STRATEGIC DETERRENCE IN

CYBERSPACE: PRACTICAL APPLICATION

GRADUATE RESEARCH PROJECT

Kevin R. Beeker, Major, USAF

AFIT/ICW/ENG/09-01

DEPARTMENT OF THE AIR FORCE

AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

The views expressed in this graduate research project are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/ICW/ENG/09-01

STRATEGIC DETERRENCE IN CYBERSPACE: PRACTICAL APPLICATION

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

Kevin R. Beeker, BS

Major, USAF

June 2009

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

AFIT/ICW/ENG/09-01

STRATEGIC DETERRENCE IN CYBERSPACE: PRACTICAL APPLICATION

Kevin R. Beeker, BS
Major, USAF

Approved:

Robert F. Mills, PhD (Chairman) — 9 JUN 09 date

Lt Col Jeffrey Humphries, USAF (Member) — 9 JUN 09 date

Michael R. Grimaila, PhD (Member) — 9 JUN 09 date

AFIT/ICW/ENG/09-01

Abstract

This research outlines practical steps that the United States can take to improve strategic deterrence in cyberspace. The unique character of cyberspace requires tailoring of traditional deterrence strategies to fit the domain. This research uses the Deterrence Operations Joint Operating Concept (DO JOC) and the New Triad as models for organizing deterrence operations. The DO JOC focuses on tailoring deterrence operations based on the actor; but deterrence operations must be also be tailored to the uniqueness of cyberspace. The effective tailoring of deterrence operations for cyberspace will require both the application of new ways and means and the tailoring of traditional deterrence concepts to fit this new domain. Practical application of cyber strategic deterrence involves: issuance of US declaratory cyber deterrence policy; removing sanctuaries for cyber adversaries; changing US and adversary mindsets and expectations for what is permitted in cyberspace; changes to military planning in order to conduct operations in consideration of adversary cyber capability; and appreciation of the key policy tradeoffs with respect to cyber deterrence implementation. Cyberspace deterrence should include all three ways of implementing a deterrence strategy: imposing costs, denying benefits, and inducing adversary restraint. Influencing the "Consequences of Restraint" fulcrum through attribution, identity management, and incentivizing trust holds great promise for cyberspace deterrence.

Acknowledgements

I would like to thank my advisor Dr. Robert Mills who has helped me in this journey towards knowledge, especially in gently guiding me to finding an answer to my brash, and ignorant questions- What do I need to know about cyberspace and why should I care about it? It took 12 months, but I am finally starting to understand.

In addition, I would like to thank Jennifer Bradley, Brian Stork and Mark Burnett at the Strategic Deterrence Assessment Lab for taking the time to teach a fighter pilot about USSTRATCOM implementation of deterrence strategy and the DO JOC.

I would also like to thank my darling wife and special children for their love, support and dedication.

Finally, I acknowledge the goodness and providence of our sovereign God and the everlasting and eternal love of His son- Jesus Christ. To him be all glory, honor and praise.

-Kevin

Table of Contents

Page

Abstract v

Acknowledgements vi

Table of Contents vii

List of Figures ix

List of Tables x

I. Introduction 1

Background 1
Motivation 2
Purpose 2
Scope 3
Results 5
Thesis Organization 6

II. Formulating Deterrence Strategy for Cyberspace 8

The need for a deterrence strategy: US dependence on cyberspace 8
The challenges of deterrence in cyberspace 10
Deterrence Operations Joint Operating Concept and the New Triad 14
Preparing for Cyberspace Deterrence: Building a cyberspace culture 21
End: Deter cyber attack on US critical infrastructure 26
Objective: Impose Costs 29
Objective: Deny Benefits 41
Objective: Encourage Restraint 58

IV. Key Policy Tradeoffs and Research Findings 78

Imposing Costs Risks Retribution 78

Greater Freedom of Action Through Deterrence 81
Findings 87
Future Research 89

Appendix A 92

The traditional view of deterrence 92
A brief review of physics- the power of the fulcrum 95
The DO JOC model of deterrence 96
The new Triad 98

Appendix B 100

Bibliography 101

Vita 108

SF 298 109

List of Figures

Figure Page

Figure 1- SD JOC model of deterrence 15
Figure 2- Consequences of Restraint 16
Figure 3- COR Fulcrum 17
Figure 4- Cyberspace "COR" Fulcrum 18
Figure 5- New Triad 18
Figure 6- Cyberspace deterrence in the "New Triad" 19
Figure 7- ORS Concept [46] 51
Figure 8- Implementation of the ORS Concept [46] 52
Figure 9- Influencing the Cyberspace "COR" Fulcrum 57
Figure 10- Cyberspace "COR" Fulcrum 58
Figure 11- Attribution's effect on the "COR" fulcrum 61
Figure 12- Identity Management Bridge 66
Figure 13- JP 5-0 Plan Development Activities 73
Figure 14- Phasing Model 75
Figure 15- Cyberspace Deterrence Model 79
Figure 16- A-10 Air-to-Air Refueling 85
Figure 17- Deterrence by Punishment Focus 92
Figure 18-Traditional View of Deterrence 93
Figure 19- Lever principles [70] 95
Figure 20- DO JOC model of deterrence [1] 96
Figure 21- Consequences of Restraint 97
Figure 22- COR Fulcrum 97
Figure 23- New Triad 98

List of Tables

Table Page

Table 1- Comprehensiveness of Sector-Specific Cyber-Security Plans [6] 8
Table 2- End-Ways-Means Deterrence Construct 25
Table 3- Technical Attribution Approaches [52]..... 60
Table 4- Critical Infrastructure Sectors..... 100

STRATEGIC DETERRENCE IN CYBERSPACE: PRACTICAL APPLICATION

I. Introduction

> ***"The major deterrent [to war] is in a man's mind. The major deterrent in the future is going to be not only what we have, but what we do, what we are willing to do, what they think we will do. Stamina, guts, standing up for the things we say—those are deterrents."***
> - Admiral Arleigh Burke, 3 October 1960, As quoted in U.S. News and World Report [1]

Background

The United States sits at an interesting decision point in its history- What is the future of United States cyberspace efforts? How will the government be organized to manage the risks and vulnerabilities created by the interdependencies of integrating nearly everything with the cyberspace domain? How will the government take advantage of the potential benefits associated with integrating into the cyberspace domain? The Obama administration's 60-day review of the state of US cyberspace policy was released near the end of this research, but no implementation of the recommendations in the review have been completed. Neither the policy review, nor the president's comments, contained an unequivocal declaratory cyberspace deterrence stance. As the US moves forward, cyberspace deterrence will gain greater importance as we seek to reap benefit from integrating into the cyberspace domain, but reduce the vulnerabilities from that same integration. It remains to be seen if the Obama administration will implement the recommendations of the cybersecurity review or implement a cyberspace deterrence policy.

Motivation

I was sitting through a briefing with a wing commander when he commented that his problem of defending Air Force networks would be easier if he could impose costs. If he could break a couple script-kiddie computers, word would get out in the hacker community and he would be able to concentrate on the bigger players- like nation-states that daily probe and "attack" the US information systems. What he was talking about was a cyberspace deterrence strategy. I combined this study of deterrence strategy with a pet project of mine- cataloging and identifying the nature and character of the cyberspace domain. This started me down the road to investigate and categorize how a practical deterrence strategy, one that considers the unique nature of the cyberspace domain, might be formulated and implemented by the United States.

Purpose

The purpose of this research is to identify how the unique character of cyberspace, when compared to the physical world, influences or modifies the application of deterrence strategies. It will identify specific means that allow the United States to pursue deterrence strategies in cyberspace in order to deter attack on the US critical infrastructure. Finally, it will identify key policy tradeoffs in advocating and constructing a cyberspace deterrence strategy.

Scope

This research looks at combining "ways" and "means" of deterrence towards the "end" of "Deterring cyber attack on the United States critical infrastructure**."** It should be noted that deterrence is a "wicked problem." [2] [1] Deterrence in cyberspace is even more "wicked". One of the characteristics of a "wicked problem is that "there is no definite formulation of a wicked problem." [2] That being said, this research contributes to cyberspace deterrence strategy by identifying and defining the most important dimensions to a very complex problem. By conducting an extensive literature review, common attributes of the cyberspace domain and their influence upon deterrence strategies emerge. Some applications may be appropriate to general cyberspace deterrence strategy formulation, while others will only be applicable to the specific end of deterring cyber attack on the United States critical infrastructure.

For the purposes of this research cyberspace is defined in JP-1 as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." [3]

As cyberspace thought and language are still developing and in flux I have used the term "cyber" throughout this work. Cyber is an adjective, but here I have also used it as a modifier as necessary to explain some concepts. For example, a cyber attack is an attack which can take place in cyberspace, on cyberspace, or through cyberspace. Its

---

[1] For a description of wicked problems see Dr. Tom Ritchey's research **"**Wicked Problems**:** Structuring Social Messes with Morphological Analysis**" at** http://www.swemorph.com/wp.html

effects can be felt both in cyberspace and outside of it. The attack can be generated from within the domain of cyberspace or from without. Another example might be cyber superiority. Cyber superiority is not a military doctrinal term. In the same grammatical way that the military uses air superiority, where air modifies superiority, I have used cyber to modify superiority. Grammatically, one should probably use words like cybersecurity, cyberpolicy or cybersuperiority, but when the majority of sources do not use "cyber" in this way I have elected to use the more common convention and use phrases such as cyber policy or cyber superiority.

