

Returning to Fundamentals:
Deterrence and U.S. National
Security in the 21st Century

The George C. Marshall Institute

The George C. Marshall Institute, a nonprofit research group founded in 1984, is dedicated to fostering and preserving the integrity of science in the policy process. The Institute conducts technical assessments of scientific developments with a major impact on public policy and communicates the results of its analyses to the press, Congress and the public in clear, readily understandable language.

Copyright © 2011

All rights reserved. No part of this book may be reproduced or transmitted in any form without permission from the George Marshall Institute.

Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century

George C. Marshall Institute
Washington, D.C.

About the Authors

Dr. Robert Butterworth

Dr. Robert Butterworth is the President of Aries Analytics, a company which provides market analyses and program development services to government, commercial and non-profit clients concerning space and space-related research and development.

Dr. Butterworth was recently Chief of Air Force Space Command's Strategic Planning, Policy, and Doctrine. He has served on the staff of the President's Foreign Intelligence Advisory Board, the Senate Select Committee on Intelligence, and at the Department of Defense. He was also responsible for the review and oversight activities, budget support and program analyses for selected space and intelligence activities.

Dr. Butterworth is a member of the Marshall Institute's Board of Directors.

Mr. Peter Marquez

From 2007-2010 Peter Marquez served as the Director for Space Policy at the White House. In that role he oversaw the development, coordination, and implementation of President Bush's and President Obama's space policies. He led President Obama's formulation of June 28, 2010, National Space Policy.

Mr. Marquez's other duties in the White House included critical infrastructure protection and resilience, regional military and security issues, and military intelligence policy. The National Security Advisor also called upon him to lead several sensitive activities and programs.

After graduating, Mr. Marquez worked for the United States Air Force on classified space programs. Peter later served in the Office of the Secretary of Defense's directorate for Space Policy and then as a special assistant to the Under Secretary and Principal Deputy Under Secretary of Defense for Policy as the director of the Department of Defense's operational special access programs.

Mr. Marquez is a Fellow at the George C. Marshall Institute.

Born in Gilroy, California, in 1976, Mr. Marquez received a bachelor's degree in political science in and master's degree in space policy from George Washington University.

Dr. John B. Sheldon

Dr. John B. Sheldon is a Marshall Institute Fellow, and professor at the School of Advanced Air and Space Studies (SAASS), Air University, Maxwell AFB, Alabama. At SAASS he teaches and directs the Space and National Security and the Information, Cyber, and Intelligence Power courses.

Prior to his Marshall Institute and SAASS appointments, Dr. Sheldon was program director for Space Security at the Centre for Defence and International Security Studies, Henley-on-Thames, UK. Dr. Sheldon is also Editor Emeritus of *Astropolitics*, of which he was a founding co-editor, a peer-reviewed space policy journal published by Routledge, and has published numerous articles and chapters on national security space policy and strategy, cyberspace, and strategic theory.

Born and raised in the United Kingdom, Dr. Sheldon formerly served in the British Diplomatic Service, and received his BA (Hons.) in Politics and International Relations and MA in Security Studies from the University of Hull, UK, and his Ph.D. in Politics and International Relations from the University of Reading, UK. Dr. Sheldon now resides with his American wife in the United States. His weblog can be found at <http://johnbsheldon.com/>

Mr. Eric R. Sterner

Eric R. Sterner is a national security and aerospace consultant in Washington, DC. He has held senior Congressional staff positions as the lead Professional Staff Member for defense policy on the House Armed Services Committee and as Professional Staff Member and Staff Director for the House Science Committee's Subcommittee on Space and Aeronautics. He also served in the Office of the Secretary of Defense and as Associate Deputy Administrator for Policy and Planning at NASA.

In the private sector, Mr. Sterner served as Vice President for Federal Services at TerreStar Networks Inc., and as a national security analyst at JAYCOR and National Security Research Inc., where his work focused on the strategic implications of emerging technologies.

His work on national security, military history, and space issues has appeared in a range of publications, including *Strategic Studies Quarterly*, *The Washington Quarterly*, *Comparative Strategy*, *Journal of the British Interplanetary Society*, *The Washington Post*, *The Washington Times*, and *Aviation Week & Space Technology*, among others.

Mr. Sterner is a Fellow at the George C. Marshall Institute.

Mr. Sterner earned a B.A. in International Studies and USSR Area Studies from The American University and separate M.A. degrees in Political Science and Security Policy Studies at The George Washington University.

Table of Contents

Introduction	1
<i>Jeff Kueter and John B. Sheldon, Ph.D.</i>	
Nuclear Force Planning: Odin or Onan?	4
<i>Robert L. Butterworth, Ph.D.</i>	
Space Deterrence: The Prêt-à-Porter Suit for the Naked Emperor	9
<i>Peter Marquez</i>	
Deterrence in Cyberspace: Yes, No, Maybe?	20
<i>Eric Sterner</i>	
A Fatal Disconnect: Conventional Deterrence in a Nuclear-Armed World	28
<i>John B. Sheldon, Ph.D.</i>	

Introduction

Jeff Kueter and John B. Sheldon, Ph.D.*

Being prone to strategic amnesia on the one hand, and enamored with fads disguised as strategic insight on the other, what explains America's rediscovery of deterrence in these past few years? After a period of seeming strategic excess, senior officials and military officers have come to realize that the United States cannot do everything; that some threats to national security are either immutable or intractable and that preemptive and preventive military action is unable to deal with them effectively. National security thinkers have trotted out deterrence, the ruling strategic paradigm of the Cold War, as the answer to these myriad, diffuse, and stubborn threats.

In reality deterrence never went away, it remained as background noise to the perceived strategic priorities in Afghanistan, then Iraq, and then Afghanistan again. Since the end of the Cold War the U.S. has maintained a comparatively large nuclear arsenal (despite the periodic cuts in warheads during the past two decades) that is supposed to be the strategic backstop for U.S. national security when and if all else fails. U.S. conventional forces also serve as a deterrent to the majority of entities that could plausibly threaten the U.S. directly, or threaten its interests abroad. The awkward fact is that the absence of a WMD attack, or a conventional attack by another state, against the U.S. is not, ipso facto, evidence that this overall force structure has actually *deterred* potential wrongdoers. The problem with deterrence is that, like intelligence, one is only confronted with its intricacies, nuances, and shortcomings when it fails. Successful deterrence is impossible, or almost so, to gauge. After all, how do we know that Cold War deterrence through mutual assured destruction actually worked? Sir Michael Howard once made such a claim when he wrote, "What is beyond doubt, however, is that we effectively deterred the Soviet Union from using military force to achieve its political objectives ...,"¹ yet equally plausible is the explanation that Soviet leadership was just as reluctant to start a nuclear war as Western leaders, and for largely the same reasons, of which deterrence may not have been one.

This pause for thought aside, the Cold War often evokes nostalgia among those concerned with and about deterrence. In those days, the enemy was easily identifiable, its capabilities were largely known, and entire bureaucratic entities and large swathes of Western academia were devoted to gleaning its intentions. Some pine for those halcyon days, often forgetting that for all of its conceptual simplicity (and this is a simplicity only understood with the luxury of hindsight) we lived under the appalling shadow of utter nuclear annihilation. If deterrence had failed before 1989 very few would have survived to debate its finer points. Today's threats are myriad, diffuse, and often hard to gauge with any measure of comforting certainty and accuracy, even though the meta-existential element of nuclear annihilation or global war has largely

* The views expressed here by John B. Sheldon, Ph.D., are his own, and do not reflect or represent in any way the views or policies of the School of Advanced Air & Space Studies, Air University, the Department of the Air Force, Department of Defense, or the U.S. Government.

¹ Sir Michael Howard, "Lessons of the Cold War," *Survival*, Vol. 36, No. 4, Winter 1994-95, p. 161.

receded. This is not to suggest that the possible threats we face are not serious, but they do not threaten to remove human civilization as we know it from the face of the earth, at least for the time being. That's the good news. The bad news is that among the U.S. and other Western powers, deterrence, like the work of Carl von Clausewitz, is often invoked more than it is understood.

Deterrence is about deterring war, not attacks against capabilities in particular domains. Deterrence demands that senior officials signal to adversaries—actual and potential—that certain actions from them which threaten U.S. national security and critical interests will elicit certain responses to protect national security and defend those critical interests. Such signaling uses scarce diplomatic and political capital, and it is also an exercise in credibility. It is strange that such scarce capital should be wasted on attempts to deter attacks in the space and cyber domains while at the same time signaling to such adversaries that we care more about attacks against satellites and network penetrations than we do about any wider conflicts. Such thinking must leave adversaries wondering just how serious the U.S. is about its national security, concomitant interests—and deterrence. This is not to say that space and cyber deterrence do not have a role, but this role must be subservient to a wider deterrence approach that provides linkages between the space and cyber domains and the other strategic domains, as well as to wider U.S. interests.

Misconceptions abound about deterrence in its contemporary context, particularly in official statements and documents. For example, the Chairman of the Joint Chiefs of Staff, Admiral Michael Mullen, recently called for a “new model for deterrence theory.”² Is Admiral Mullen challenging a deficiency in the body of deterrence theory, or rather, how that theory is applied to a complex contemporary strategic environment? More worrisome than this is the popular idea that the overall objective should be to deter.³ This opinion infers some unique insight into how much is enough for deterrence to be achieved. Given the diffuse nature and growing number of contemporary threats, and the fact that many of them cannot be reliably verified by traditional technical means, how can anyone plausibly claim that they know how much deterrence is enough? Another concern is the idea that niche areas of capability, such as space and cyberspace, require their own deterrence strategies in order to deter others from attacking U.S. interests in these domains. This idea is false. Furthermore, such an approach dangerously deters us from using these critical domains to their fullest capacity to further our security and interests. It also misses the point of deterrence and, in turn, wastes both capability and scarce diplomatic and political capital.

The following essays seek a return to deterrence fundamentals. Each author believes that the U.S. has lost its intellectual compass in conceptualizing deterrence and in implementing policies and strategies intended to deter. The first essay, by Robert L. Butter-

² Michael G. Mullen, “It’s time for a new deterrence model,” *Joint Force Quarterly*, No. 51, (4th Quarter), 2008, p. 3.

³ See, for example, General Kevin Chilton, USAF, and Greg Weaver, “Waging Deterrence in the Twenty-First Century,” *Strategic Studies Quarterly*, Vol. 3, No. 1, Spring 2009, pp. 31-42. One wages war, not deterrence. The successful waging of war can have great deterrent value.

worth, Ph.D., explores the many challenges facing U.S. nuclear forces in the coming years and their role in deterrence. He writes that, in pursuing deterrence, “the country is seeking security through a concept that requires unavailable data about unknown processes, that is not empirically testable, and that cannot be shown to be working.”

The next essay, by Peter Marquez, formerly of the National Security Council, examines current thinking and strategies on space deterrence and finds both lacking in substance. Marquez writes, “Policy makers need to remember that deterrence is a gamble and when it comes to deterring hostile acts against our space systems, the U.S. currently has a very bad hand and a lot of chips on the table. Deterrence should not be viewed as a replacement for defense or a less expensive way to protect our satellites.”

Eric Sterner, a former staff member on the House Armed Services Committee, who has also served in the Office of the Secretary of Defense and as an Associate Deputy Administrator at NASA, examines the emerging cottage industry of cyber deterrence and concludes that, “for its security, the United States must depend on its ability to prevail in a cyber conflict—which may, or may not be associated with an armed conflict or even a state. The front line is not deterrence of attack, but the interaction of attack and defense at the point of attack ... Whether they do so in a manner sufficient to deter an attack or affect an attacker’s choices about ends and means remains to be seen, but such possibilities suggest deterrence as a concept is not a lost cause in cyberspace. Even so, we have a long way to go in making it so.”

John B. Sheldon, Ph.D., a professor at the School of Advanced Air & Space Studies, Maxwell AFB, Alabama, and a former British diplomat, takes a critical look at the challenges facing conventional deterrence in the coming era of austerity, and calls for the end of the contrived conceptual separation of conventional and nuclear deterrence. He writes that it is “nonsensical to speak of nuclear or conventional deterrence, because to do so is to imply that the theory and logic required for each is somehow different when in fact it is not. There is no such thing as nuclear or conventional deterrence—there is, in stark reality, only deterrence that applies across the vertical spectrum of conflict and the horizontal spectrum of means.”

