 24 April 2009, http://www.telegraph.co.uk/news/worldnews/asia/northkorea/5212630/North-Korea-now-fully-fledged-nuclear-power.html.

COMING SUMMER 2013
ASIA-PACIFIC
SPECIAL EDITION

SSQ STRATEGIC STUDIES QUARTERLY WINTER 2012 AU PRESS



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