In reviewing the available literature, and presenting the results in this research, a deliberate attempt was made to keep the data as fresh and current as possible. The Obama administration has withheld comment on many cyberspace policy issues. Despite the completion of the 60-day cyberspace review, very few specifics are available. Where there is currently no new public policy, this paper has referenced cyberspace policies and statements developed from the previous administration of President George Bush. Part of this research has involved the careful review of speeches from General Kevin Chilton, commander USSTRACOM, and Lt General Keith Alexander, Director National Security Administration (DIRNSA) and Commander Joint Force Component Command for Network Warfare(JFCC-NW), as these public officials often speak out on cyberspace related issues.

Results

According to the Deterrence Operations JOC: Joint military operations and activities contribute to the "end" of deterrence by affecting the adversary's decision calculus elements in three "ways":

- Impose Costs
- Deny Benefits
- Encourage Adversary Restraint [4]

This research looked at combining these "ways" of deterrence towards the "end" of "Deterring cyber attack on the United States critical infrastructure**."** To be successful cyberspace deterrence strategy must first be issued from the office of the President of the United States. The president must declare what is important, and then explain the lengths to which the United States will go to protect its critical infrastructure against a cyber attack. The United States must be ready to impose costs to cyber adversaries. Defenses and Responsive Infrastructure as a means of implementing cyber deterrence strategy are incomplete without the complementing means of Strike. In addition, to declaratory policy, and maintaining a robust force prepared to impose cost across the spectrum of policy options, the United States must seek to deny safe havens to cyber adversaries and garner international support for norms and laws that are favorable to the US position

As the United States seeks to deny the adversary benefit to their actions, some traditional ways of conducting deterrence operations may not directly translate to cyberspace. "Detect and Preempt" is not a viable deterrence strategy to apply to nation-states in cyberspace. Garnering deterrence lessons from other domains such as space or concepts in other established mission areas like WMD holds great promise. As such, denying the adversary the benefit of their actions by proving the US ability to fight through a cyber attack will potentially serve as great deterrent to adversaries. As the US

military plans for future conflict with cyber-capable foes, it must consider how its actions will be perceived by that enemy. JOPES planning should be updated to provide planning considerations for appropriately dealing with cyber-capable foes that could potentially attack the critical infrastructure of the United States. With some modifications, many of these considerations could be modeled after the already present nuclear sections in the JOPES planning process.

A balanced deterrence strategy contains all three elements in the DO JOC model; efforts to encourage restraint have the potential for the largest gains. Factors in the cyberspace domain which contribute to moving the "consequences of restraint" fulcrum include: attribution, identity management, and moderating trust relationships. Application that addresses these means will serve to multiply the effectiveness of US attempts to impose costs and deny benefits to the adversary.

Thesis Organization

This chapter presents the motivation, purpose, scope and results for this research, and concludes with the document's organization. Chapter 2 introduces the concepts of deterrence, the characteristics of the cyberspace domain, and lays out some of the challenges of creating a cyberspace deterrence strategy. It also demonstrates the use of the Deterrence Operations Joint Operating Concept and the New Triad as a basis for analyzing cyberspace deterrence strategy formulation. Chapter 3 uses an ends/ways/means approach to demonstrate practical steps by which a cyberspace deterrence strategy might be undertaken. Finally, Chapter 4 identifies the key policy

trade-offs associated with establishing a cyberspace deterrence policy and explores areas for future research.

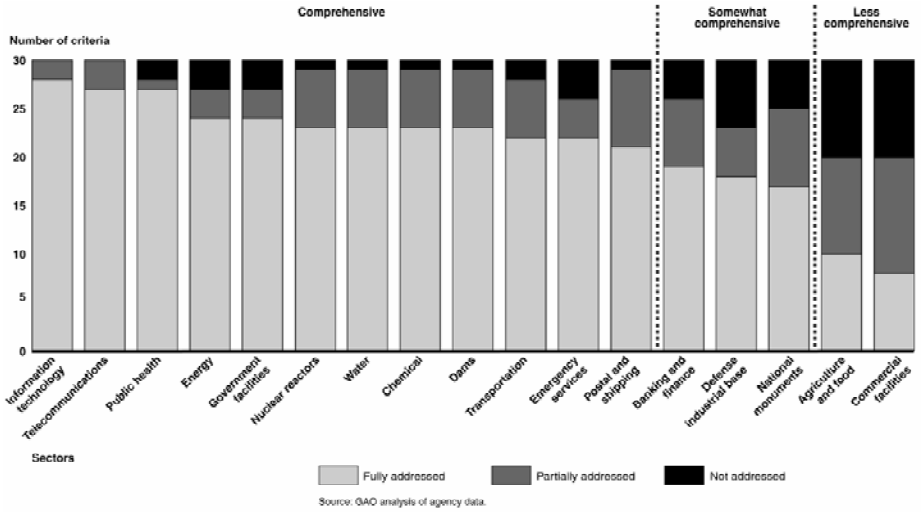
II. Formulating Deterrence Strategy for Cyberspace

The need for a deterrence strategy: US dependence on cyberspace

> *The United States must treat cybersecurity as one of most important national security challenges it faces. This is a strategic issue on par with weapons of mass destruction or global jihad, where the Federal government bears primary responsibility.*
> - Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency [5]

In May 2007, the Department of Homeland Security released an assessment of the cybersecurity plans for 17 critical infrastructure sectors.[2] The report found that no sector had completely addressed all 30 of the cybersecurity-related criteria. [6] This failure demonstrates the vulnerability of US critical infrastructure to cyber attack.

Table 1- Comprehensiveness of Sector-Specific Cyber-Security Plans [6]



[2] Reference the Appendices to see a full listing of the critical infrastructures of the United States

A scathing critique from the Government Accounting Office in March of 2009, reported that the Department of Homeland Security has not yet fully satisfied its cybersecurity responsibilities and the nation remains at risk from cyber attack. [7] In particular the report cited several examples of failures in strategy, guidance, organization and management of cybersecurity initiatives.

Modern critical infrastructure systems are complex and adaptive in nature. They rely heavily upon scale-free networks, like the internet. [8] As analyst Sean Gorman has pointed out, "while these types of networks are very resilient to random failures, they are very vulnerable to targeted attack. . . . [S]elf-organizing competitive networks are highly efficient, but have the negative externality of systemic vulnerability." [8] [3] Although, they can handle isolated outages, they are "susceptible to well-targeted, systematic, repetitive attacks on key nodes." This vulnerability makes cyberspace a center of gravity. In addition, this vulnerability entices US adversaries to attack the United States in and through cyberspace presenting a challenging deterrence scenario.

Cyberspace must be considered to be a part of the critical infrastructure of the US. "In its plan for protecting these critical infrastructures, DHS recognizes that the Internet is a key resource composed of assets within both the information technology and the telecommunications sectors." [9] This means that the United States must not only work to defend the information on its networks, not only protect the missions and processes that run in the domain of cyberspace, but that the actual structure of cyberspace must be

---

[3] Miller and Lachow quote Sean Gorman in their article from the following source: Sean Gorman, *Networks, Security and Complexity: The Role of Public Policy in Critical Infrastructure Protection* (New York: Elgar, 2005), 8.

designated critical infrastructure and defended at a level commensurate with its value. In fact, in the National Strategy to Secure Cyberspace, Cyberspace is described as the nervous system for which all other critical infrastructures depend upon-"the control system of our country." [10]

One construct that will help enable the defense of the information, processes and systems of cyberspace is the adoption and execution of a cyberspace deterrence strategy. Cyberspace deterrence may hold some promise to deal with the risks and vulnerabilities created by US cyberspace dependencies, particularly with regard to the critical infrastructure of the United States. However, deterrence strategies in cyberspace will only be as effective as the US ability to impose costs, deny benefits, and communicate the consequences of restraint to an adversary.

The challenges of deterrence in cyberspace

> *We face emerging forms of 21st Century warfare -- transnational terrorism, cyber warfare, and counter-space warfare -- which we have little experience in deterring. We need to think carefully about how deterrence will or will not apply to these threats and we need to tailor our deterrent strategy and associated capabilities accordingly. I believe deterrence does have a critical role to play in these threats.*
> –Vice Admiral Carl V. Mauney, Deputy Commander, USSTRATCOM [11]

Traditional deterrence, wrought out of Cold War prevention of conflict, escalation and ultimately nuclear war has several base advantages when compared to the issues of establishing a cyberspace deterrence policy. The fact that nuclear deterrence policy is more mature in its processes and thinking is certainly an advantage, but some of these

thoughts can shed light onto the issues surrounding cyberspace deterrence. Nuclear deterrence policy development is different from that in cyberspace, because nuclear weapons are costly and technologically difficult to develop. Materials to build nuclear weapons are limited and can be monitored and controlled in some respects. On the other hand, cyberspace technical expertise is widely available, and developing attack capability is relatively cheap. In his testimony before congress, Sami Saydjari described a scenario that he and other intellectuals developed to show to susceptibility of the United States' critical infrastructure to attack. Named Dark Angel, the exercise illustrated the damage that a campaign conducted across multiple attack vectors could cause to the United States. The goal of the exercise was to prove how easy it would be to destabilize the US and depress its economy through a series of attacks including those conducted in cyberspace. The projected cost of executing this plan: $500 million and three years of preparation. [12] This cost puts a devastating cyber-attack capability well within the purview of most nation-states and many modern organizations, including terrorist organizations and organized crime.