In the spirit of intellectual honesty and candor, these essays aim to provide the material for further public debate on this vitally important topic. All of these authors assert the idea that it would behoove all who are concerned with U.S. national security—and with furthering and protecting U.S. interests—to reacquaint themselves with the rich body of deterrence theory and strategic theory. Doing so will outfit the U.S. to avoid the worst excesses of gross misconception and self-referential wishful thinking, while advancing the probability that the intrinsic value of our strategies, force structure, and capabilities designed to prevail in any given scenario *might* have the beneficial outcome of really deterring our adversaries.

Nuclear Force Planning: Odin or Onan?¹

Robert L. Butterworth, Ph.D.^{*}

Over the next twenty-five years or so, the United States plans to recapitalize its triad of submarines, bombers, and missiles that deliver strategic nuclear weapons, building new versions of these weapons to extend a fifty-year-old force structure for another half century. Yet today's strategic environment is not that of the 1960s, and tomorrow's may differ even further, if only because of regional nuclear powers and non-state adversaries. Are the challenges of that environment best met by replicating, presumably with fewer weapons, a force structure intended to survive, at least in part, a massive Soviet attack? And is the thinking that produced the earlier plans the best way to approach future challenges?²

A Hope, Not a Plan

The central concept underlying the current force structure, of course, is deterrence, an aspiration embraced in the nuclear era as a default option imposed on military planners by weapon technologies. Unable to prevent a comparably-armed enemy from destroying the U.S., Americans could only hope to avoid being disarmed. What the surviving weapons would be used for is the subject of Presidential guidance and has long been debated, but the ability to retaliate, whatever the targets, was thought to provide the best achievable response to mortal threats.

The threat to use nuclear weapons, however, proved difficult to extend when the challenges were less than immediate and dire. If invoked to deter minor harassments, the threat of massive retaliation would seem almost risible, defying the perceptual conventions of proportionality and connectedness.³ And if the possession of nuclear weapons by the U.S., the only country to have used atomic weapons in war, posed an implicit threat, it was not enough to preclude problems of flexible response, compellence, escalation, and conflict termination.⁴

¹ A version of this essay was published at <http://defense.aol.com/2011/07/18/is-nuclear-deterrence-out-of-date/>.

² The House Armed Services Committee is asking similar questions and notes that "the assumptions and scope of cold war-era nuclear analyses are vastly different than what is needed today. Today's geopolitical environment presents a diverse range of new threats and opportunities." Report on Department of Defense Authorization Act for FY 2012, p. 220.

³ Or so it seemed, at least, in the eyes of American planners; the threat of devastating retaliation has not been tested in practice, though it might have been had the U.S. not quickly modified the first public expressions of the 1953 massive retaliation policy. The classic analysis of this case is William W. Kaufmann, "The Requirements of Deterrence," in William W. Kaufmann, ed., *Military Policy and National Security* (Princeton, N.J.: Princeton Univ. Press, 1956), 12-38.

⁴ "In every case, whatever the nations involved, devastation could reach such proportions that a nation's very existence would have to be threatened before it would consider using its atomic arsenal. For the rest, one must accept the notion of a *fait accompli*. If Soviet pursuit planes force down an American plane or if American artillery opens fire on a Soviet plane, nothing happens. Nothing happens—except diplomatic protests and demands for indemnities—because nothing can happen. . . . The devastation would so obviously be out of all proportion to the misdemeanor that such a war is unthinkable." Pierre Galois, *The Balance of Terror: Strategy for the Nuclear Age* (Boston, MA: Houghton Mifflin, 1961) p. 8.

Whether tests like these might be deterred in the future has become a popular question. Seminars, workshops, conferences, and interagency working groups have been considering how deterrence might be pursued to forestall land, sea, air, space, and cyber threats. At least one panel at a forthcoming conference, for example, asks not how deterrence might help the U.S. with recent developments in the Middle East, but rather what those developments might tell us about deterrence. And to a former commander of Strategic Command the policy primacy of the concept was unquestioned: "The concept of deterrence is sound," he wrote, "and we have the means necessary to implement it against the full range of threats that are reasonably susceptible to deterrence. The challenge that remains before us is to allocate the resources and create the processes necessary to proactively and successfully 'wage deterrence' in the Twenty-First Century."⁵ Also of note in this regard is the recent emphasis in defense policy on the alleged deterrent effects of entangling U.S. security programs with those of other countries, in the hope that common interests could be fertilized and would-be aggressors confronted with a larger status quo coalition. Over the past year, for example, various Pentagon leaders have urged that we replace half the GPS constellation with the satellite navigation systems of Europe, Russia, and China, and that we design and operate spy satellites jointly with allies.⁶

But deterrence is an emergent property of circumstances that are often quite complicated and only partly known, and is correspondingly difficult to use as a general guide for planning.⁷ The search for meaning is frustrated by the recourse to accounting-style tautologies about balances of costs and gains, risks and rewards, and by simplistic models portraying only military threats between two unitary actors who experience payoffs or outcomes determined by the product of coherent strategic choices decided on the basis of expected-value maximization. The inability to specify critical values and relationships a priority makes these approaches vacuous.⁸

⁵ Kevin Chilton and Greg Weaver, "Waging Deterrence in the Twenty-First Century," *Strategic Studies Quarterly* (Spring 2009), pp. 31-42, accessed 13 March 2009 on web at www.au.af.mil/au/ssq/Spring/chilton.pdf

⁶ Such proto-Functionalism would make David Mitrany proud. Decades of research have found no dependable association between interstate transaction flows and peaceful relations. General Cartwright, vice-chairman of the Joint Chiefs of Staff, advanced the GPS argument in several fora last year; Deputy Secretary of Defense Lynn announced plans for spy-satellite co-production in a speech at Strategic Command last fall.

⁷ Freeman Dyson found that deterrence is not a useful strategic concept because "that word has too many meanings. Any deployment of weapons by one country, with the aim of dissuading another country from doing something disagreeable, is a form of deterrence." He cites the forty million gas masks deployed by British civil defense in 1939 as an example. Recognizing the problem, analysts generally tried to bound it by describing particular types or circumstances in which deterrence might be found. Kahn, for example, had three types; John Sheldon was more comprehensive and described seven. Herman Kahn, *On Thermonuclear War* (Princeton, N.J.: Princeton University Press, 1960), pp 282ff; John Sheldon, "Space Power and Deterrence: Are We Serious?" paper presented at the George C. Marshall Institute's Washington Roundtable on Science and Public Policy, 13 November 2008, available at <http://www.marshall.org/article.php?id=616>

⁸ The outcomes, as Snyder noted, must be quite broad, reflecting overall expectations, including factors separate and apart from expectations about what might be experienced at the hands of the other party, and taking into account possible changes in the status quo regardless of what action either might take. The challenge for practical applications is to identify and measure operational indicators of these elements, as well as such additional complications as communications gaps, command and control weaknesses, and inertia. Glenn H. Snyder, "Deterrence and Defense: A Theoretical Introduction," in Richard G. Head and Ervin J. Rokke, eds., *American Defense Policy* (Baltimore: Johns Hopkins University Press, 3rd ed., 1973), pp. 99-112; p. 110.

Nor is there much planning guidance to be gained (yet, at least) from historical research. As a practical matter, it has been virtually impossible to show who was deterred from what and why. Credible information is practically never available in the detail required to characterize the actors, interests, perceptions, decisions, and expected outcomes well enough to prove cause and effect.⁹ Lack of such proof invites simple logical errors of the lurking post hoc fallacy together with potentially dangerous misperceptions of how arms and influence might transpire in particular circumstances. Similar problems challenge nearly every attempt to pursue policies and programs aimed at creating deterrence, whatever the type or degree of analytical complexity, owing to a shared morphological paradox: adversary expectations are (a) the central focus and measure of merit for policies and programs, while they are (b) characterized almost exclusively by introspection and a priori speculation. Projective psychology is the essence of deterrence policies, and the temptation can be overwhelming to sketch the adversary in ways that best accommodate the options that one is most inclined to pursue.

Empirical data can help, of course. Post mortems of challenges that occurred even before the nuclear age can increase awareness of the possibilities of surprise, of how things can go wrong, of the merits of different styles of leadership and decision-making and crisis management. But the lessons for deterrence are inevitably situation-specific.¹⁰ Should commitments be expressed or implied, unbending or flexible, defined early or later? Should responses be automatic or subject to decisions at the time? Does having a range of capabilities undercut or increase the credibility of the threat? History answers these and related questions with Yes and No. One analyst illustrated the complexities by summarizing failures of deterrence as shown in the table on the facing page.

Moreover, even when empirical data about adversary views and calculations are unambiguous, they may have little to do with structuring the policies and programs intended to create the conditions for deterrence, even when the stakes are extremely high. The U.S. did relatively little, for example, to make its nuclear posture score highly in the warfighting terms with which the Soviet Union assessed the correlation of forces; the introduction by Secretaries Schlessinger and Rumsfeld of limited strategic options was opposed by many Americans who feared that the policy would make nuclear weapons more usable. This chronic tension between making the force credible but usable only in extremis remains another illustration that the pursuit of deterrence as a practical matter can only be determined by the situation at hand. "Tailored deterrence" is a redundancy.

⁹ "Historical support for the idea that calculation of probabilities of success in terms of the prewar balance of forces exerts a decision effect on deterrence would have to come from cases in which a government wished to start a war, but refrained because the balance was insufficiently favorable. Clear examples of this sort in the last half-century are hard to find." Richard K. Betts, "Conventional Deterrence: Predictive Uncertainty and Policy Confidence," *World Politics* 37:2 (January 1985), p. 155.

¹⁰ Smoke and George found that deterrence below the assured destruction (what they call the "strategic") level "is very largely a *context-dependent* problem" (emphasis in original). Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), p. 54.

Conditions to Deter	Causes of Deterrent Collapse
Preemptive war	Deterrer becoming too strong
Preventive war	
Enemy optimism	Deterrer too weak
Calculated risks	
Miscalculation	Deterrer's strength irrelevant
Accidental war	
Catalytic war	
Irrational acts	
Source: Collins, "Principles of Deterrence" ¹¹	

If You Want Peace ...

Deterrence, in sum, can be a desirable goal but an impossible guide. In pursuing it the country is seeking security through a concept that requires unavailable data about unknown processes, that is not empirically testable, and that cannot be shown to be working.¹² In practice, American interests are challenged typically when an adversary doing something that the U.S. wants to stop or reverse. Such compellence tasks are different analytically and operationally from deterrence, and deterrence postures, which enshrine responses to the initiatives of others, are poorly suited to managing them.

Moreover, deterrence logics can encourage second-order effects that undercut preparations to fight and win wars. American policy has long insisted on a force posture that encourages deterrence, and that also provides the ability to win the fight should deterrence fail. It is no easy matter to design a force structure that optimally serves both objectives. Strong defensive capabilities might exert a powerful deterrent effect, and so might weak ones; similarly, weak or strong defenses might create little

¹¹ John M. Collins, "Principles of Deterrence," *Air University Review* (November-December 1979).

¹² The Defense Department claimed in 2006 to have a handbook that "outlines the ways and means necessary to achieve the end of deterrence" and that offered "a means of evaluating the effectiveness of alternative deterrence choices" (Deterrence Operations Joint Operating Concept, p.6). The document reports the answer to achieving deterrence is to influence adversaries' perceptions of the benefits of a course of action, the costs of that course of action, and the benefits and costs of not taking that course of action. The means of evaluating alternative deterrence choices include identifying and measuring variables of importance to the adversary, together with the expected impact of "deterrent actions" (p. 53). Department of Defense, "Deterrence Operations Joint Operating Concept," Version 2.0, 2006.

deterrence.¹³ But emphasizing the deterrent purpose can produce a force with less warfighting capability, which in some settings could in turn undercut deterrence.¹⁴

These considerations might have little consequence if tomorrow's world could safely be assumed to replicate yesterday's. But it seems sure to be quite different, involving difficult challenges from adversaries armed with at least a few nuclear weapons—adversaries that might be regional powers, global contenders, or non-state terrorists. Kehler's 1996 warning remains true today: "Operations against a regional adversary either having or presumed to have nuclear weapons would present problems that have never been directly faced and are not yet fully understood."¹⁵ Absent a Cold War competition in which core national values were at stake, the credibility of American threats might not be so immediately evident to all. There might then be situations in which American credibility would require clear demonstrations of capability; perhaps events might even compel U.S. leaders to consider using one or two nuclear weapons.