Jon Ramsey, chief technology officer for SecureWorks provides a good summation as to why cyber-warfare activities are so attractive:

- The low cost to launch cyber attacks compared with physical attacks
- The lack of cyber defenses
- The "plausible deniability" the Internet affords
- The lack of "cyber rules of engagement" in conflicts between nation states [13]

Compared to deterring attacks in the cyber-world, attacks conducted in the physical world must overcome the frictions imposed by time and space. This allows intelligence agencies the ability to identify key indicators that evidence when an attack is

imminent or in progress. Intelligence can then be focused to look for these key indicators, or named areas of interest, to monitor the status quo and report deviations. This time and space also permits command and control agencies and leadership the time to make decisions based on the information (indicators) and issue orders to respond to the attack. Carrying the example of the nuclear attack further, one of the ways a nuclear strike might be conducted is by delivering a nuclear weapon on the tip of a missile. Therefore, the United States has invested great quantities of money, time, manpower and energy into detecting, tracking and predicting when missiles are launched. The threat (ie risk) necessitates this investment. Satellites are deployed to watch for missile launches around the globe. The information is sent to command and control agencies that analyze the trajectories, process the information, and make determinations as to the purpose of the missile (is it launching a satellite into space, or carrying a nuclear warhead bound for the US?). They are empowered to communicate the information to leadership and issue orders to counter the threat. Communications links are established that allow leadership to receive the information, make decisions, and render orders. All of this occurs within the time-of-flight of a missile inbound to the United States. Again, the threat to the country, the populace and the way of life of the American people dictates that it must be so and it dictates this significant investment.

An attack conducted through cyberspace does not have the same frictions with regard to time and space. Ones and zeros travel around the globe at the speed of light. Vice Admiral Carl V. Mauney, Deputy Commander USSTRATCOM, described this characteristic of warfare conducted in cyberspace as moving at “net speed” in his address to the Network Centric Warfare 2009 conference. [14] This decreases the amount of time

it takes to for an attack launched through cyberspace to reach the United States. This characteristic of attacks conducted through cyberspace offers an asymmetric advantage, and is a key benefit to the adversary. This is one reason cyber attacks are so attractive to an adversary and so difficult to deter.

There are no plumes to detect in cyberspace; named areas of interest are difficult to identify. Key identifiers to predict, detect, track, and describe an incoming cyber attack are reduced or minimal as compared to the physical world. When a bit shows up at your door, is it a "good" bit or an "evil" bit? If it is an "evil" bit, the warning time is, in effect, zero. The attack is in progress. Again, the reduced ability to detect, track and categorize a cyber attack increases the likelihood of an adversary using a cyber attack, and makes deterrence more challenging. Cyberspace deterrence approaches must take into account these facets of the domain. They must also provide schemes to deny the benefits of exploiting these same characteristics of cyberspace.

Finally, attribution and identification are extremely challenging in cyberspace. This makes imposing costs on a cyber adversary complicated. Developing proportionate responses that target the appropriate actor without undue collateral damage (due to the global interconnectedness and potential commandeering of private and commercial systems, like bot-nets) are difficult.

Any successful cyberspace deterrence policy will have to seek to reduce the benefits of the cyber attack to the adversary, increase the adversary's cost of using cyber attacks, and provide attractive alternatives to cyber attacks that encourage adversary restraint.

Deterrence Operations Joint Operating Concept and the New Triad

Deterrence Operations Joint Operating Concept

> *Deterrence operations convince adversaries not to take actions that threaten US vital interests by means of decisive influence over their decision-making. Decisive influence is achieved by credibly threatening to deny benefits and/or impose costs, while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome.*
> –Deterrence Operations Joint Operating Concept [4]

According to the DO JOC executive summary:

> The central idea of the DO JOC is to decisively influence the adversary's decision-making calculus in order to prevent hostile actions against US vital interests. This is the "end" or objective of joint operations designed to achieve deterrence.
>
> An adversary's deterrence decision calculus focuses on their perception of three primary elements:
>
> - The <u>benefits</u> of a course of action
> - The <u>costs</u> of a course of action
> - The <u>consequences of restraint</u> (i.e., costs and benefits of not taking the course of action we seek to deter)
>
> Joint military operations and activities contribute to the "end" of deterrence by affecting the adversary's decision calculus elements in three "ways":
>
> - Deny Benefits
> - Impose Costs
> - Encourage Adversary Restraint

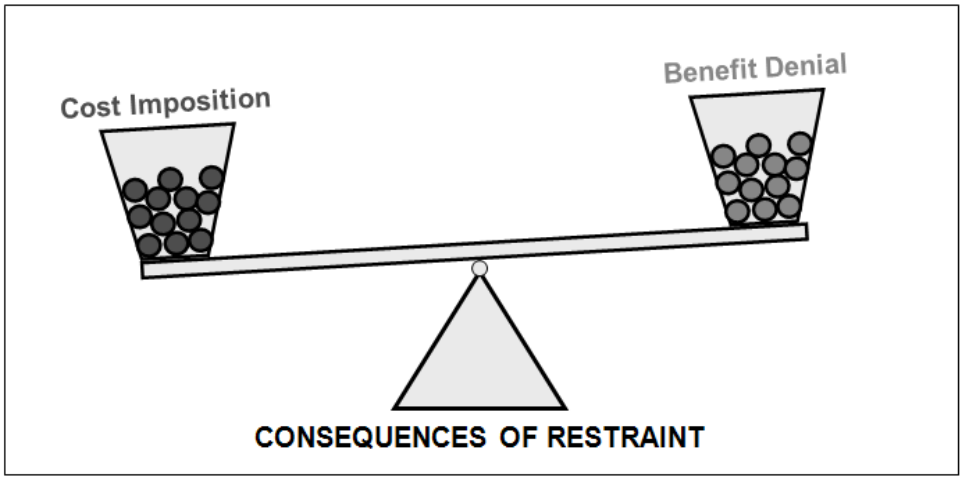


Figure 1- SD JOC model of deterrence

Deterrence is successful, in the DO JOC model, when the perceived costs incurred by an adversary outweigh the perceived benefits in regard to the consequences of restraint (fulcrum).

Deterrence fails in this model when an adversary perceives that the benefit of taking an action outweighs the costs, and thus the adversary takes the actions which are contrary to US interests.

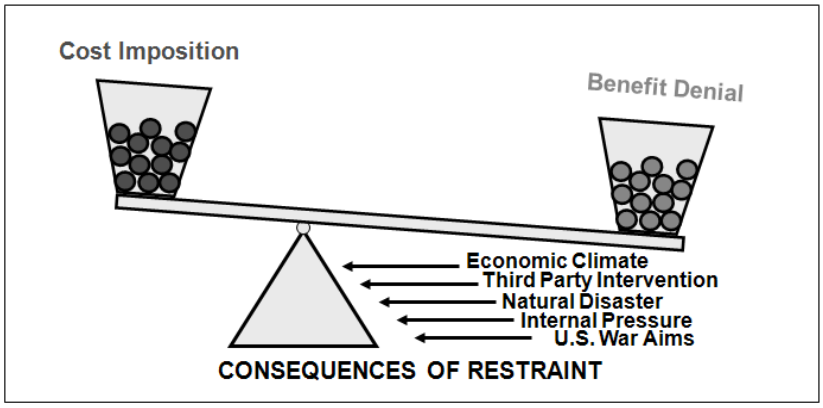


Figure 2- Consequences of Restraint

The difference of the DO JOC from older deterrence conceptualizations is found with the consequences of restraint fulcrum. "Given an otherwise favorable situation, forces exist that may cause an adversary to act contrary to US interests. Increasing adversary consequences of restraint can (over time) result in deterrence failure. These factors influence the capabilities the US must employ to maintain/restore deterrence." [1] Obviously, if the physics upon which the model is based hold true, then deterrence efforts will have their greatest effect when they move the "consequences of restraint" fulcrum so as to make imposing costs on the adversary and denying adversary benefit more effective.

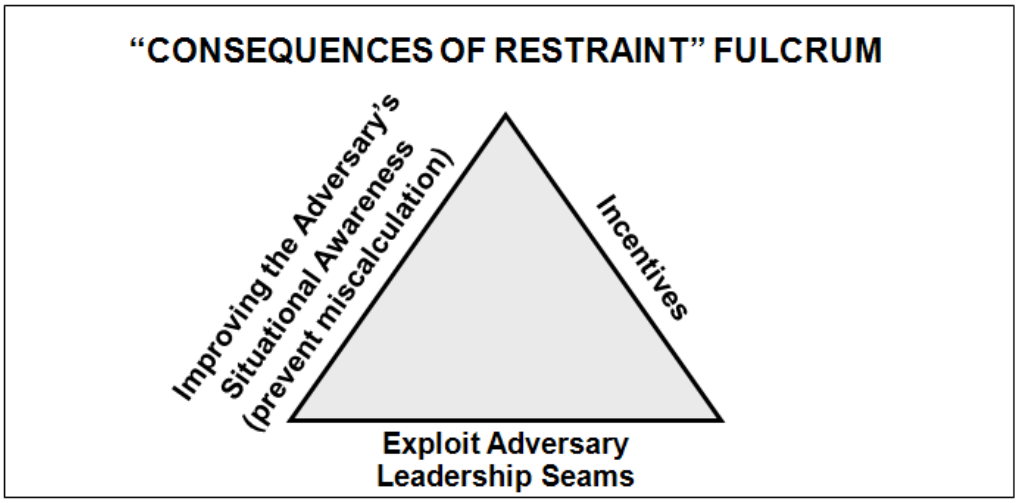


Figure 3- COR Fulcrum

The elements of the consequence of restraint fulcrum are not well established or agreed upon, but the authors of the SD JOC[4] feel it includes at a minimum: Improving the Adversary's Situational Awareness, Providing Incentives to the adversary, and Exploiting Adversary Leadership seams." [1] Attribution, Identity Management and moderating the trust relationships of cyberspace should be considered as potential concepts that influence the "consequences of restraint" fulcrum in cyberspace deterrence.