Preparing for a future of that sort entails rethinking core elements of the strategic planning paradigm developed fifty years ago. Will assured destruction continue to be the best available strategy to prevent nuclear attacks against the American homeland? Should it be reinforced and eventually replaced with defenses as they become increasingly effective? Should American nuclear forces be more versatile, flexible, and capable of engaging diverse targets around the world with precise and precisely limited effects? Should nuclear testing be resumed, with a view to developing such weapons? Should delivery systems include in-flight retargeting and termination? Is there a continuing need for land-based ICBMs? Will there be a need for some conventionally armed ICBMs? How might limited nuclear operations be integrated with forces for the joint fight? Is there a role for allies in these matters, and how might alliances be structured to deal with them?

Rethinking these questions and the many others that will then arise poses a vital challenge to planning and to the political consensus that has sustained the American approach to strategic affairs for a half-century and more. The planned modernization of the strategic delivery systems provides an opportunity to do so, and the changing strategic environment demands that we take it. After all, it may not only be our hardware that is out of date.

¹³ "Deterrence does not vary directly with our capacity for fighting wars effectively and cheaply." Snyder, *op.cit.*, p. 100. Betts expands the point: "Many deterrence theories focus on military variables—force structure and doctrine—as the constraints that drive political decision. . . . Strategic decision does not follow laws of mechanics because risk, misperception, and miscalculation are subjective phenomena. Measurable elements constrain choice, but do not determine it." Betts, *op.cit.*, p. 177.

¹⁴ Some of the early arguments advanced for the strategic defense initiative, for example, insisted that the performance of American ballistic missile defenses would be sufficient if they simply made Soviet leaders more uncertain about the effectiveness of their offenses. The emphasis on deterrence might also encourage a kind of Maginot Line mindset, in which the initiative is left to the aggressor.

¹⁵ C. Robert Kehler, "Nuclear-Armed Adversaries and the Joint Commander," *Naval War College Review* XI:IX (Winter 1996), pp. 7-18.

Space Deterrence: The Prêt-à-Porter Suit for the Naked Emperor¹

Peter Marquez

“The objective of keeping space immune from conflict appears unrealistic unless one can also eliminate the political warfare that underlies it.” (Bloomfield, 1965)

The concept of “space deterrence” is now in vogue. The idea behind the concept is that the United States would prevent attacks on our satellites by deterring hostile actors. How would one deter or respond to a hostile act in space? A more fundamental question is, should the U.S. expend the resources to potentially reduce the probability of a hostile act in space? Even if the U.S. could develop the capabilities necessary to deter an attack when would the U.S. be willing to respond with violence when the deterrent failed?²

Defending space systems is critical due to the strategic capability and force multiplier effect derived from them.³ The U.S. should undertake initiatives that mitigate the effects of a hostile attack on U.S.-utilized space systems.⁴ But is space deterrence the keystone for this overarching initiative?

Recently posited theories of space deterrence misuse the term deterrence; they do not grasp the intent of deterrence, the full range of other security constructs, and, most importantly, what should be done when, not *if*, deterrence fails. Compounding this situation is the growing belief that deterrence is an element of defense. This essay attempts to lay bare the futility of a space deterrence construct and also provides potential options for achieving the goal of assuring critical missions enabled by U.S. national security satellites.

¹ With sincerest flattery to Oran R. Young and his review titled “Professor Russett: Industrious Tailor to a Naked Emperor” in *World Politics*, Vol. 21, No. 3, 486-511.

² As William Kaufmann noted, “In principle, then, the requirements of deterrence are relatively simple. In practice, however, they turn out to be exceptionally complex, expensive, and difficult to obtain.” (Kaufmann, 1956)

³ Presidential Decision Directive 4 (PDD-4), “National Space Policy”, June 28, 2010, describes this critical dependency; “The utilization of space has created new markets; helped save lives by warning us of natural disasters, expediting search and rescue operations, and making recovery efforts faster and more effective; made agriculture and natural resource management more efficient and sustainable; expanded our frontiers; and provided global access to advanced medicine, weather forecasting, geospatial information, financial operations, broadband and other communications, and scores of other activities worldwide. Space systems allow people and governments around the world to see with clarity, communicate with certainty, navigate with accuracy, and operate with assurance.”

⁴ The President directed the departments and agencies of the Executive Branch to achieve the goal of increasing assurance and resilience of mission-essential functions in PDD-4.

Deterrence and Compellence Defined

For the purpose of this discussion it is important to clearly define coercion, deterrence, and compellence. This fundamental exercise is required because some arguments regarding space deterrence have confused deterrence, compellence, defense, and offense.⁵

Coercion attempts to influence an adversary's behavior by imposing costs, through violence, diplomacy, economics, or the threat of imposing costs for the purpose of limiting the adversary's options and/or affects the adversary's assessment of the costs and benefits of its options—in particular, the options that are counter to the wishes of the coercer. A coercer can demand the adversary act in a certain way or refrain from acting in a certain way.⁶

Deterrence, an element of coercion, is the process of influencing an adversary's political and military risk calculus by making its leaders understand that the cost of taking specific actions is of no value or too great. Deterrence works by making an adversary believe that it has a low probability of achieving its goals, known as denial of benefit, or that the punishing response of the target will be greater than any benefit gained through the adversary's action. Deterrence asks an adversary to refrain from taking action.^{7, 8}

Deterrence requires three overt elements; attribution, signaling, and credibility. The coercer must maintain and demonstrate the capability to attribute acts of malfeasance by the adversary. In this case it means the U.S. requires a demonstrated capability to attribute attacks on our satellites. Secondly, the coercer must provide clear signals that it considers certain acts to be counter to its interests. This means the U.S. would need to publicly enunciate what it considers to be acceptable and non-acceptable behavior in space. In practice this could take the shape of confidence building measures, treaties, or red lines. Finally the U.S. must develop, maintain, and exhibit willingness to use power to punish hostile actions- this is the credibility that the U.S. will act when threatened or attacked.⁹ Unless all these components are overt, the coercer will find themselves in a Strangelovian Doomsday Device situation.¹⁰

⁵ See Harrison, R. G., Jackson, D. R., & Shackelford, C. G. (2009). Space Deterrence: The Delicate Balance of Risk. *Space and Defense*, 3 (1), 1-30.

⁶ Schaub Jr., G. (2004). Deterrence, Compellence, and Prospect Theory. *Political Psychology*, 25 (3), 389-411.

⁷ Kaufmann, W. W. (1956). The Requirements of Deterrence. In W. W. Kaufmann, (Ed.), *Military Policy and National Security*. Princeton: Princeton University Press.

⁸ George, A. L., & Smoke, R. (1974). *Deterrence In American Foreign Policy: Theory and Practice*. New York: Columbia University Press.

⁹ Schelling stated this very clearly, "To project the shadow of one's military force over other countries and territories is an act of diplomacy. To fight abroad is a military act, but to persuade enemies or allies that one would fight abroad, under circumstances of great cost and risk, requires more than a military capability. It requires having those intentions, even deliberately acquiring them, and communicating them persuasively to make other countries behave." in Schelling, T. C. (1966). *Arms and influence*. New Haven: Yale University Press.

¹⁰ Dr. Strangelove, "Of course, the whole point of a Doomsday Machine is lost, if you keep it a secret! Why didn't you tell the world, eh?" Ambassador de Sadesky, "It was to be announced at the Party Congress on Monday. As you know, the Premier loves surprises."

Compellence, deterrence's sibling, is the process of using influence to create a desired action. Far from being a derogatory term, "compellence" is an often underappreciated component of statecraft in which the coercer demands an adversary take desired action through "carrot" or "stick" incentives.^{11, 12}

Deterrence is coercing an adversary to maintain its current behavior and/or expected path and refrain from actions not in the interest of the coercer. Compellence is coercing an adversary to break its current behavior and/or expected path and act in a manner more in the interests of the coercer.

Both deterrence and compellence require the coercer to expend significant resources to shape an adversary's risk calculus. This calculus is based on how the adversary perceives: 1) the benefits of a course of action; 2) the costs of that course of action; 3) the probability of various responses from the target country; and 4) the probability of achieving the objective.¹³ Cumulative prospect theory posits that compellence requires significantly more effort on the part of the coercer to change the expected path of the adversary.^{14, 15} This means that if the U.S. needed to compel an adversary it would require greater political, military, and economic resources than deterring an adversary.

Coercion is but one tool that should be utilized for a comprehensive range of options for responding to hostile acts. Furthermore, coercion is not an end-state but is a fluid position that requires constant review and updating as the capabilities and intentions of the U.S. and adversaries change.

With coercion, deterrence, and compellence defined, it is also important to note what deterrence is not. Deterrence is not defense. Deterrence is a political high-stakes gamble with the intent of convincing an adversary to not take a specific action.¹⁶ Defense is the actual possession of capabilities, materiel and non-materiel, that will protect against or mitigate attacks by an adversary. A good defensive capability can

¹¹ Schelling, T. C. (1966). *Arms and influence*. New Haven: Yale University Press.

¹² Freedman, L. (1998). Strategic coercion. In L. Freedman (Ed.), *Strategic Coercion: Concepts and cases* (pp. 15-35). New York: Oxford University Press.

¹³ Snyder, G. H. (1961). A Theoretical Introduction. In G. H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (pp. 12-13). Princeton: Princeton University Press.

¹⁴ Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*, 5, 297-323.

¹⁵ Cumulative prospect theory, as differentiated from expected utility theory, posits that a coercer must carefully calculate the prospective values an adversary places on certain gains and losses, not how the coercer values those items, and the adversary's belief in the probability of incurring those gains or losses. Expected utility theory, in some instances, assigns a constant value to certain probabilities whereas prospect theory takes into account the psychological biases of an adversary and, for example, allows for an adversary that is either risk-averse or risk-acceptant. I have oversimplified the nuances of cumulative prospect theory for the purposes of brevity and clarity but for an excellent discussion of the application of cumulative prospect theory to deterrence and compellence please read Gary Schaub in "Deterrence, Compellence, and Prospect Theory"

¹⁶ Or, in the case of compellence, it is gambling with the intent of making the adversary believe that the pain of non-compliance outweighs defying the coercer.

enhance deterrence but defense will always be needed when deterrence fails. Said another way, deterrence requires defensive capability but defense ultimately operates in the absence of deterrence.

It should also be noted that formalized coercion theory is still relatively new. A constant refrain in nearly every academic critique of deterrence, especially rational deterrence theory, is that no empirical evaluation of the theory exists and in the instances where specific case studies were evaluated against coercion theories the expected results did not match the predicted outcome. Lebow and Stein stated this clearly, “The problem with rational models is not that they contain idealizations but that these idealizations are fundamental to their assumptions. Such assumptions as the rational decision maker, perfect information, and apolitically neutral environment are idealizations that lack any empirical referent. Rational deterrence theories are accordingly “theories” about nonexistent decision makers operating in nonexistent environments.”¹⁷

Coercion and, by extension, deterrence theory was mostly developed for large-scale strategic conflicts—nuclear war or massive conventional force conflict. Many theorists believe that coercion theory at this macro level can be scaled down to handle regional skirmishes, non-state actors, limited war, or other “substrategic” conflict. Unfortunately substrategic conflicts are vastly more complex to predict via existing coercion theory models. Substrategic situations are more dependent on contextual issues and variables making the scenarios more dynamic and ambiguous.¹⁸ Much of the coercion theory intended for use in space was developed for a situation where both actors had a gun pointed at the other’s head. The issues in space today are not the same as those faced in the Cold War.

In light of all this, should the U.S. be willing to gamble its strategic space advantage on a generalized theory?

Detering Hostile Acts, Compelling Security, and Assuring the Mission

So how do policy makers and military commanders “do deterrence” for space? What is the U.S. trying to deter? How does compellence fit into the equation? Is deterrence necessary for space? Are deterrence and/or compellence even practical for space? These questions are germane to the debate.

Going back to the foundational premise that U.S. space systems are critical to national security, a situation arises where the vital functions performed by those spacecraft must be assured. The U.S. must protect those missions and convince adversaries that there is no overall benefit to be gained by attacking the U.S. satellites that enable those missions. Therefore the purpose of coercion, as applied to U.S. satellites, is to keep

¹⁷ Lebow, R. N., & Stein, J. G. (1989). Rational Deterrence Theory: I Think, Therefore I Deter. *World Politics*, 41 (2), 208-224.