[4] The DO JOC has also been called the Strategic Deterrence Joint Operating Concept (SD JOC)

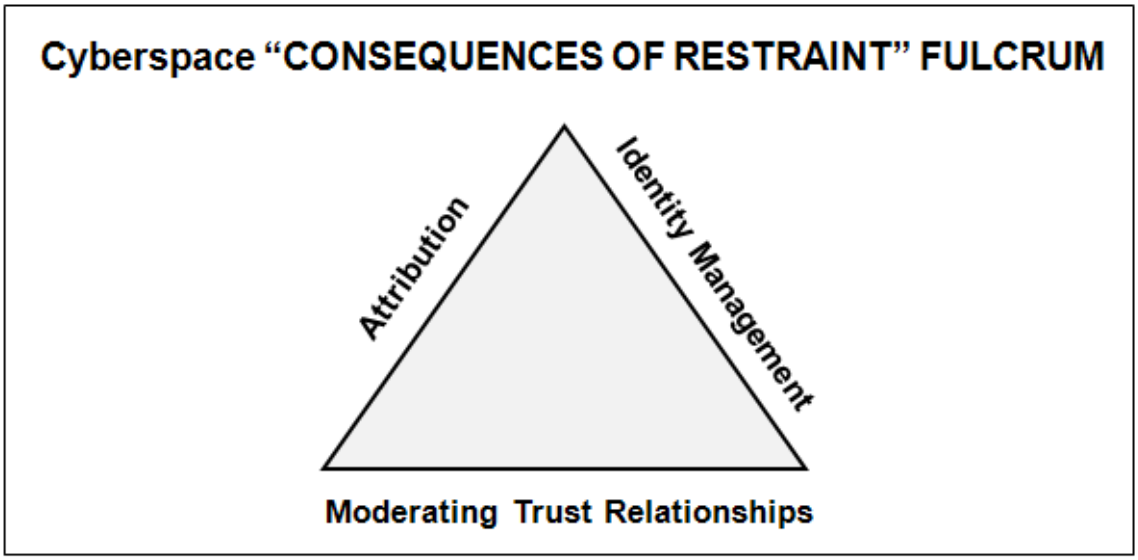


Figure 4- Cyberspace "COR" Fulcrum

The New Triad

Another emerging idea, and a way that deterrence has changed from the Cold War era, is in the concept of the New Triad. In January of 2002, President George W Bush, announced a new strategic triad in the Nuclear Posture Review (NPR). This new triad is based on: nuclear and precision non-nuclear strike forces; passive and active defenses; and a revitalized defense infrastructure. [15]

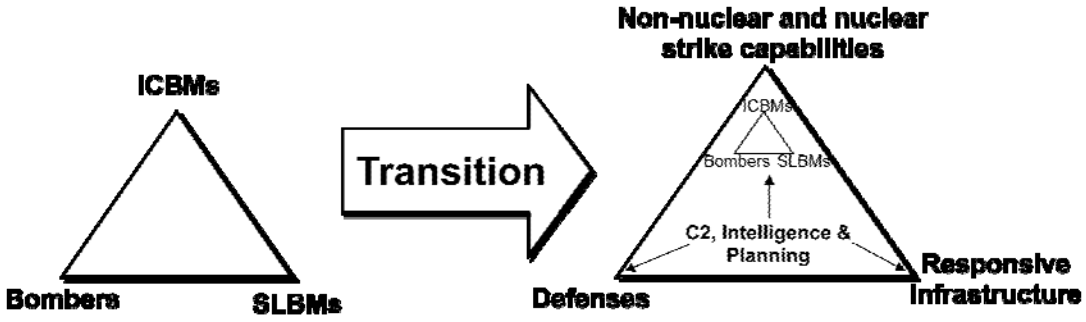


Figure 5- New Triad

In the new triad, deterrence is bolstered through the US ability to respond with tailored means to aggression. Although conceived originally for nuclear deterrence, the new triad can stand in nicely on other deterrence efforts- including efforts in cyberspace. Cyberspace deterrence efforts can be categorized into the Strike, Defense and Responsive Infrastructure legs. Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Operations (CNO) all fit neatly into this paradigm.

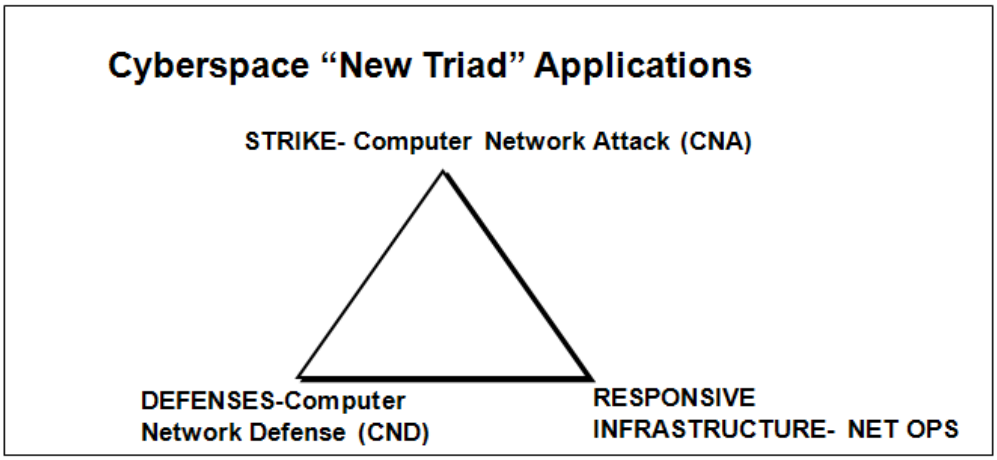


Figure 6- Cyberspace deterrence in the "New Triad"

One drawback to the new construct is that it doesn't account for the adversary's consequences of restraint. This can be found in the DO JOC construct of describing deterrence strategy. When combining the new triad with the DO JOC concept of deterrence, you have an able means of both categorizing US deterrence efforts in the new triad, and describing deterrence effects focused on an adversary with the DO JOC.

Deterrence is about decision making. It involves influencing the adversaries' perceptions- what they might gain or not gain as a result of their actions, and what they might gain or not gain as a result of their restraint from action. The DO JOC follows an Ends-Ways-Means construct to operational deterrence strategy. This construct is highly useful for communicating how a deterrence strategy may be constructed, implemented and monitored. The End-Ways-Means construct will be leveraged for examining cyberspace deterrence strategy formulation and for analyzing the affect of the unique character of the cyberspace upon developing deterrence strategies.

Preparing for Cyberspace Deterrence: Building a cyberspace culture

> *We have to transition from a culture of convenience to a culture of responsibility. We must recognize vulnerability -- the vulnerability that one system can create here on the other side of the world, not just locally.*
> -General Kevin Chilton, Commander USSTRATCOM

General Kevin Chilton, Commander USSTRATCOM, advocates that the military needs a change in culture, conduct, and capabilities in order to address the challenges of operating in the cyberspace domain. Many of his efforts are aimed at educating people: congressman, military personnel, and citizens on how to best operate in and defend the military's use of cyberspace. Education is necessary to effectively employ a deterrence strategy for cyberspace. These education efforts must not be limited to the military, but must encompass many across the nation's population. Part of this education process must include an understanding of how US actions seek to deter adversaries from attacking the United States and its critical infrastructure. This policy needs to be enunciated from the highest levels of the US government.

US Deterrence policy is hampered by the fact that no one is in charge of a unified cyberspace deterrence effort that spans government and civilian efforts. US Strategic Command (STRATCOM) develops deterrence plans and cyberspace plans for the Department of Defense (DOD). However as General Kevin Chilton, Commander USSTRATCOM stated in his testimony before the house armed services committee, "STRATCOM is chartered to operate and defend our military networks only. And so we worry about the dot-military networks. We are not asked today to defend the dot-edu, the dot-com, the dot-gov. The consideration for defense of vulnerabilities in that area falls to the Department of Homeland Security." [16] Thus, overall authority must rest with the president of the United States.

The Obama administration's 60-day cyberspace review was released on 29 May, 2009. In his remarks, President Obama indicated that a Cybersecurity Coordinator will be appointed to centralize US cyberspace policy decisions; time will tell whether this individual can successfully coordinate all cyberspace issues including deterrence policy. In his remarks on securing the nation's cyber infrastructure the president did confirm that networks and computers will be treated "as a strategic national asset." He mentioned that the US would "deter, prevent, detect and defend against attacks;" however, he did not issue a declaratory policy that clearly establishes the US intent to use any means at its disposal to protect the US use of cyberspace. [17]

Current cyberspace security efforts could easily be categorized into the new triad deterrence framework. Examples of strike, defenses and responsive infrastructure abound. Without the enabling means of a coherent cyberspace deterrence strategy, these efforts will not serve the interest of strategic deterrence. New firewalls may make it more difficult for adversaries to achieve their cyberspace goals, and cyber-attack squadrons may add new strike proficiencies to the arsenal, but they will not necessarily contribute significantly to deterring aggression against the United States and its allies.