¹⁸ George, A. L., & Smoke, R. (1989). Deterrence and Foreign Policy. *World Politics*, 41 (2), 170-182.

an adversary from attacking satellites and threatening the security of the U.S. and its allies and, when that fails, responding with force.^{19, 20}

At this juncture it must be asked, who are these nebulous adversaries? What capabilities do they have? What are their intentions? What capability does the U.S. have to detect attacks from these adversaries (attribution)? Does the adversary know what behaviors the U.S. finds hostile (signaling)? What has been the U.S. response to previous hostilities against U.S. satellites, when would the U.S. be willing to react, and with what capabilities (credibility)?

First, coercion, deterrence, and compellence do not work blindly in domains. There is no sea, air, or land deterrence. For deterrence to be effective it must take into account the motivations of a specific actor and how that actor perceives the capabilities and motivations of the U.S. An operating domain, like airspace or land, has no motivations or interests. Deterrence has to be specific to the players and the values they assign to all probable outcomes. Space deterrence promoters think this capability can be purchased “off-the-rack” and will fit all scenarios and actors but deterrence must be custom tailored for the coercer and the target.

Effective deterrence is dependent upon: the actor to be deterred; when to deter the actor (e.g., peace, pre-hostility, war); what specific action(s) must be prevented; what specific capabilities are to be protected; and how to respond if deterrence fails (violence, economics, unilateral sanctions, multilateral condemnation, private admonishment, etc.). Here, because there are a multitude of variables and dependent specific values assigned by the adversary and coercer, the application of a grand unified theory of “space deterrence” fails. You deter an actor not a domain.^{21, 22}

Who is the U.S. trying to deter? For the sake of simplicity, potential hostile actors can be placed in two categories: global powers and regionalists. The global powers are China and Russia. Both nations have global security interests and the capacity for global military and economic power projection. China and Russia have developed weapons that can attack U.S. satellites and both nations have exhibited previous political willingness to use those weapons. These near-peers form the clearest immediate threat to U.S. space security. The regionalists are actors who either have or

¹⁹ This principle is codified in the U.S. National Space Policy, “The United States will employ a variety of measures to help assure the use of space for all responsible parties, and, consistent with the inherent right of self-defense, deter others from interference and attack, defend our space systems and contribute to the defense of allied space systems, and, if deterrence fails, defeat efforts to attack them.

²⁰ The overall purpose of this coercion, and deterrence, is not to protect the satellites but to ensure the continuity of the services performed by the satellites.

²¹ George & Smoke, 1989

²² Alexander George and Richard Smoke made this point, “The formulation of contingent generalizations is necessary in order to capture the fact that deterrence is characterized by the phenomenon of what the General Systems Theory refers to as ‘equifinality’...Equifinality refers to the fact that similar outcomes on a dependent variable (e.g., deterrence failures) occur as a result of different causal processes, thus making the search for robust universal causal generalizations infeasible.”

may develop counterspace capabilities for the purposes of defending their national and regional interests. The regionalists lack either the capability or political willingness to destroy U.S. space systems but they may have capabilities that the U.S. considers non-existential threats (e.g., communications or ISR jammers). Examples of countries in this category are North Korea, Iran, and India.²³

China, Russia, and the U.S. have global interests and the U.S. enjoys tremendous asymmetric advantages due to its space capabilities, so it should come as no surprise that China and Russia pose the greatest immediate threat to U.S. satellites. Political realism accurately predicts that China and Russia would develop the capacity to hold U.S. satellites at risk. Following the realist philosophy one can assume with high confidence that China and Russia believe the U.S. maintains a capacity to attack their satellites and any other elements of global power projection.²⁴

The regionalists are more concerned with regional geopolitical dynamics. They do not intend to hold all U.S. space systems at risk or pose an existential threat to the U.S. but rather they would attack those capabilities that threaten their interests. Examples of this are Iranian and Libyan jamming of communications satellites. Attacks from these nations do not threaten the wholesale security of the U.S., but because the U.S. has not responded to previous attacks from these actors, the results may have hurt U.S. credibility.

Unfortunately, the U.S. does not have the capability to deter these actors. From a military standpoint the U.S. is unlikely to bomb Iran or North Korea because they jammed a communications satellite. From a diplomatic and economic standpoint there are few levers the U.S. has not already pulled regarding sanctions, freezing of assets, embargoes, etc. Some have stated that the U.S. should take action against these actors for jamming the satellites of the U.S. and its allies. It is unclear what action we should take that would convince the aggressor to stop its activities. In the case of Iran, for example, the Iranians have threatened an ally, Israel, are developing nuclear weapons, and have held U.S. citizens hostage. Are we to believe that the U.S. taking a strong stance about the jamming of a satellite will be the issue that causes the Iranians to change their ways?²⁵ The U.S. has already punished many of these nations and they continue to act undeterred. Obviously deterrence through punishment and cost

²³ I include India in this category not because they threaten the United States but because they have stated a desire to potentially develop and deploy anti-satellite (ASAT) weaponry. The possession and proliferation of ASAT weapons could be potentially destabilizing and therefore India's pursuit of ASATs could affect the overall security of the U.S.

²⁴ Realism and deterrence are inextricably tied. If one believes in the theory of deterrence then one accepts a realist view of international security. Realism maintains the belief that the primary objective of all nations is security and survival. If a coercer can credibly threaten another nation's security or survival then the coercer can deter the target from taking certain actions or compel them to take certain actions.

²⁵ It is true that the U.S. has a stated policy that attacks on satellites are infringements of its rights and a perceived lack of enforcement of that policy may serve to undermine the credibility of that policy and the overall credibility of the U.S. But the U.S. also has stated positions on non-proliferation, support to allies like Israel, and protecting U.S. citizens.

imposition will not work on these actors.²⁶ The only viable option for these actors is to deny them any benefit they seek to achieve through their actions.

To meet these challenges the U.S. will need to incorporate space security into its deterrence strategies for China, Russia, Iran, North Korea, etc. Heretofore space deterrence theorists have put the proverbial cart before the horse and placed space deterrence as the primary objective. The actual goal of the U.S. is to protect its national security, not protect its satellites, and the prevention of attacks on our satellites is but one of many interests in this broader strategy.

As previously stated, China and Russia have already developed counterspace capabilities and have shown the political willingness to use these weapons.²⁷ This means that the U.S. is not in a deterrence relationship with China and Russia but rather a compellence relationship. China and Russia have counterspace capabilities that threaten U.S. global power projection and threaten the homeland. To alter this reality the U.S. must compel China and Russia to give up these counterspace capabilities or change their existing political valuation of the utility of employing these weapons. It stands to reason that so long as the U.S. derives significant national power from its satellites it will be near impossible to convince China and Russia that their counterspace weapons have no value regardless of the threats, demands, and deadlines imposed. However, if the U.S. can convince China and Russia that there is no overall strategic benefit in employing these weapons and that the U.S. has the capability to deny them what they want (e.g., destroying the capacity for precision maneuver and strike, missile warning, etc.) the U.S. may be able to compel China and Russia to change their positions on using such weapons.²⁸ How one goes about compelling China and Russia is described in the next section.

What about the regional actors? These actors have either fielded low-level weapons that do not immediately threaten the security of the U.S. or they are contemplating the development and deployment of counterspace weapons. Because the regionalists are focused on local politics and security they have not made a decision to develop counterspace weapons capable of holding all U.S. satellites at risk the U.S. may be able to deter them from making the decisions that send them down the path of China and Russia. Therefore, I contend that the regional actors are in a deterrence situation.

²⁶ Exceptions to this position would be emerging space powers like India and Brazil. These nations have shown a desire to act responsibly in space, despite an academic discussion of ASAT weapons by the Indians, and the U.S. should continue to foster the constructive growth of these nations' space capabilities.

²⁷ The counterargument is that China and Russia have shown a willingness to promote and sign a treaty, the Prevention of Placement of Weapons in Outer Space Treaty (PPWT), banning the deployment of weapons in space. This proposed treaty is a farce as it: 1) does not ban the weapons already employed by the Chinese and Russians, ground-based and direct ascent anti-satellite weapons; 2) has no means of verification; and 3) does not define "space weapon" in any useful and pragmatic way. The purpose of the treaty is not to increase the overall security of the space domain but to rather politically embarrass the U.S. through the international codification of the logical fallacy of the loaded question. Here China and Russia are asking the U.S., "Why do you still want to put weapons in space?"

²⁸ Pape, R. A. (1996). *Bombing To Win: Airpower and Coercion in War*. Ithaca, NY: Cornell University Press.

There are two elements of deterrence that are common to dealing both the global powers and the regionalists: attribution and signaling. The U.S. must have the ability to know it is being attacked in space and attribute those attacks to a specific actor. Current U.S. situational awareness capacity is poor. To make matters more difficult the operating environment of space requires an attribution capability that is not only precise but also timely—an attack on a satellite could literally come at the speed of light. The combatant commander and policy makers must have precise attribution information quickly to respond to an attack. Unfortunately, despite considerable financial and intellectual investment by intelligence agencies there exists no perfect and instantaneous intelligence collection capability.²⁹ There has been a long-enduring discussion about the placement of warning sensors on our satellites. Such sensors would definitely be helpful but they cannot discern whether an attack took place, who perpetrated an attack, and most importantly to policy makers, why an attack occurred.

The U.S. must also let all other nations know what actions it finds offensive in space. I would strongly recommend against the use of technically defined redlines for signaling. The space community likes to talk about exclusion zones for satellite proximity, reversible jamming, dazzling, as the concerns. Setting redlines that are focused on the capabilities of certain weapons invites an adversary to approach but not cross a redline.³⁰ I recommend that the U.S. employ signals that certain conditions, not weapons or operations, are unacceptable. For example, if the U.S. were to state that that precision position, navigation, and timing signals are critical to international security and economics it allows the U.S. to respond to a broad range of attacks on GPS satellites in a variety of different ways rather than if the U.S. had stated that it is against the use of GPS jammers. Similarly, if the U.S. were to state, “foreign satellites should not be closer than 1 kilometer of our National Technical Means” our response options would be limited and it would invite an adversary to stand 1.1 kilometers away from our NTM. In contrast, if the U.S. had stated, “the integrity of our intelligence collection assets is critical to the national security of the U.S. and its allies and any actions, perceived or real, to interfere with those assets will be considered a violation.” The latter language is clear in intent, puts the responsibility on the aggressor to prove that they are not intending to interfere with our satellites, and the U.S. is willing to react to a wide range of potential threats.

For maximum signaling effectiveness the U.S. should couple public declarations of what is unacceptable with public declarations of what is acceptable in space. Since the Eisenhower administration, the U.S. has clearly stated what behavior is acceptable and more recently the State Department is promoting specific Transparency and Confi-

²⁹ This situation, along with the fact that satellites must follow the laws of physics and therefore follow predictable paths, is why a war in space has long favored the initiator.

³⁰ “A more complex model of strategic interaction...is needed to grasp the interplay between a Defender who employs deterrence strategy and an Initiator who is considering not merely *whether* to challenge but *how best* do so at an acceptable cost-benefit level. Employing such a model of strategic interaction enabled us to score some cases as having mixed outcomes, i.e., the deterrence strategy employed may have succeeded in dissuading the Initiator from choosing riskier options for challenging the status quo but it failed to dissuade the Initiator from employing ‘limited probes’ or ‘controlled pressure’ strategies to bring about change.” in George, A. L., & Smoke, R. (1989). Deterrence and Foreign Policy. *World Politics*, 41 (2), 170-182.

dence Building Measures (TCBMs) to help the international community understand what is considered responsible behavior. The U.S. should continue to lead and shape this discussion.

Finally, there is the issue of credibility. If U.S. satellites are attacked will the U.S. be willing to respond? The track record of the U.S. in responding to attacks on its satellites is not great, but one would be hard pressed to find a response option that was realistic to any of these attacks.³¹

We then come to the conclusion that punishment is a possible but unlikely option. On the other hand, if we helped the target of the jamming utilize other satellites and other signals so they could continue to broadcast then it would deny the Iranians the effect they are trying to achieve. In many cases, that is what the U.S. and other nations have done and it may be the only credible response, especially for the regionalist aggressor.

With the actors to be deterred identified, the actions to be deterred set out, and how these are to be deterred agreed upon, it is unfortunate that the maturity and capacity of the three requisite components of deterrence is lacking. So while it is understood who, why, and what is to be deterred, what is not understood is “how”.

Given the current lack of deterrent capability for attacks on U.S. satellites and the fact that deterrence is at best an educated gamble the U.S. must prepare for the eventuality of an attack on its satellites. The U.S. does not have a well understood plan for responding to attacks on satellites. Policy makers have a difficult time quantifying the value of a satellite or, as the late Lieutenant General Roger Dekok, Commander U.S. Strategic Command, has put it, “Satellites don’t have mothers.”