The new triad of strike, defense and responsive infrastructure provides the bones from which to hang the sinews and muscle of a coordinated cyberspace deterrence strategy. However, a concerted educational process must be initiated to communicate both to adversaries and to the nation. How will the adversary decision-maker be convinced of the costs of his actions, lest the United States reveal its capability to strike him? Cyber capabilities are locked up in compartmentalization and classification. Just as in the

nuclear arena, some capability must be demonstrated and revealed in order for the threat to be a part of the cyber-adversaries' calculations, but not every secret must be exposed to make that threat credible.

Friendly forces also must be educated. Once a cyberspace deterrence strategy has been implemented, the players at each tip of the triad must understand how they contribute to overall cyberspace deterrence, and how their actions contribute and interplay with the focused deterrence efforts for individual actors. How does the ISP admin contribute to the deterrence policy of the United States in the infrastructure leg? He's not even in the military. What is the role of the Joint Task Force- Global Network Operations in the defense branch or the responsive infrastructure branch? Understanding the answers to these types of questions will enable a more effective cyberspace deterrence posture.

When I went through requalification training for the A-10 at Barksdale AFB, LA, I had to go get a flight physical. While at the hospital- they locked my medical records in a small folder. They had the only key. Why? There are B-52s at Barksdale capable of carrying nuclear weapons. Hospital personnel locking medical records contributed to national deterrence strategy. Assuring that medical records were not compromised helped nuclear operators and maintainers complete their missions as part of the Old Triad- a legacy of Strategic Air Command (SAC). Deterrence policy in this case focused people and rallied them around an ideology. "Ideology is the fuel that drives the

decentralized organization," [18] according to Ori Brafman and Rod Beckstom[5] in their book "The Starfish and the Spider." One way to get at the culture change that General Chilton speaks about is to consider how to hybridize the centralized US government and decentralized cyberspace. Put another way, the US must take the best aspects of centralized and decentralized organizations in order to better operate in cyberspace: a domain characterized by decentralization. Cyberspace deterrence policy can be one way to express ideology which will focus effort and help people understand their roles in defending the United States.

Creating an effective deterrence policy will entail creating new relationships and educating the operators and maintainers of cyberspace on how they fit into that plan. As Lt. General Alexander reported to the House Armed Services sub-committee on Terrorism, Unconventional Threats and Capabilities, "Realistically, [a cyber attack] will be asymmetrical against industry and critical infrastructure. So the question is the partnership between defense, the Department of Homeland Security and intelligence community. That has to be clear and the rules have to be laid out and walked through. We haven't gone far enough yet." [19]

[5] Rod Beckstrom served as the former Director of the National Cyber Security Center.

III. Practical Implementation and Application of Deterrence Strategy in Cyberspace

Table 2- End-Ways-Means Deterrence Construct

End: Deter cyber attack on US critical infrastructure.		
Objective:	**Ways (effects)**	**Means**
Impose Costs	**US will escalate in response to an attack**	**Declaratory policy-** view cyberspace as part of our critical infrastructure and reserve the right to respond with cyber and non-cyber means to an attack
	US will hold the adversary's infrastructure at risk	**Maintain and Exercise Capabilities-** Concerted plan to study actor infrastructure, establish and maintain a presence and be prepared when called upon to conduct a debilitating attack.
	US coalition likely to grow	**International Agreements-** Enhance cyber norms, condemns unwanted behavior, reinforces negative consequences for adversary actor
Deny Benefits	**Preparation for attack seen as likely to be detected and preempted by US**	**"Detect and Preempt"** Deterrence effectiveness questionable due to Cyberspace/physical world differences
	Attack will not provide asymmetric advantage sufficient to defeat US forces	**Contested Operations-** US not completely dependant on cyberspace, but prepared to operate in a contested environment and fight-through attacks, compare to US preparations to fight in a chemical environment
	Active Defense of targets seen as highly effective	**Robust Infrastructure** **Obfuscation techniques** **Response Options**
	Information Networks viewed as secured and robust	**Cyberspace training, Network accountability and readiness-** automated security protocols and

		updates **Identity Management**- control who has access to cyberspace domain systems
Encourage Restraint	**Certain targets not justifiable (**US critical infrastructure)	**International consensus-** what are legitimate targets in cyberspace
	Incentives	**Trust**- disconnect from those adversaries who abuse trust
	Situational Awareness Maintained by adversary leadership	**Shared situational awareness-** specific actor engagement or define what is acceptable CNE
	US war aims appear limited	**Consider adversary cyberspace capabilities**- Transform military planning through JOPES

End: Deter cyber attack on US critical infrastructure.

> *Our critical infrastructure systems are fundamentally dependent on the Internet and IP-based technology, and there are interdependencies between them that our enemies will seek to exploit. Cyber warfare completely evens the playing field as developing nations and large nations with a formidable military presence can both launch equally damaging attacks over the Web.*
> – Professor Howard A. Schmidt, Georgia Tech Information Security Center [13]

The Wall Street Journal headlines blare out the warning- "**Electricity Grid in U.S. Penetrated By Spies.**" [20] According to the article, cyberspies from China, Russia and other countries have penetrated the US electrical grid and left software behind that could potentially disrupt the flow of electricity. [20] After the revelation, US Homeland Security Secretary Janet Napolitano said, "The vulnerability is something that the

Department of Homeland Security and the energy sector have known about for years. We acknowledge that ... in this world, in an increasingly cyber world, these are increasing risks." [21]

This example gets at the crux of the issue with cyberspace deterrence- what do we want to deter and how do we deter it? We have known about the threat for years, but we haven't done very much to deter the threat. Two main perspectives emerge from this electrical grid compromise. First, should the US only seek to deter the actual debilitating attack which actually results in the loss of critical infrastructure, lives, property, military or government capability? In the example case, deterrence policy would not seek to dissuade the Chinese, Russians and other nations who have embedded potentially devastating software in the US electrical grid. After all they didn't actually conduct an attack on the system, they only gained access and maintained to ability to conduct the attack. According to this view, the goal of deterring attacks against the critical infrastructure of the United States is best pursued by deterring only the actual attack against the infrastructure.

The other point of view is that a cyberspace deterrence policy should focus on deterring an actor from even attempting the initial access let alone implanting potentially harmful software in the system. Obviously, the first perspective has the advantage that it bounds the problem and its potential solutions to just the realm of deterring the attack on the critical infrastructure of the United States. The second perspective poses more problems, since it must deter activities on a much wider scale. These pernicious activities- obtaining unauthorized access to a system, hacking, introducing malware or

viruses are widespread. These activities cross the gamut of categorization: criminal, espionage, war. Can any policy, or multiples of deterrence policies, satisfactorily address the issues raised with this kind of approach?

Deterrence strategies are tailored to influence adversaries. When pursuing an end like "Deter cyber attack on US critical infrastructure," who should you focus your efforts on? Starting with the most capable cyber actors seems logical. Breaking those actors out into those who have the means and the motivation will further refine the search. In the electrical grid example- starting with Russia, China and the other countries involved in breaking into the systems would seem prudent. According to Andrew Macpherson director of the technical analysis group at Justiceworks:

> Nation states potentially pose the greatest threat with regard to cyber security to the United States. Clearly Russia and China are two of the top countries because they have more developed capabilities, but it may not be in their interest to use cyber attacks for strategic attacks ends.[sic] Both countries have worked on doctrine and there is some evidence that they are incorporating it into their military training as well. However, individuals, political groups, religious groups and organized crime groups also pose ongoing risks and should be considered cyber threats, as well. [22]

Identifying the most capable and motivated actors requires a large personnel and intelligence investment. Further, consideration should be given to examining what type of activities will be accepted and which activities a US cyberspace deterrence policy will be focused on preventing. The ways in which a deterrence policy is formulated can be categorized as imposing costs, denying benefits and encouraging restraint. To

accomplish an end such as “Deter cyber attack on US critical infrastructure” all three ways will need to be incorporated.

Objective: Impose Costs

> *Nowadays, electronic attacks are increasingly seen as a cheap and easy way for one nation to attack another. "It's the ultimate bargain hunter's way of destroying everyone's way of life. It may even be free.”*
> - Glenn Zimmerman, a cyberspace specialist at the Pentagon. [23]

Deterring cyber attacks on the critical infrastructure of the United States must involve the ability to impose costs. Currently there are so few costs applied that attacking the US critical infrastructure via a cyberspace means incurs very little cost or risk to an actor. Part of his judgment must be to re-consider conducting cyber attacks against the United States, based on the costs of such actions. There are several means by which a cyberspace deterrence policy may be constructed. Declaratory policy and the formation and application of response options are two such means that might be applied to impose costs on an adversary to influence their decision making.

The inherent character of cyberspace influences the effectiveness and application of means to influence an adversary’s decision to conduct an attack on the critical infrastructure of the United States. The predominant characteristic of cyberspace that influences actor decision making is attribution: Attribution is difficult in cyberspace. One of the conclusions from STRATCOM Cyberspace Symposium (April 2009) cyberspace deterrence working group was that “Attribution is key to imposing costs.” The ability of the United States to determine attribution for attacks is a thread which runs

throughout all of the ways in which deterrence policy is applied: imposing costs, denying benefits and encouraging restraint. For this reason, attribution is a leveraging ability[6] which multiplies the effectiveness of deterrence policy, and is addressed as a means to encourage adversary restraint.