This situation presents a problem. Under what conditions and thresholds will the U.S. act against an adversary and with what capabilities? For deterrence to be viable and useful the U.S. must have an overt, communicated, and credible response plan.³²

³¹ Having been involved in some of these response discussions the dialogue goes a bit like this:
“Iran is jamming a commercial communications satellite,” says the intelligence officer.
“What diplomatic options do we have?” asks the White House of the State Department.
“We don’t have any diplomatic relations with Iran so...,” states the State Department.
“Can we freeze any assets or implement any embargoes?” asks the White House of the Treasury Department.
“We’ve already frozen everything we can touch,” states the Treasury Department.
“Are there any military options?” asks the White House of the Joint Staff.
“None, other than dropping iron on Tehran and you guys said that’s not really an option,” states the Joint Staff.
“Can we go to the ITU?” asks the White House.
Everyone laughs in unison.

³² The actual response need not be overt. An adversary, in some instances, may be more likely to accede to the demands of the coercer if the adversary is not publicly admonished or threatened. Also, “credible” is understood to include proportional and graduated responses. For example, responding to the jamming of a commercial communications satellite with nuclear weapon is not credible whereas responding to the destruction of a missile warning satellite with a nuclear weapon is credible.

When Deterrence Fails: Responding to Hostile Acts

To reach the goal of assuring these critical missions the U.S. will need to employ a broad range of response and defensive capabilities. Policy makers will first need to decide under what circumstances they will respond with force. The determination of the threshold(s) required to invoke a U.S. military response would be an enlightening discussion among the leadership of the U.S. Once the use of force decision criteria have been developed then the U.S. can then determine what capabilities are needed for defensive and offensive responses. These capabilities can be non-materiel, in the form of diplomacy, policy statements, and/or economic incentives or punishments, or they can be materiel. A secondary function of these capabilities is to perform a coercive function that is intended to allow the U.S. to anticipate, prevent, and/or shape the decisions of adversaries.

Among the materiel capabilities in which the U.S. should invest are responsive launch and disaggregated satellite constellations to increase resilience and complicate adversary targeting. The U.S. should procure and exercise backup space capabilities and not eschew the use of commercial satellites, where appropriate, to perform these functions. The U.S. should integrate non-space capabilities, like fiber optic cables or airborne ISR, to provide a defense in-depth capability. The U.S. also needs to invest in attribution capabilities- not just for deterrence but for defense and response as well.

Regarding non-materiel solutions the U.S. needs to fully integrate all elements of national power to deter an actor bent on attacking our satellites. The “all elements of national power” phrase has become cliché but regarding the protection of space systems it is critical. The President and the Cabinet need to take the language in the National Space Policy and provide some more directed language regarding what it considers to be unacceptable behavior. The State Department should continue to lead the discussion with allies and adversaries as to what is acceptable behavior in space.

The topic of cooperation with allies raises another curiosity of the “space deterrence” debate. The concept of entanglement and all of its aliases as a deterrent to an attack is an intellectual dead end. Entanglement has been proven to not work in space. Regionalists attack commercial satellites with customers from all nations. China has conducted an ASAT test and the resultant debris has threatened all space faring nations. Far from being a deterrent, entanglement is actually an encouragement. An adversary can now target one satellite and hit multiple targets and then continue on its campaign while the coalition tries to decide what its response plan will be. An entangled deterrent is only as strong as the weakest member of the group. Even if one suspended reality and gave space entanglement a deterrent value it would still fail because the signaling and credibility attributes of deterrence are ambiguous or nonexistent in entanglement. Each nation would have its own thresholds for response based upon the value it placed on the satellite and its relationship with the attacker and it would hold its own beliefs on a proportional response. Given the tremendous strategic value the U.S. places on its satellites it would be an equivocation of our sovereignty if we allowed other nations to determine how best to respond to a threat to our security.

Conclusions

The U.S. needs to stop using the phrase “space deterrence” and focus on deterring actors and their capabilities. Bloomfield’s quotation that opens this paper is just as applicable now as it was nearly 50 years ago.

The U.S. has several key components in place to form the foundation of a credible deterrent capability against hostile actors. But there remain several areas that need to be developed before the U.S. can claim a true deterrent capability. The U.S. will need to address these capability shortfalls before publicly unveiling a deterrence and/or compellence strategy. Deploying an incomplete deterrence strategy encourages hostile acts and forces the U.S. to accept actions or conditions that are against its national and foreign policy objectives. Therefore, announcing a deterrent capability before such a capability actually exists will lead to a regressive cycle in which U.S. credibility is continually reduced and the deterrent value goes below zero and actually becomes an encouragement.

Even if the U.S. develops those capabilities it is unlikely that a committed aggressor will be deterred because of the critical role satellites perform for the U.S. and its allies. Additionally, aggression in space favors the initiator. So any deterrence capacity will begin with two major strikes against them. Therefore the best possible option is to deny the adversary any benefit they seek to gain from an attack.

The new National Space Policy, building upon the policies of previous administrations, provides the foundational guidance for developing these missing capabilities, materiel and non-materiel, and integrating them into a larger suite of U.S. capabilities.³³

Policy makers need to remember that deterrence is a gamble and when it comes to deterring hostile acts against our space systems the U.S. currently has very bad hand and a lot of chips on the table. Deterrence should not be viewed as a replacement for defense or a less expensive way to protect our satellites. The U.S. should focus its near-term efforts on cultivating defensive capabilities and developing and exercising response plans. If the U.S. can build this broad suite of tools then deterrence may take care of itself.

³³ See sections in PDD-4 on Principles, Goals, International Cooperation, Preserving the Space Environment and the Responsible Use of Space, Assurance and Resilience of Mission-Essential Functions, and National Security.

Deterrence in Cyberspace: Yes, No, Maybe?

Eric Sterner

Since science fiction author William Gibson coined the term in the 1982 short story “Burning Chrome,”¹ cyberspace has represented a perplexing domain for policymakers. It simultaneously represented massive opportunities for society and an entirely new set of national security problems. The United States, like most developed economies, has incorporated cyberspace into its economic foundations. Everything from retail sales and inventory management to manufacturing operations and infrastructure management occurs in cyberspace. The military was similarly quick to adopt cyber capabilities and integrate them into its combat capability. As artificial as the domain may be, predictably human conflict has followed human interaction into the realm of cyberspace. Yet, the dynamics of conflict in cyberspace differ from those found in the traditional domains of sea, land, air, and even space. In particular, analysts question the logic of deterrence—that the capability to impose unacceptable costs on an actor as punishment for undesired behavior will lead the actor to restrain himself—obtains in cyberspace, largely due to the difficulties associated with attributing any attacks to a specific challenger and identifying the challenger’s motives. More often than not, these analysts have accepted the notion that “denial deterrence,” which is deterring a challenger by denying him the outcomes he seeks, is the only realistic course of action available.² A quick examination of the dynamics of conflict in cyberspace suggests there may be less to both assertions than meets the eye.

Conflict in Cyberspace

Cyberspace is a contested domain in which conflict is commonplace. As long ago as 2007, the Combatant Commander for U.S. Strategic Command testified to Congress that “America is under widespread attack in cyberspace.”³ More recently, a former director of the National Security Agency wrote, “The United States is fighting a cyber-war today, and we are losing.”⁴ Indeed, the scale of malicious interactions in cyberspace is astonishing. A recent report estimated roughly “1.8 billion cyber attacks if varying sophistication targeting Congress and federal agencies each month.”⁵ The number would grow exponentially if one included attacks on non-federal institutions, such as state governments, foreign governments, and the private sector (U.S. and foreign).

¹ See William Gibson, “Burning Chrome,” *Omni*, July 1982, pp. 72-77. Many believe that Gibson first coined the term cyberspace in his 1984 novel *Neuromancer*; in fact it was first coined in this 1982 short story.

² Indeed, the concept of denial deterrence may be a misnomer in that it does not require the imposition of retaliatory costs. A defender may just “sit there.” Dissuasion may be a more appropriate phrase, but policy documents persist in calling dissuasion by denial “denial deterrence.” Note the citation of Deputy Secretary of Defense William Lynn below. For the purposes of this essay, I will accept the phrase “denial deterrence.”

³ General James Cartwright, USMC, *Statement Before the Strategic Forces Subcommittee*, Senate Armed Services Committee, 28 March 2007, pp. 4-5

⁴ Mike McConnell, “To win the cyber-war, look to the Cold War,” *The Washington Post*, 28 February 2010, p. B-1.

Clearly, not every one of these attacks is significant. Indeed, the vast majority may be of no more concern than a passing summer rain. Yet, truly frightening attacks are buried within the numbers. Governments are frequent targets and their ability to use cyberspace has been significantly harmed. Perhaps the two best-known cases are Estonia (2007) and Georgia (2008), which were essentially forced off the net. Moreover, states are finding themselves increasingly vulnerable as cyberspace penetrates national infrastructures. As is well documented elsewhere, the stuxnet worm (thankfully) set back Iran's nuclear program by attacking automated controllers buried in Iran's nuclear infrastructure, demonstrating the ability to use cyberspace to attack a nation's infrastructure.⁶ The class of threats that stuxnet represents is not unique.

Stories of the hacking of private companies are commonplace. In just recent weeks, Sony, the security firm RSA, Sega, Epsilon Data Management, Lockheed-Martin, PBS, and Hyundai Capital Company were all publicly hacked with a variety of impacts.⁷ Such attacks may accomplish several goals: undermining the firm's competitiveness, embarrassing it, stealing its intellectual property, or simply robbing its finances.

Analysts have found it challenging to describe the sources of these attacks, and thus the nature of threats in cyberspace. Actors in cyberspace are "created" in cyberspace. Anyone—states, companies, criminals, activist movements, individuals—with access to cyberspace can create such cyber actors, which may, or may not, correspond to the identity of their creator. Consequently, it is exceedingly difficult to link an actor in cyberspace to its counterpart in the physical domain. Indeed, it may be prohibitively so.

The challenges associated with attributing a specific attack to a specific attacker aside, it is possible to roughly categorize threats. Early attackers may have been motivated more by the technical challenge of a feat than any desire for personal gain. That ethic still exists among some attackers. A significant portion clearly involves financial motives. Others have a political agenda, but treat cyberspace more as a domain for political activism than strategic conflict. A range of parties may use the web for espionage against governments and corporations. Finally, some actors view cyberspace as a strategic domain useful in conflicts short of war and warfare itself.

Unfortunately, there are not clear dividing lines among these characterizations. For example, activists may do significant financial or economic harm or have strategic

⁵ Kristin M. Lord and Travis Sharp, *America's Cyber Future: Security and Prosperity in the Information Age, vol. 1.*, (Washington, DC: Center for a New American Security, May 2011), p. 7. The definition of "attack" used in this report is questionable and likely includes probes and scans. The FY2009 FISMA report, for example, lists nearly 109,000 attacks on federal networks, nearly two-thirds of which were phishing attacks. *Fiscal Year 2009 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*, (Washington, DC, Office of Management and Budget, 2010), p. 10. It suggests the nomenclature policymakers use in cyberspace may be too limiting.

⁶ Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier*, Symantec Security Response, February 2011.

⁷ Ben Worthen, Russell Adams, Nathan Hodge, and Evan Ramstad, "Hackers Broaden Their Attacks," *Wall Street Journal*, 31 May 2011; Hayley Tsukayama, "Sega cyber attack breaches 1.3 million accounts," *Washington Post.com*, 20 June 2011.

effects. Recent attacks on corporations and police institutions by LulzSec, for example, may undermine confidence in cyberspace as a reliable domain for economic activity and law enforcement, whereas LulzSec appears motivated more by activist intent.⁸ States may seek a strategic purpose, but disguise their attacks as criminal or activist enterprises. For that matter, states may “rent out” the capabilities of criminal networks and talented individuals in order to conduct specific campaigns or attacks. LulzSec’s anonymity, for example, would make it a reasonable “front” for state or criminal activity. Consequently, it can be difficult for defenders to identify, assess, and counter a specific attacker and his attack. It may be more useful to view cyberspace threats as a kind of threat cloud, or threat “blob,” constantly changing in size, scope, capability, and intent with only vague boundaries among all categories. This does not excuse the need to understand and characterize threats, either collectively or individually; it only suggests that threat characterization be alert to sudden changes in the nature of the cloud and leave open the possibility that one kind of attack is, in fact, another.