As General Chilton reported to Congress:

> Well, deterrence in any area involves a couple things. One, a position needs to be taken on -- a policy position, if you will. So you have to be able to look at somebody in the eye and say, "If you do this, then." And then whatever the "then" is has to be credible, both credible internally, but most important, credible in the individual's eye who you are trying to deter. [16]

If the US is to have any success at imposing costs it must establish a cyberspace deterrence policy and communicate that policy to potential cyber adversaries. Cost must be applied to adversaries in both cyberspace and in other domains as necessary to deter violent or undesired activities. One of the costs that the US must seek to impose on cyber adversaries can be called “denial of sanctuary.” Adversaries must be held accountable for their actions and denied safe haven if they insist on opposing the United States or its allies.

---

[6] See Appendix A for a description of the unique advantages offered by the consequences of restraint fulcrum.

Strategic Communication

> *Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself.*[7] [24]

Nation-states must carefully contemplate cyber actions against Russia, based on this communicated policy. By expressing a cyberspace deterrence stance the Russians are more effective at deterring cyber aggression than the United States? The United States lacks declaratory policy in relation to cyber attack. The same Russian theoretician who gave the above quote stated:

> From a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not . . . considering the possible catastrophic consequences of the use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces [24]

The United States has no such consideration when it comes to cyber attacks. The view that the US takes towards cyber attacks against its critical infrastructure or military needs clear enunciation. The US must be careful when crafting its declaratory cyber policy, because not everyone will understand the message in the same way. When trying to understand these Russian comments, it is important to understand that the Russian

---

[7] As quoted from V. I. Tsymbal, "Kontseptsiya `Informatsionnoy voyny'" (Concept of Information Warfare), speech given at the Russian-US conference on "Evolving Post-Cold War National Security Issues," Moscow 12-14 September 1995, p. 7.

definition of Information Warfare varies from the United States' definition.[8] This is one reason it is important to tailor deterrence policy. This is also one difficulty with tailoring deterrence policy, especially declaratory policy.

A declaratory policy focused at the Russians, may communicate something entirely different to the Chinese. If the goal of deterrence is to influence the perceptions, decisions and actions of an adversary, what the United States communicates through its actions and words is critical to the contribution or detraction of deterrence. [25] A lack of communication, or silence, is in itself a communication. The interpretation of US silence on declaratory cyber policy is even more difficult to ascertain than if the US had issued a declaratory policy.

In 1997, the Report to the President's Commission on Critical Infrastructure Protection listed three steps that might be taken to reduce vulnerability to attack and how they should be accomplished in cyberspace:

> Step 1: Declare a Policy and Build International Consensus
> Step 2: Harden Targets and Deny Access
> Step 3: Share Information, Conduct Analysis, and Issue Warning notices

[8] "Russian definitions of IW encountered thus far do seem to adhere to a common theme that differs from the U.S. view, namely that information warfare is conducted in both peacetime and wartime. In its peacetime use, the term refers to the information security of society and the government in the psychological, scientific, cultural, and production aspects, among others. In its wartime use, it refers to the attainment of superiority in the use of information protection and suppression systems, to include command and control, EW, and reconnaissance." [76]

All three of these steps are just as viable today as they were twelve years ago. Unfortunately, they are still just suggestions and not realities. The findings of the report remain relative for today:

> While the US government as a whole has not yet framed a declaratory policy concerning cyber attacks and cyber attackers, public statements from individual government agencies avow US intent to pursue a peacetime program of offensive information operations. This apparent disconnect needs to be addressed. To deter cyber activities against the United States, The US government, not individual agencies, must declare its policy toward cyber intrusions, and then begin the work of forging an international consensus in support of that policy. [26]

There is no doubt that the departments of the US government are focused on developing offensive cyberspace capabilities and developing cyberspace deterrence policies.[9] Nevertheless, with no over-arching US declaratory cyberspace deterrence policy, adversaries must attempt to cut through the din of voices, and try to discern what US response might be in relation to a cyber attack. The report from the CSIS Commission on Cybersecurity for the 44th Presidency, recommended that "the president, as one of his earliest actions, should make a statement of fundamental government policy for cyberspace. This statement should make clear that cyberspace is a vital national asset that the United States will protect using all instruments of national power." [5 p. 18] This statement would obviously go beyond protecting US critical infrastructure assets and the

---

[9] The DOD's 2009 QRM stated, "The Department's vision is to develop cyberspace capability that provides global situational awareness of cyberspace, U.S. freedom of action in cyberspace, the ability to provide warfighting effects within and through cyberspace, and, when called upon, provide cyberspace support to civil authorities." Moreover, the mission statement of USSTRATCOM is "The missions of US Strategic Command are: to deter attacks on US vital interests, to ensure US freedom of action in space and cyberspace …"

US military from cyber attacks, but would make cyberspace itself a strategic asset to be protected. Some have even suggested that a “cyber Monroe Doctrine” is what is called for.[10] President Obama’s public policy statements have not risen to the standard of a cyber Monroe Doctrine, let alone implement the recommendations that presidential advisors have been making since 1997.

US national-security officials have alleged that the Chinese and Russians have left behind software that could be used to disrupt the US electrical system. In response to these claims, the Chinese Foreign Ministry spokeswoman Jiang Yu said at a regular press conference “The intrusion doesn’t exist at all.” [27] A spokesman for the Chinese Embassy in Washington, Wang Baodong stated that "some people overseas with Cold War mentality are indulged in fabricating the sheer lies of the so-called cyberspies in China." [20] No US declaratory policy may be pointed at to guide US response and take appropriate action or impose costs. The US will instead rely upon the other two legs of the “New Triad”: Defense and Responsive Infrastructure. Until a declaratory cyber policy is made, cyber adversaries will not conceive of the US as willing to impose costs to their cyber hostilities.

---

[10] During a hearing of the House Armed Services' Terrorism and Unconventional Threats Subcommittee, Rep. Jim Cooper, D-Tenn., asked NSA Director Lt. Gen. Keith Alexander if he thought the United States should develop a "cyber Monroe Doctrine." Lt Gen Alexander, dual-hatted as the commander of the Joint Functional Component Command for Network Warfare, replied, "Yes, I think we need a cyber Monroe Doctrine." [84]

"Information Warfare[11] attacks on the United States are deterred by the same policy that deters other types of attack. Acting under its rights as a sovereign state, the U.S. stands ready to respond to any attack on its interests with all appropriate means, including law enforcement as well as military capacity." [28] Unless this is the established strategy from the top of the US government, US deterrence efforts will be stymied or fail.

Denial of Sanctuary

> *We know that if someone flies -- you know, shoots missiles at us, they're going to get a certain kind of response. What happens if it comes over the Internet, if it's a terrorist group, if it's a terrorist group sitting in a safe haven, if it's a nation state enabling the terrorist group, if it's a nation state itself, and what is the level of proof we're going to need, and what are the steps we're going to take to respond? That is the kind of doctrinal strategy that we haven't put together yet.*
> –Former US Secretary of Homeland Security Michael Chertoff [29]

International borders and physical location do not present the same impediments to an attacker in cyberspace as in the physical world. [26] However, government agents (like the DOD) or cyber investigators do restrict themselves with physical borders, jurisdictional issues, and international law. There is a reason that many see attribution as the key to imposing costs in cyberspace. Cyber attackers take advantage of safe havens due to the characteristics of the internet that allow one to be anywhere in the world and create effects in other parts of the world. They can physically reside in nation states that look the other way and do not enforce the rule of law. Thus, the US is left in the

---

[11] Information Warfare is not synonymous with cyber warfare or the same thing as warfare conducted in cyberspace. The reader should consider the quotation in light of cyber warfare being a subset of information warfare, but not all cyber warfare is information warfare. The basic principle at work is that the same deterrence policy which deters other types of attacks can apply to deterring cyber attacks.

quandary of imposing and enforcing a nation-state paradigm as it acts in a borderless cyber commons.

Take for example, the story of Russian hackers Alexey Ivanov and Vasiliy Gorshkov. The two flew to Seattle for a job interview with a tech company, only to find themselves arrested in a sting operation to net foreign hackers. In order to get evidence for prosecution, the FBI recorded the two hacker's keystrokes. The FBI then hacked the pair's computers in Russia and conducted a search obtaining 250 gigabytes of information. This was all done without obtaining the Russian authorities' approval. The defense argued that the FBI over-stepped its search and seizure authority when it hacked Ivanov and Gorshkov's computers. Russia's intelligence agencies claimed that the FBI's actions were "illegal and criminal." U.S. District Judge John C. Coughenour dismissed this argument saying the US government's search was not entitled to Fourth Amendment protection, because the files remained on Gorshkov's computer in Russia. "Coughenour also said that even if the Fourth Amendment did apply to data in a foreign country, the government had good reason to conduct a warrantless search." [30]

This example is obviously not a case of an attack against the critical infrastructure of the United States. However, it reveals some of the difficulty that a nation-state has in operating within the constraints of geographic boundaries and traditional law in the border-agnostic domain of cyberspace. If the two Russian hackers had never come to the US, they most likely would never have been arrested and prosecuted for any crime. If the US investigators had not conducted a search and seizure of information across

international boundaries to computers physically located in Russia, without Russian approval, the US would not have had sufficient evidence to convict the two hackers.

The larger issue becomes how to deter those, intent on attacking the US critical infrastructure, who take refuge outside the US with either implicit or tacit government approval. The news is filled with stories of adversaries that daily "attack" US systems or prepare for attacks against the US critical infrastructure. [31]

Another way in which adversaries take advantage of physical borders and are provided sanctuary is by routing traffic through countries which do not have the technical means or do not have the desire to cooperate with a cyber investigation. Finally, these adversaries can use cyber attacks to exploit legal and conceptual sanctuaries created by US confusion over defending private, commercial, government and military networks.

Cyber adversaries receive sanctuary in nation-states that condone cyber attacks, maintain laissez-faire attitudes towards cyber attacks, or are too weak or too technically deficient to police those who conduct cyber attacks. If it sounds familiar, it is because similar arguments have been made in deterring the use of terrorists or those extremists who wish to do the Unites States harm. In the 2006 National Strategy for Combating Terrorism (NSCT), the US strategy was stated as:

> The United States and its allies and partners in the War on Terror make no distinction between those who commit acts of terror and those who support and harbor terrorists. Any government that chooses to be an ally of terror has chosen to be an enemy of freedom, justice, and peace. The world will hold those regimes to account.

One way to provide greater deterrent to those who would plan attacks against the US critical infrastructure through cyberspace, is to hold nations accountable for the cyber activities conducted within their borders. Drawing further parallel from the NSCT, further international agreement on what constitutes an attack in cyberspace, or recognition for support of the US view on these issues is necessary. "Yet some countries will be reluctant to fulfill their sovereign responsibilities to combat terrorist-related activities within their borders. In addition to cooperation and sustained diplomacy, we will continue to partner with the international community to persuade states to meet their obligations to combat terrorism and deny safe haven under U.N. Security Council Resolution 1373."

The NSCT does recognize that "Cyber safe havens" exist, but as declaratory policy goes, it is weak. The declared policy of the US to counter terrorism in the cyberspace domain is to "discredit terrorist propaganda by promoting truthful and peaceful messages" and "to deny the Internet to the terrorists . . . for their propaganda, proselytizing, recruitment, fundraising, training and operational planning." It does not seem that terrorists are deterred from using the internet for any of these purposes, let alone conducting an attack against the critical infrastructure of the United States. A cyberspace deterrence strategy must incorporate a declaratory policy that goes beyond the NSCT definition of "cyber safe havens." It must acknowledge that those who would attack the US critical infrastructure through cyberspace, or plan for the attack, will be pursued and brought to justice. This policy must recognize that cyberspace infrastructure is part of the critical infrastructure of the United States and will be protected from harm. The US will have to work with other nation-states, just as it does to combat terrorism,

across the spectrum of policy options- assisting in the prosecution of those who would threaten the US and forcing governments to acknowledge their role in conducting, or permitting cyber attacks on the US.

It will be important for the US to engage other nations through many venues including the United Nations in order to remove sanctuaries for cyber adversaries. The United Nations International Telecommunication Union (ITU) just established a new partnership with the International Multilateral Partnership Against Cyber-Threats (IMPACT) in Malaysia in order to enhance the global community's capacity to prevent, defend and respond to cyberthreats. [32] On February 18th, 2009, UN Secretary-General Ban Ki-moon stated that the UN's Advisory Board on Disarmament Matters will be considering cyber warfare and its impact on international security. [33] "Ban said recent breaches of critical systems represent 'a clear and present threat to international security', since the public and private sectors have grown increasingly dependent on electronic information." [23] Unfortunately, as the report from the CSIS Commission on Cybersecurity for the 44th Presidency notes, "It is ironic that some of the countries that most vigorously advocate a UN treaty are known sanctuaries for cyber crime and are themselves suspected of launching cyber attacks."

Focusing international attention on this area of security is a positive step, but the United States has something to lose in these talks. As Secretary-general Ban stated, cyber weapons are "to be added to the list of arms falling under the remit of the UN's Advisory Board on Disarmament Matters." [23] This would impose limits to US means to project cyber power. The fear is that the US would be obligated to abide by weapons restrictions, but that these restrictions would create opportunity for those actors who do

not observe UN restrictions or limitations. Thus, a sanctuary from US cyber attacks, or ability to impose costs, is created by this kind of limitation on cyber weapons. Cyber weapons controls would be hard to enforce and regulation could be cost prohibitive. [34] On the positive side, it might give the US more diplomatic leverage to apply other means of power against those nations, rogue nations, or extremist movements who use the banned cyber attacks or weapons, as well as establish normative behavior defining what is acceptable and not acceptable. [34] Imposing costs and removing sanctuaries through international agreements are worthwhile pursuits that contribute to a cyberspace deterrence policy, but care must be taken that US cyberspace freedom of action is not unduly sacrificed in the process.

Objective: Deny Benefits

One way to deter an adversary who seeks to conduct behaviors unacceptable to the United States is to deny them the benefit of their actions. A prime example of this is the way that the US military deters adversaries from using chemical weapons during a conflict. The US military equips its forces with gas masks and protective clothing. It trains its members to carry out their missions despite the use of chemical weapons on the battlefield. Like me, every fighter pilot has an orientation flight flown in chemical protective garb to demonstrate to an enemy one thing- your use of chemical weapons on the battlefield will not achieve your desired result. Sucking rubber may make it more inconvenient for me to conduct my mission, but it will not keep me from accomplishing my mission. The adversary is deterred from using chemical weapons because the reward they seek is denied. Paralleling the military's preparation for the use of chemical weapons on the battlefield, US cyberspace deterrence strategies must also seek to deny the adversary benefit from their attacks on the US critical infrastructure.

Detect and Preempt

> *Depriving Americans of electricity, communications, and financial services may not be enough to provide the margin of victory in a conflict, but it could damage our ability to respond and our will to resist. We should expect that exploiting vulnerabilities in cyber infrastructure will be part of any future conflict.*
> - Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency [5]

As an example, the Deterrence Operations JOC offers one objective, or way, to deter an adversary: "Preparation for attack seen as likely to be detected, preempted by US." This detection and preemption of an attack deters an adversary because the benefit

of conducting the attack is denied by preemption. This is one area where the realities of the physical world and the characteristics of cyberspace differ enough as to make this way of implementing deterrence strategy ineffective.

In the physical world, there are tell-tale indicators of when an adversary launches a missile potentially carrying a nuclear warhead. The US has built an entire system around detecting ballistic missile launches. Satellites that look for plumes, systems which analyze missile trajectories to differentiate between space launches and attacks, command and control structures to rapidly process the information and communicate orders. Depending on where the missile was launched from, decision makers have roughly 20 -30 minutes to decide what to do and whether to launch a retaliatory strike. [35 p. 16] This is probably one of the most time restricted attack scenarios in the physical domain. Other types of attacks, like a WMD attack by a rogue state or organization, would also have many indicators which would enable one to implement a "detect and preempt" strategy, thus contributing to strategic deterrence.

As described earlier in this research, attacks conducted in cyberspace do not suffer the same frictions based upon time and space as physical domain attacks do. This means the warning time necessary to "detect and preempt" is reduced for several reasons. Take for example an internet based attack on US critical infrastructure. Is that bit entering your network a "good" bit or an "evil" bit? If it is an "evil" bit, the warning time is in effect- zero. The attack is in progress.

If people rode rockets instead of airplanes to go between Moscow, Russia and New York City, USA this would significantly complicate the process of evaluating when

an attack via nuclear armed missiles was in progress. The sheer number of bits flying across the internet makes discrimination between legitimate traffic and an adversary's attack difficult. The same types of things that are done to conduct espionage in the cyberspace domain are the same things that are done in attacking the system: scanning, gaining access, gaining control of processes, and leaving a backdoor for future access. Discriminating between espionage and an attack is difficult. This is compounded by the fact that today's espionage could easily provide the access for tomorrow's attack. The fact that you can't portend the purpose of a bit until it arrives seems to nullify the "detect and preempt" strategy entirely.

General Kevin P. Chilton, Commander USSTRATCOM has an answer to this problem with "detect and preempt". He stated at the USSTRATCOM Cyberspace Symposium in April 2009:

> But you know, at the end of the day I believe we ultimately have to be even faster than network speed if we're going to defend this network appropriately. How do you do that? I'm not defying the laws of physics here. You do it by focused high-tech intelligence. You do it by focused high-tech intelligence, focused all-source intelligence, that [sic] tries to get you out and anticipate threats before they arrive. You have to be able to anticipate them and when you can preempt those threats and preempt those attacks before they arrive at your base, post, camp or station, or at your laptop on your desk. [36]

In General Chilton's view we get around the inherent characteristics of cyberspace through our intelligence- our ability to predict or anticipate threats. The implication of this statement is that our intelligence agents are pre-positioned in the adversaries' systems to such a degree that they can provide intelligence that allows preemption. This puts a

“detect and preempt” strategy back into play as a viable means to deny benefit to an adversary attempting to conduct an attack against the critical infrastructure of the United States. In fact, it allows the United States to deny benefit across a variety of cyber goals (ends) including preempting attacks on the US critical infrastructure or government.

The downsides to this strategy are two-fold. First, the US capability must be credible, if not demonstrated, for an adversary to be deterred by “detect and preempt”. How far does the US go to reveal the information discovered in its detection and or preemptive operations without revealing the sources of that information? This struggle is not unique to cyber intelligence, but the ends of intelligence may conflict with the ends of detecting and preempting adversary cyber attacks as part of a cyberspace deterrence policy.