To Deter or Not to Deter

These factors have undermined a fundamental principle of deterrence as U.S. policymakers understood it during the Cold War. By and large, only states were capable of organizing, mobilizing, and using the military forces capable of attacking another state and causing it serious harm. Consequently, an attacker’s identity would always be known. Retaliation, and thus its threat, was a function of means and will. Without firm knowledge of an attacker’s identity, and thus against whom to retaliate, deterrence becomes problematic.

The problems of applying deterrence theory to cyberspace do not end there. In theory, successful deterrence of nuclear attack during the Cold War depended on stable relationships between a low number of actors with roughly equal power, similar expectations, and a shared interest in avoiding nuclear warfare at all costs. None of these elements are present in cyberspace, where the number of actors is immense and constantly changing, interests are asymmetrical, and expectations are not uniform. Finally, because the infrastructure of cyberspace (server farms, transmission lines, communication nodes, etc.) is largely privately owned and crosses national boundaries, retaliatory attacks have a high propensity to cause collateral damage. Worse, attacks (retaliatory or otherwise) always have the potential to expand a conflict as the states in which this infrastructure exists feel compelled to respond. Thus, potential attackers have reason to doubt the credibility of retaliatory threats. A defender may lack both the capability and the will.

The difficulties associated with retaliatory deterrence in cyberspace led many to advocate a form of denial deterrence. Essentially, they assumed that the ability to foil an attack would lead challengers to forego their attacks by changing their cost-benefit analysis. One analyst, for example, suggested, “Cyber deterrence could benefit from greater attention to defense. Increased attention to defense and resiliency could reduce the perceived gains of an opponent from cyber attack, thereby changing an attacker’s

⁸ Associated Press, “Collective opposed to Ariz.’s immigration policy says it hacked into state public safety files,” *WashingtonPost.com*, June 24, 2011.

decisions in ways that are not achievable by threatening reprisal or retaliation, and decreasing the chances for successful attack and increasing the costs of detection.”⁹ Deputy Secretary of Defense William Lynn echoed the call, noting in a widely-read article, “deterrence will necessarily be based more on denying any benefit to attackers than on imposing costs through retaliation.”¹⁰

The argument has some merit. Launching a cyber attack requires resources. Someone has to marshal the resources necessary, limited though they may be. Using those resources to launch an attack involves opportunity cost. Once used, a weapon will often reveal its operating characteristics, immediately enabling a defender to begin neutralizing it. Stuxnet, for example, is being routinely dissected and assessed by knowledgeable analysts around the world. It cannot be used again. In short, cyber attacks are not necessarily cost free; some attacks run the risk of breaking the weapon.

Denial deterrence might further be strengthened by robust risk mitigation and consequence management strategies. Thus, even if an attack successfully achieved its tactical goals, such as penetrating a secured network, it may not have a significant impact on the larger entity—be it a company, an agency, or a nation—because the target is prepared for the eventuality. Indeed, this has become a favored approach for several analysts and experts.¹¹

Round Two to Deterrence?

Despite the initial analysis of deterrence’s limited applicability to cyberspace, further examination suggests that the cause is not lost. At its heart, deterrence is about imposing costs on an attacker such that the cost of an attack exceeds the expected benefits in the attacker’s mind.¹² It has long been a tactic, if not a strategy, in international security. With that in mind, other deterrence models may become relevant to the cyber domain. Richard Kugler, for example, suggests a deterrent posture based on both denial and retaliatory capabilities.¹³ He argues that such a multipronged approach can affect an adversary’s thought process by impacting multiple aspects of a challenger’s strategic calculus.

⁹ James Lewis, *Cross-Domain Deterrence and Credible Threats*, (Washington, DC: Center for Strategic and International Studies, July 2010), p. 4.

¹⁰ William J. Lynn, III, “Defending a New Domain,” *Foreign Affairs*, September/October 2010, pp. 99-100.

¹¹ See, for example, Greg Rattray, Chris Evans, and Jason Healey, “American Security in the Cyber Commons,” in Abraham Denmark and James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World*, (Washington, DC: Center for a New American Security, 2010).

¹² The Defense Department has a two-part definition. Deterrence is “The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.” See *DOD Dictionary of Military Terms and Associated Terms* as amended 15 May 2011. Available at http://www.dtic.mil/doctrine/dod_dictionary/. The first sentence could encompass denial deterrence.

¹³ Richard Kugler, “Deterrence of Cyber Attacks,” in Franklin Kramer, Stuart Starr, and Larry Wentz, eds., *Cyberpower and National Security*, (Washington, DC: National Defense University Press/Potomac Books, Inc., 2009).

Other models come to mind. Israel, for example, adopted a posture of horizontal escalation at various points in its history in order to alter the strategic environment in which its attackers operated. Such a posture might work in cyberspace. Holding the domain's creators accountable for the use of their infrastructure would force them to take additional steps to strengthen security and deny challengers the safe haven of anonymity.¹⁴

The means by which one might hold infrastructure providers or challengers accountable is open to some discussion. Legal and economic tools are available. Arguably, today, legal mechanisms are the most relied upon means of sanctioning cyber attackers, but not infrastructure providers. Most simply, states attempt to identify, arrest, prosecute, and punish malicious actors. They have naturally run into difficulties, starting with attribution and the challenges of cross-border investigations, but continuing through poor domestic laws against cyber attacks and the incompatibility of various criminal statutes across national boundaries. Economic tools, such as those used against serial proliferators, might also prove useful in imposing some costs. Sunshine banking laws may also provide useful models in dealing with infrastructure providers. However, they are not well developed for cyberspace.

Cyber/in-kind retaliation remains a difficult challenge. Those tools that the U.S. might have at its disposal generally remain classified. The government is understandably reluctant to reveal them, lest they become unavailable for significant strategic scenarios. Of course, this limits their value as a retaliatory threat. Similarly, cyber retaliation may also compromise intelligence collection. Moreover, given the globalized nature of cyberspace, it has a high likelihood of affecting third parties. During the Russo-Georgian cyberwar, for example, cyber attacks originating in Russia succeeded in significantly degrading the Georgian government's presence in cyberspace. Georgia was able to work with friendly-minded countries and relocate some of its cyberspace servers to the U.S., Estonia (which had endured extensive cyber attacks the year before), and Poland.¹⁵ After the relocation, persistent attacks on those reconstituted Georgian cyber capabilities would have required attacks on cyberspace infrastructure located in those three countries, arguably widening the cyber conflict. While the administration hopes that such concerns might affect an attacker's cost-benefit calculus, they also affect a defender's contemplation of any retaliatory cyber attacks.

Military means of retaliation are a more controversial option. Notwithstanding the issues of attribution and collateral damage, the proportionality of the response is a factor. As often as not, the issue is framed as one of taking lives in defense of bytes, a trade generally thought to be disproportional.¹⁶ Nevertheless, the United States has

¹⁴ For a longer discussion, see Eric Sterner, "Retaliatory Deterrence in Cyberspace," *Strategic Studies Quarterly*, Spring 2011. See also Jonathan Shimshoni, *Israel and Conventional Deterrence*, (Ithaca, NY: Cornell University Press, 1988).

¹⁵ Stephen Kornis and Joshua Kastenber, "Georgia's Cyber Left Hook," *Parameters*, Winter 2008-2009.

¹⁶ See, for example, Martin Libicki, *Defending Cyberspace and Other Metaphors*, (Washington, DC: National Defense University, 1997). p. 44; Richard J. Harknett, "Information Warfare and Deterrence," *Parameters*, Autumn 1996. Harknett was particularly concerned about violating the principle of proportionality.

used force to protect its vital interests in the past—even when the lives of American citizens were not directly threatened. Interests in cyberspace should be no different. Indeed, the administration’s international cyber strategy does not rule out any retaliatory means, instead “reserving the right to defend national assets as necessary and appropriate.”¹⁷ According to press reports the potential for significant damage to the nation has led policymakers to retain military retaliation as an option, essentially treating some cyber attacks on the U.S. as acts of war.¹⁸

Finally, the Obama Administration’s international strategy for securing cyberspace holds out the additional hope of deterring attacks by building international alliances. It argues that, “interconnected networks link nations more closely, so an attack on one nation’s networks may have impact far beyond its borders,” therefore affecting a cost/benefit calculation. In theory, an attacker might be willing to attack U.S. networks, for example, but unwilling to do so if it also entailed damaging networks in other countries due to the globalized nature of cyberspace. The aforementioned Russo-Georgian conflict offers one such example.

Challenges for a Deterrent Posture

Since its early dismissal as a means for securing cyberspace, deterrence has clearly made a comeback. It is not so easily dismissed in theory and the Obama administration clearly believes it has value. Even so, much remains to be done before policymakers place significant weight on deterrence as a pillar of U.S. national security in cyberspace. Quite simply, deterrence of cyber attack is not ready for primetime.

First, the policy community must wrestle with a stunning lack of evidentiary support for a deterrent theory. The foundational understanding of behavior and response needed for deterrence to work is lacking for cyberspace. Individuals and organizations behave differently in cyberspace than they do in the physical world. For example, individuals post more personal information on-line than they often would share with their next-door neighbors. They may even take instructions (“participate in this flash mob,” “click on this link”) from faceless cyber actors that they would not follow if received face-to-face. How do these different behaviors affect the cost-benefit analysis in considering whether trying to do harm to another? Might some be more prepared to destroy a website or a network than they are to destroy a building? Do they understand that the former might have greater consequences than the latter? Do they even go through a meaningful cost-benefit calculation in making such a decision? How do individual calculations differ from those of states? Does criminology have anything to offer? Do large organizations behave in a fundamentally different manner from either individuals

¹⁷ President of the United States, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, (Washington, DC: The White House, May 2011), p. 12.

¹⁸ Siobhan Gorman and Julian Barnes, “Cyber Combat: Act of War,” *The Wall Street Journal*, May 31, 2011. This raises an important question which, unfortunately, lies beyond the scope of this essay: namely, the relevance of the laws of armed conflict (LOAC). Such laws nominally govern legitimate reasons to go to war and define legitimate means of waging the war. While LOAC may be relevant for the United States in contemplating military means of retaliation, it is less obvious that they are relevant to a conflict that remains contained within cyberspace, as was the case in Estonia in 2007.

or states? Answers may be derived intuitively, but intuition will not serve as an adequate foundation for U.S. national security. Answering these kinds of questions is critical if any country seeks to establish a deterrent posture for cyberspace. Otherwise, a deterrent posture can be based on little more than untested assumptions and theory. The good news is that, unlike nuclear conflict, analysts will not be lacking for observational data and opportunities for experimentation.

Second, the parameters under which retaliatory decisions may be made also require examination. Command authorities need to have a reasonable idea about what kinds of attacks warrant retaliation, what retaliatory tools are at their disposal, who is responsible for the decision to retaliate, who will execute the retaliatory act, and what legal and normative regimes will govern retaliatory behavior. Policymakers have focused on these questions over the last few years. Much of the debate has revolved around the question of which legal regimes should guide retaliatory actions: those regarding espionage, crime, or armed conflict. In theory, once those questions were answered, other issues of roles and missions are more easily answered. In developing internal guidance, much of which remains classified at this writing, the administration is seeking to settle these questions. Indecision has stymied policymaking for years while the political system wrestled with them.

While policy clarity is welcome, policymakers must remain open to changing the answers over time. Attempting to fit cyber-conflict into existing legal regimes and institutional roles/missions may well be trying to fit a square peg into differently sized round holes. The existing regimes were built up over years to deal with specific scenarios, many already experienced in human history. Cyberspace appears to present something entirely new. At the moment, it seems likely that regimes, processes, and institutions designed to deal with one phenomenon may prove inadequate or inappropriate for dealing with something else. Experience in national security in cyberspace will be necessary to continually ask whether decisions made at the beginning of the information age are still relevant decades later. In all likelihood, they will not be.

Third, there is the question of willpower. Normally, for a challenger to take a threat of retaliation into consideration, the threat has to be credible. Credibility is usually broken down into two ingredients: means and the will to use them. It is not clear that the U.S. has either, at least not in sufficient quantity to constitute a credible deterrent. Whether federal systems are attacked 1.8 billion times a month or 109,000 times a fiscal year, the number of criminal prosecutions for such events is miniscule by comparison. Any cyber retaliatory actions are likely secret, and therefore have little deterrent value vis-à-vis challengers who are not privy to their existence. As of this writing, the U.S. has not retaliated economically or contemplated any form of military retaliation for a specific attack. In that environment, any expectation of credibility that requires a response to every attack is unrealistic. Thus, redlines are moot. Instead, analysts will need to assess various retaliatory mechanisms that focus on risk. How much risk needs to be imposed before potential challengers take it into account? How much does tolerance for risk vary among potential challengers? How much risk is the country

willing to threaten? Is the U.S. self-deterred by the possibility of collateral damage? By the risk of escalation? By limitations imported from existing legal and normative regimes? By the cost of creating retaliatory tools? In his book on cyberspace, former National Security Council staffer Richard Clarke takes the current and past administrations to task for their reluctance to increase regulation of cyberspace.¹⁹ They have been, in effect, unwilling to pay the cost of threatening the innovation created by a more free-wheeling cyber environment. If this and future administrations are unwilling to bear such costs, then can a reasonable deterrence posture be crafted?

Finally, the mechanics of decision-making and deterrence must be put into place. These include situational awareness, which is critical. Interagency processes have to be improved to improve cross-agency information sharing and establish command and control procedures. Given the private nature of much critical infrastructure, this will also entail closer cooperation with the private sector, while the globalized nature of cyberspace necessitates cross-border cooperation. It will be tempting to develop a more sophisticated understanding of thresholds and a clear declaratory policy, largely in order to put unresolved questions to rest. Yet, doing so before one has fully established a useful model of deterrence risks ruling possible deterrence options out unnecessarily.

In many ways, deterrence in cyberspace is eminently more complicated than deterrence in the Cold War. The nature of the domain makes it so. Even the most sophisticated theories behind nuclear deterrence will prove inadequate for dealing with the complexities of a man-made domain with a virtually infinite number of constantly changing actors, motivations, and capabilities.

Ultimately, for its security, the U.S. must depend on its ability to prevail in a cyber conflict—which may, or may not—be associated with an armed conflict or even a state. The front line is not deterrence of attack, but the interaction of attack and defense at the point of attack. Eventually, the U.S. will also have to go on the offensive against its attackers, either in conjunction with a cyber campaign or some other political-military action. It stands to reason that these capabilities will affect a potential attacker's cost-benefit analysis. Whether they do so in a manner sufficient to deter an attack or affect an attacker's choices about ends and means remains to be seen, but such possibilities suggest deterrence as a concept is not a lost cause in cyberspace. Even so, we have a long way to go in making it so.

¹⁹ Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (New York: HarperCollins, 2010).

A Fatal Disconnect: Conventional Deterrence in a Nuclear-Armed World

John B. Sheldon, Ph.D.*

The recent revival of deterrence as a strategic concept has produced many studies and analyses on 21st century nuclear deterrence, conventional deterrence, and even cyber and space deterrence. With deep defense cuts in the coming years coupled with an ambitious policy to eliminate nuclear weapons—and given the heavy reliance on its conventional forces in most strategic heavy lifting demanded by the National Security Strategy and foreign policy in general—the question must be asked whether the United States is adequately preparing for the favorable conditions in which deterrence might plausibly succeed.

The purpose of this essay is to highlight the significant challenges facing U.S. conventional deterrence capacity in a nuclear-armed world when leaders openly advocate nuclear abolishment, or do not acknowledge the political and strategic value of the nuclear weapons in their charge. Furthermore, in this era of great strategic change and uncertainty, this essay makes the case for reconnecting conventional force structures with nuclear forces in order to establish the favorable conditions needed for holistic deterrence to plausibly succeed. Holistic deterrence does away with any contrived distinction between conventional and nuclear deterrence, echoing Colin S. Gray's admonition that the "subject is deterrence; it cannot sensibly be treated as either conventional or nuclear."¹ Such a reconnection runs counter to this administration's declarations seeking to eliminate all nuclear weapons—more commonly known as Global Zero.² As well-meaning as such a policy goal may seem, the chances of it succeeding are grim. Furthermore, even if it were to somehow succeed, the implications for a United States without nuclear weapons are unfavorable: such a situation would place intolerable strain on U.S. conventional forces, which in turn will most emphatically *not* create favorable conditions for deterrence to plausibly succeed.³ Indeed, one might convincingly argue that because senior administration figures and senior leaders of key allied nuclear powers are so keen to get rid of nuclear weapons and disavow their strategic and political usefulness,⁴ such an unwanted and intolerable strain has *already* been placed on conventional forces for the purposes of deterrence.

* The views expressed in this essay are those of the author alone, and do not in any way reflect or represent the views or policies of the School of Advanced Air & Space Studies, Air University, the Department of the Air Force, Department of Defense, or the U.S. Government.

¹ Colin S. Gray, *Modern Strategy* (Oxford, UK: Oxford University Press, 1999), p. 167.

² See, for example, "Move the base camp," *The Economist*, June 18th, 2011, pp. 18-20; for an overview of the Global Zero agenda, see David Cortright and Raimo Väyrynen, *Towards Nuclear Zero* (London: IISS/Routledge, April 2010).

³ On creating and maintaining the conditions where deterrence might plausibly succeed, see Colin S. Gray, *Maintaining Effective Deterrence* (Carlisle, PA: Strategic Studies Institute, August 2003).

⁴ On the abandonment of assigning political and strategic value to nuclear weapons, from a British perspective, see Hew Strachan, "The Strategic Gap in British Defence Policy," *Survival*, Vol. 51, No. 4, August-September 2009, pp. 56-57.

Deterrence Defined

At this juncture deterrence must be defined and its attendant risks identified. Conceptually, deterrence is (or at least, should be) simple. In practice, however, the application of deterrence is both difficult and fraught with uncertainty—an uncomfortable fact among some in the U.S. where there is a tendency is to employ metrics as measures of success or failure. Unfortunately, attempts at quantifying deterrence success are utterly irrelevant since it can rarely if ever be known what relevant decision-makers, who are the object of deterrent attempts, are thinking. With this in mind, I have previously effectively defined and described deterrence as follows:

Deterrence is the attempt to persuade an adversary by the threat of force (and other measures) not to pursue an undesirable course of action. As a result, to be deterred is a state of mind, something that is not easily quantifiable for measuring success in attempts to deter. Given that deterrence is essentially an exercise in psychological manipulation in order to modify, or prevent, modes of behavior, it is fraught with uncertainty. Deterrence fails - and throughout strategic history, has failed often - because the object of deterring measures fails to notice them, does not find the measures credible, or is pursuing an agenda sufficiently important enough to its interests that it is prepared to ignore the deterrence attempt.⁵

Conventional deterrence is the attempt to persuade an adversary not to pursue undesirable actions using the threat of conventional force. Unfortunately, the challenge for conventional deterrence in a nuclear-armed world is likely to be Herculean. This is not to say that deterrence by conventional means is irrelevant in the emerging strategic environment—far from it. The issue, rather, is that deterrence by conventional means alone is unlikely to be fit for purpose where it would matter the most.

The challenges facing U.S. conventional deterrence capacity identified here are diminished capabilities that may result from likely defense budget austerity; the acquisition, development, and spread of anti-access capabilities designed to thwart U.S. conventional power projection capabilities; the development and acquisition of nuclear weapons by certain states in order to offset U.S. conventional military superiority; and lastly, the fatuous attempt to conceptually bifurcate conventional and nuclear deterrence that, as a result, has only undermined the credibility of U.S. deterrent threats. The essay will examine each of these challenges in turn.

Defense Budget Austerity

Outgoing Chairman of the Joint Chiefs of Staff, Admiral Mike Mullen, has identified the national debt as the single biggest threat to U.S. national security today.⁶ Without a sound economic foundation that provides for sustained national prosperity, the ability of the U.S. to maintain the largest and best trained and equipped military force in the

⁵ John B. Sheldon, “Space Power and Deterrence: Are We Serious?” *Policy Outlook* (Washington, DC: The George C. Marshall Institute, November 2008), p. 1.

⁶ See Roxana Tiron, “Joint Chiefs chairman reiterates security threat of high debt,” *TheHill.com*, June 24, 2010.

world will remain fatally compromised. Undoubtedly, reducing deficits and restoring fiscal confidence, along with helping the faltering economy to find its way back to prosperity, are political priorities and will require sacrifice and compromise across the board. In such times it is unrealistic to argue that the defense budget should be exempt from any cuts, especially when the American taxpayer is being asked to accept cuts elsewhere. Defense cuts, of course, are already underway to the tune of \$400 billion over the next ten years. More recently, however, calls for a further \$400 billion cut to the defense budget have surfaced in the political debate surrounding the debt ceiling negotiations on Capitol Hill.⁷

These additional proposed cuts to the defense budget threaten key defense programs across the board. For the U.S. Navy, such cuts mean the possible loss of one aircraft carrier battle group; for the U.S. Air Force they mean a threat to the long-range bomber program scheduled to replace its aging bomber fleet.⁸ Furthermore, the Air-Sea Battle concept currently under joint development by these two services is in question in this emerging austere budget environment, raising real doubts about the ability of the U.S. to project conventional military power in key regions such as the Persian Gulf and Southeast/Northeast Asia, where anti-access capabilities are prevalent and growing in range and sophistication.⁹ Without enough capable and technologically advanced air and maritime conventional forces, the ability of the U.S. to make good on its security guarantees to friends and allies in these regions and beyond comes into question.

Defense budget cuts without a commensurate adjustment of U.S. interests and security commitments create the challenge of maintaining conventional forces capable of mission assurance over great distances while also developing future capabilities to ensure that the U.S. can continue to fulfill its policy commitments in the decades to come. Failure to meet this challenge will mean that long-term U.S. security interests will lack the capability to fulfill the obligations attendant to those interests. If further budget cuts are inevitable, and U.S. interests and commitments do not change in line with fiscal realities, it is imperative that such cuts are explicitly tied to a defense strategy that identifies the national security priorities which truly impact critical national interests.¹⁰ Rather than cutting big ticket defense items which gratify short-term political expediency at the expense of long-term security interests—like aircraft carriers and long-range bombers—it is better to trim U.S. security interests to more accurately reflect the core interests. In other words, decide first what is critical to U.S. security interests and then, if necessary, cut capability. The alternative that favors short-term political expediency threatens to seriously reduce U.S. conventional military strength where it matters, and in turn stymies the creation of favorable conditions for holistic deterrence to plausibly succeed.

⁷ See Megan Scully, "McKeon Balks at 'Gang of Six' Defense Cuts," *NationalJournal.com*, July 20, 2011.

⁸ See Craig Whitlock, "Pentagon braces for much deeper military spending cuts as part of debt deal," *The Washington Post*, July 20, 2011.

⁹ See Spencer Ackerman, "Budget Storm Could Sink U.S. Plan to Rule Sea and Sky," *Wired.com*, July 20, 2011. For an overview of the Air-Sea Battle concept, see Andrew F. Krepinevich, *Why AirSea Battle?* (Washington, DC: Center for Strategic and Budgetary Assessments, 2010).

¹⁰ See, for example, Michael O'Hanlon and Peter W. Singer, "The Real Defense Budget Questions," *Politico.com*, July 21, 2011.

Foreign Anti-Access Capabilities

Since the defense budget is likely to shrink significantly, a number of countries which are of particular interest to U.S. security interests have, for some time, been developing and acquiring a range of anti-access, or area denial, weapon capabilities designed to deny the U.S. and its allies the air, maritime, and space dominance they have become accustomed to over the past two decades.¹¹ The development of sophisticated, precise long-range anti-ship cruise missiles poses a threat to U.S. Navy surface power projection capabilities.¹² Similarly, the proliferation of modern and robust integrated air defense systems threatens to deny long-standing U.S. air supremacy in regions of key importance to U.S. security interests.¹³ Also of concern is the spread of numerous counterspace capabilities to a range of countries, threatening the *de facto* space dominance enjoyed by the United States since the end of the Cold War.¹⁴

On top of these denial capabilities, the proliferation of ballistic missiles has not abated, and satellite technologies of increasing sophistication disseminate to more and more countries with each passing year. These capabilities allow countries to target and possibly attack U.S. and allied fixed forward bases from long ranges, as well as monitor friendly force deployments.¹⁵ As U.S. defense budgets decline, potentially threatening the ability of the U.S. to overcome these area denial challenges, and area denial and anti-access capabilities both proliferate further and become increasingly sophisticated—so again it becomes even more challenging to create favorable conditions for plausible deterrence to succeed, because the capability, and thus credibility, of U.S. conventional forces are not able to guarantee mission assurance at politically acceptable levels of effort.

The Threat of Nuclear Weapons

As a concept, conventional deterrence appeared during the Cold War as Western powers sought to deter Soviet aggression in Europe. One of the earliest, and perhaps most prominent, proponents of conventional deterrence, John Mearsheimer, noted that, “[N]uclear weapons of course continue to play a role in deterring war in Europe and will do so as long as they remain available. Nevertheless, growing acceptance of the disutility of nuclear weapons for purposes of defense has brought greater interest in the conventional balance in recent years.”¹⁶ Of course, Mearsheimer considered conventional deterrence within the context of U.S.-Soviet nuclear-armed mutual assured

¹¹ On the genesis of the development of these capabilities see Timothy D. Hoyt, “The Next Strategic Threat: Advanced Conventional Weapons Proliferation,” in Henry Sokolski and James M. Ludes (eds.), *Twenty-First Century Weapons Proliferation* (London: Frank Cass, 2001), pp. 33-51.

¹² See, for example, Bradley Perrett, “China Details Anti-Ship Missile Plans,” *Aviation Week & Space Technology*, July 19, 2011.

¹³ See Carlo Kopp, “Surviving the Modern Integrated Air Defense System,” *Air Power Australia Analysis*, February 2009. <http://www.ausairpower.net/APA-2009-02.html>.

¹⁴ See National Air and Space Intelligence Center (NASIC), *Challenges to U.S. Space Superiority* NASIC 1441-3894-05 (Wright-Patterson AFB, OH: NASIC, March 2005).

¹⁵ See Andrew Krepinevich, Barry Watts, and Robert Work, *Meeting the Anti-Access and Area-Denial Challenge* (Washington, DC: Center for Strategic and Budgetary Assessments, 2003).

¹⁶ John J. Mearsheimer, *Conventional Deterrence* (Ithaca, NY: Cornell University Press, 1983), p. 13.

destruction, and indeed reading *Conventional Deterrence* provides little comfort for anyone seeking solace from conventional deterrence in a nuclear-armed world. After the Cold War, Western conventional deterrence ascended in perceived importance again as nuclear weapons became victim, in the West at least, to “declining political-military utility.”¹⁷ Yet while the perceived value of nuclear weapons receded in the minds of some, U.S. and allied conventional military capabilities increased exponentially in terms of sophistication, destructiveness, accuracy, and range. The paradox is that this increase in conventional military might has provided a number of states, such as Iran and North Korea, the pretext for acquiring and developing nuclear weapons in order to deter the U.S. and its allies from intervening in their affairs, with the aim of offsetting U.S. conventional military might—a strength with which they cannot ever hope to compete.¹⁸

In terms of quantity there may well be less nuclear warheads today than there were during the Cold War, but these weapons have spread to other countries beyond the established nuclear powers of the U.S., Russia, France, United Kingdom, and the People’s Republic of China. As well as India, Pakistan, Israel, and possibly North Korea, it is widely believed that Iran is actively pursuing nuclear weapons, and more recently, Saudi Arabia’s Prince Turki al-Faisal has suggested that if Iran succeeds in its nuclear ambitions then Saudi Arabia will be left with little choice but to acquire its own weapons.¹⁹ It is interesting to note that substantive U.S. conventional military presence in key regions may be in part responsible for a number of these previously mentioned countries acquiring nuclear weapons. For example, the large presence of U.S. conventional military forces in the Persian Gulf and in South Korea may have done too well in their deterrence mission, leaving both Tehran and Pyongyang little alternative but to seek a nuclear capability in order to attempt to deny U.S. and allied conventional military success. Michael S. Gerson notes that with conventional deterrence “the “local” balance of military power—the balance between the conventional forces of the attacker and those of a defender in a local area of conflict—often plays a critical role in conventional deterrence, since it is local forces that will impact an aggressor’s calculations regarding a quick victory.”²⁰ When the local balance of conventional forces are such that U.S. conventional forces are so powerful and capable in comparison to the forces of their opponents, it cannot come as a surprise if a number of antagonists decide that their security interests are best served by seeking to acquire nuclear weapons. Such a capability, from their perspective at least, provides them with the means of checkmating U.S. conventional military might.

¹⁷ Gary L. Guertner, “Deterrence and Conventional Military Forces,” in Max G. Manwaring (ed.), *Deterrence in the 21st Century* (London: Frank Cass, 2001), p. 61.

¹⁸ See, for example, Derek D. Smith, *Deterring America: Rogue States and the Proliferation of Weapons of Mass Destruction* (Cambridge, UK: Cambridge University Press, 2006); and Stephen M. Walt, *Taming American Power: The Global Response to U.S. Primacy* (New York: W.W. Norton & Company, 2005), pp. 138-139.

¹⁹ See Jason Burke, “Riyadh will build nuclear weapons if Iran gets them, Saudi prince warns,” *Guardian.co.uk*, 29 June 2011; accessed 29 June 2011.

²⁰ Michael S. Gerson, “Conventional Deterrence in the Second Nuclear Age,” *Parameters*, Vol. XXXIX, No. 3, Autumn 2009, p. 38.

It must also be considered that with the receding specter of global nuclear annihilation, and a number of states acquiring nuclear weapons for a variety of reasons (including U.S. conventional military superiority), the prospect that a nuclear weapon might be used in anger at some point in the 21st century is, tragically, a real one. Some in the West may have convinced themselves that a nuclear taboo is in effect, but it is far from certain that this idea has taken root in the minds of decision makers in Moscow, Beijing, Tehran, Islamabad, or Pyongyang.²¹ Such a scenario may not even directly involve U.S. forces, since nuclear tensions exist between India and Pakistan and, potentially, Israel and Iran. Yet if the use of a nuclear weapon in war were to occur, it is almost certain that the U.S. would be drawn into such a conflict, even if only to extricate both belligerents from further escalation. The Joint commander cannot dismiss the possibility that U.S. conventional forces will have to operate in not just a nuclear *armed* environment, but quite possibly in an environment where nuclear weapons have actually been *used*.²²

This means that the possibility that U.S. forces may have to face down a nuclear-armed opponent in the 21st century cannot be summarily dismissed. If such a scenario were to arise, comfort should not be found in U.S. conventional superiority—especially as the particular political, strategic, and military context of such conflicts change from scenario to scenario. It is impossible to gauge how the U.S., and its allies, might react in such a situation, never mind the reaction of a putative nuclear-armed foe.²³ To expect U.S. conventional forces, no matter how overwhelming and advanced, to deter a nuclear-armed opponent is not only to unnecessarily court deterrence failure by encouraging rash behavior on the part of such a foe, but leaves something catastrophically dangerous to chance for the U.S. and its deployed forces. It is with such circumstances in mind that mature thinking about nuclear weapons—to include a cold assessment of their political and strategic value—is required, and in turn, that their contribution to creating favorable conditions for plausible deterrence success be explicitly coupled to the same contribution made by conventional forces. Furthermore, when senior officials and military officers ascribe the power to deter solely to nuclear weapons—as the oft-repeated phrase ‘the nuclear deterrent’ reveals—they conversely suggest that conventional forces are *not* capable of doing the same. As Hew Strachan of Oxford University notes, such thinking incorrectly implies:

... that conventional military capabilities do not also have deterrent functions, and also suggests that there is a distinction—rather than convergence—between the political and strategic roles of both conventional and nuclear capabilities. The function of strategy is to integrate the political and military. If the nuclear deterrent is compartmentalised, separated from other military capabilities, it is gradually robbed of utility and relevance.²⁴

²¹ See Nina Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons Since 1945* (Cambridge, UK: Cambridge University Press, 2008).

²² On this matter, see Col. C. Robert Kehler, USAF, “Nuclear Armed Adversaries and the Joint Commander,” *Naval War College Review*, Vol. LXIX, No. 1, Winter 1996, pp. 7-18.

²³ For example, the eloquent James M. Acton posits that threats of nuclear retaliation on the part of the United States in certain conflict contingencies will lack credibility. Perhaps, but ultimately, how can anyone credibly and plausibly know? See Acton, *Deterrence During Disarmament: Deep nuclear reductions and international security* (London: IISS/Routledge, March 2011).

²⁴ Strachan, *op.cit.*, p. 57.

Of course, not all possible strategic futures of the 21st century pit the U.S. against nuclear-armed foes. More often than not, the U.S. and its allies will find themselves dealing with adversaries that are not nuclear-armed, and for which balanced, well-trained and equipped conventional forces—backed by doctrine and strategy that emphasizes the need to prevail in any given conventional fight—should make a significant contribution to favorable conditions for plausible deterrence. In such circumstances the threat of nuclear weapons might be silent, if not explicitly disavowed on the part of the United States.²⁵ However, even in such cases, there remains the possibility that U.S. conventional forces alone may not be able to create the conditions necessary for plausible deterrence to succeed if imprudent and hasty defense cuts occur.

The Fatal Disconnect

The Global Zero initiative is silent on the threat to effective deterrence that will undoubtedly transpire if nuclear weapons were ever to be eradicated. If, as Strachan convincingly suggests, treating nuclear deterrence in isolation is fundamentally unwise, then the idea that U.S. conventional forces can deter nuclear-armed adversaries—when U.S. leaders have effectively devalued the deterrent effect of nuclear weapons—verges on imprudence. Only by seamlessly converging U.S. conventional (to include the space and cyber domains) and nuclear forces will U.S. leaders and their joint commanders be able to face down nuclear-armed foes with a greater degree of confidence—and with the ultimate backstop of the threat of nuclear retaliation in the event that an opponent should resort to its nuclear capability. Also worthy of serious consideration is the potential role played by nuclear weapons not just in preventing the outbreak of major war, but in limiting wars when they do occur.²⁶

By denying the political and strategic value of nuclear weapons, or by publicly disavowing their very use and calling for their abolishment, political leaders undercut the deterrent credibility of the nuclear forces in their charge, as well as the deterrent credibility of the conventional forces under their command. There are no guarantees with deterrence, even under the very best of circumstances. Still, when the backstop against the worst of all scenarios is either devalued or disavowed, the conditions for plausible deterrence to be effective are fatally compromised. This poses serious ethical and strategic challenges for political leaders, the military, and the public. Any debates on the merits and demerits of Global Zero or nuclear weapon modernization must continue in a spirit of intellectual honesty. In light of this, it must be asked how the U.S. can be expected to deter—or even overcome—nuclear-armed opponents when it has purposefully abandoned nuclear weapons altogether or publicly dismissed their political and strategic value? In a nuclear-armed world, where the more worrying owners of such weapons seem impervious to the moral clarion call of Global Zero, the outlook for effective deterrence is cloudy at best.

²⁵ See the discussion on this issue in Gerson, “Conventional Deterrence in the Second Nuclear Age,” *op.cit.*, pp. 35-36.

²⁶ See Strachan, *ibid.*, p. 57.

However, an improved outlook is possible. Edward Luttwak, in his classic work *Strategy: The Logic of Peace and War* writes that it is nonsensical to speak of nuclear strategy, or naval strategy or air strategy.²⁷ Rather, Luttwak reminds us, there is only strategy—the conceptual bridge that links political purpose with military feasibility²⁸—and that this logic governs the use of military force in all domains, to include the nuclear realm. Similarly, it is just as nonsensical to speak of nuclear or conventional deterrence, because to do so implies that the theory and logic required for each is somehow different, when, in fact, it is not. There is no such thing as nuclear or conventional deterrence—there is, in stark reality—only deterrence that applies across the vertical spectrum of conflict and the horizontal spectrum of means. Thinking of deterrence in this fashion is the first step to much-needed conceptual clarification and the creation of more fertile conditions to allow effective deterrence to have more than a fighting chance to succeed.

²⁷ See Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge, MA: The Belknap Press of Harvard University Press, 1987), p. 159.

²⁸ See Gray, *Modern Strategy*, op.cit., p. 17.

GEORGE C.
Marshall
I N S T I T U T E

BOARD OF DIRECTORS

Will Happer, Chairman

Princeton University

William O’Keefe, Chief Executive Officer

Solutions Consulting

Jeffrey Kueter, President

Robert Butterworth

President, Aries Analytics, Inc.

Gregory Canavan

Los Alamos National Laboratory

Mark Mills

Digital Power Capital

John H. Moore

President Emeritus, Grove City College

Rodney W. Nichols

*President & CEO Emeritus
New York Academy of Sciences*

Mitch Nikolich

CACI

Roy W. Spencer

University of Alabama-Huntsville

1601 North Kent Street, Suite 802
Arlington, VA 22209

Phone

571-970- 3180

Fax

571-970-3192

E-Mail

info@marshall.org

Website

marshall.org

August 2011