The second downside is the question of cyber egalitarianism. Is it reasonable to maintain an obtrusive intelligence presence, one that might be construed as an attack in and of itself, in an adversary’s systems and not expect the adversary to attempt the same amount of surveillance in US systems? The very character of cyberspace, which is that attacks are difficult to discriminate and detect, drives us to “attack” adversary systems to gain intelligence in order to pursue a “detect and preempt” strategy of deterrence. Further, preemption in the form of a cyber response requires long scanning and planning times. It requires maintaining an unauthorized presence on the adversary’s systems. Having an expectation that an adversary will refrain from obtaining the same intelligence and presence on US systems is philosophically hypocritical and not practical to implement. However, it might be possible to engage some of the most capable cyber

nations to establish out-of-bounds areas- like critical infrastructure such as electric plants and water treatment facilities. This would allow the United States and cyber adversaries to pursue "detect and preempt" in other cyber venues such as government, military and intelligence circles. Where this strategy might hold greater promise, without as exposing the United States to as great a risk of retribution is in dealing with extremists who wish to do the Unites States harm. By applying this strategy to extremists or terrorists, illegitimate by definition, you do not run the risk of condoning cyber attacks/intrusions to prevent cyber attacks. Careful consideration must be given as to where the extremists host their illicit cyber activities and the means taken to preempt their activity. The intelligence gathering and preemption of cyber activities when hosted on legitimate commercial services or within the borders of our own country, or other friendly nations, significantly complicates "Detect and Preempt". This leads to clandestine operations, which greatly reduces the deterrent effect of "Detect and Preempt". If an extremist, planning an attack on the United States' critical infrastructure, suddenly has the blue-screen-of-death on his computer, he may believe it is a computer glitch, or operating system problem. This doesn't deter him in the same way as knowing the US is onto him and pursuing him in order to preempt his attack. At the same time, limitations in law, policy and geography must not be allowed to create sanctuary for the cyber adversary.

"Detect and Preempt" as a deterrence strategy in the cyberspace domain has limitations. Some leadership see this as a viable strategy in cyberspace due to focused high-tech intelligence. In order to be successful, this strategy relies upon intrusive intelligence gathering for detection; and it relies upon the ability to impose cost, or hold at risk those systems and individuals which might perpetrate an attack. It has the

drawback of actually condoning some types of cyber attacks in order to detect and preempt others. While "detect and preempt" may be necessary to safeguard the nation's security, it may not effectively contribute to cyberspace deterrence.

Strategic Deterrence in a contested environment

> *Cyber superiority ensures freedom of action in all domains (and denies freedom of action to adversaries) … predicate to all military and national security ops*
> – Lieutenant General Robert Elder, Commander, 8AF [37]

If cyber superiority was easily gained, then there would be little need for the military to deter an adversary from conducting attacks against the US or its critical infrastructure. In Operation Desert Storm, the Iraqi Air Force flew 122 aircraft to Iran to avoid destruction by the United States. [38] If those 122 aircraft were all that composed the Iraqi air defense, then air superiority would have been easy. . The coalition led by the United States actually had lost 37 fixed wing aircraft and 5 helicopters. [39] Air superiority had to be established by different degrees in different areas. JP 1-02 defines air, space and information superiority as

> **air superiority —** That **degree** of dominance in the air battle of one force over another that permits the conduct of operations by the former and its related land, sea, and air forces at a given time and place without **prohibitive** interference by the opposing force. [40]
>
> **space superiority —** The **degree** of dominance in space of one force over another that permits the conduct of operations by the former and its related land, maritime, air, space, and special operations forces at a given time and place without **prohibitive** interference by the opposing force. [40]
>
> **information superiority —** The operational advantage derived from the ability to collect, process, and disseminate an **uninterrupted** flow of

> information while exploiting or denying an adversary's ability to do the same. [40]

While there is no joint definition of cyber superiority, 8th Air Force defines cyber superiority as: "the freedom to operate in the cyber domain while denying that same freedom to an adversary." [41]

Like flying their aircraft away to Iran, if all cyber adversaries could be frightened from attacking the US or defending their cyber territory, then establishing cyber superiority would be a relatively easy matter. The difference in terminology of information superiority (one part of cyber superiority) and air or space superiority hints at one of the false notions of cyber superiority. Information superiority has an "**uninterrupted**" flow of information. Air and space superiority have a "**degree**" of dominance, and no "**prohibitive**" interference. A potential misunderstanding of cyber superiority is that adversaries will be denied success as they attempt to degrade, deny, disrupt, or damaging our cyber systems or dependence on those systems. The 8th AF definition of cyber superiority is open to this incorrect interpretation The January 2009 DOD Quadrennial Roles and Missions Review Report states that the vision of the DOD is "to achieve superiority in military-relevant portions of cyberspace." [42] Even allowing for the fact that one could determine the military-relevant portions of cyberspace and the non-military-relevant portions, achieving superiority will be difficult due to the strategic fragility of cyberspace and the US reliance upon cyberspace. The US cannot assume complete cyber superiority will be had or maintained in a military campaign, or when its critical infrastructure is under attack, and must plan for operations which contend over cyberspace. Cyber plans must not only be composed of cyber actions and responses.

Options across the full Range of Military Operations and the DIME must be developed and considered. US government responses to cyber attack should include asymmetric responses (ie non-cyberspace related). The US government should plan to use kinetic responses to a cyber attack.

As General Chilton reported to Congress:

> It's not necessarily linked that if there's a cyber-threat, that you have to have a capability in cyberspace to deter somebody, or if there's a space problem, that it has to be a space capability that deters them, or conventional, either. I mean, you can go cross-domain and cross-areas and draw the lines in different areas. It could be an economic deterrence: "If you do this, then you will suffer these economic or diplomatic penalties." That can be part of a deterrent strategy as well. There's just lots of elements that you can bring to bear in the quiver here. [16]

Preparing for this fight- the contention of cyberspace, has deterrence implications, and provides one of the strongest means of denying benefit to the adversary. The US, especially its military, must have the ability to fight through a cyber attack. To deny benefit to an adversary, the US must demonstrate the ability to establish cyber superiority more in line with the “degree of dominance” concept of air or space superiority. Moreover, they must show the capacity to carry the fight to the adversary without cyber superiority. By proving the ability to operate without complete dependency upon the cyberspace domain, an adversary is convinced not to conduct an attack against the United States’ critical infrastructure. This is because the desired benefit of incapacitating the US, or its military, is denied to the adversary.

Illustration from space

There is a growing common ground between space and cyberspace strategies. US military commanders are facing the fact that after 50 years of a clear space advantage, if not outright space superiority, their assumption of superiority is under attack. The US cannot rely upon space superiority as a given. A new special area of emphasis, or SAE, titled "Space as a Contested Environment," was introduced by Admiral Mike Mullen, the chairman of the Joint Chiefs of Staff on March 30, 2009. Commenting on the new SAE, the director of Air University's National Space Studies Center, Colonel Sean D. McClung stated, "Many decades ago space was thought of as a sanctuary. We are entering into a new era where space is a contested environment." [43]

In many ways, space and cyberspace are on similar paths towards deterrence policies. First, according to Colonel McClung: “America’s way of life is dependent on space.” [43] The GAO’s report on Military Space Operations recognizes that space systems play an “increasingly important role in DOD’s overall warfighting capability as well as the economy and the nation’s critical infrastructure.” [44 p. 14] In fact, “This growing dependence, however, is also making commercial and military space systems attractive targets for adversarial attacks.” [44 p. 1] Attribution for space attacks and appropriate responses to a space attack are also key considerations of space deterrence policy. Space assets are vulnerable to a variety of attack vectors, varying from electronic jamming and dazzling, to debris fields that cause collisions The greatest difference between the challenges facing planners in the space and cyberspace domains comes in the form of the cost of entry. Costs include gaining the required technical expertise, the ability to command and control attacks, and the time to develop attack capabilities as well as the dollar costs to participate in the given domain. While barriers to entry in the form of

costs are traditionally higher in space as compared to cyberspace, the advent of cross-domain cyber attacks on space systems starts to change the equation. Space is ripe for cross-domain cyber attacks which interfere with or corrupt data as it is transmitted.

Another finding from the GAO report was that "The Space Commission recognized that stronger DOD-wide leadership and increased accountability were essential to developing a coherent space program" [44] This is why General Chilton emphasizes that a change in culture that holds people and commanders accountable for their activities in the cyberspace domain is so critical to US success in this domain. [36]

As the DOD and US leadership start to come to terms with a decreasing ability to maintain space superiority, the same leadership must recognize that cyber superiority has not been a given for a while, and any prediction for "uninterrupted" superiority is a chimera. Let me offer two illustrations of how space strategy is changing in face of this loss of superiority. These illustrations address a key deterrence issue and communicate strategically to our adversaries that attempts to attack our space systems will not result in the benefit they seek. These illustrations can then be used as a means of comparison to help formulate cyberspace deterrence policy.

Rapid Satellite development and launch

Part of US Strategic Command's Operationally Responsive Space (ORS) office at Kirtland Air Force Base, NM, is a new lab known as Rapid Response Space Center or the Chile Works. [45] The lab is not expected to be fully operational until 2015. It will use pre-built components- solar arrays, power sources, and control mechanisms to attach to payloads- imagery or data dissemination, in order to rapidly field a satellite to fill a gap in

days. This lab is a tier-2 ORS strategy. The ORS concept involves 3 tiers in order to meet JFC needs.

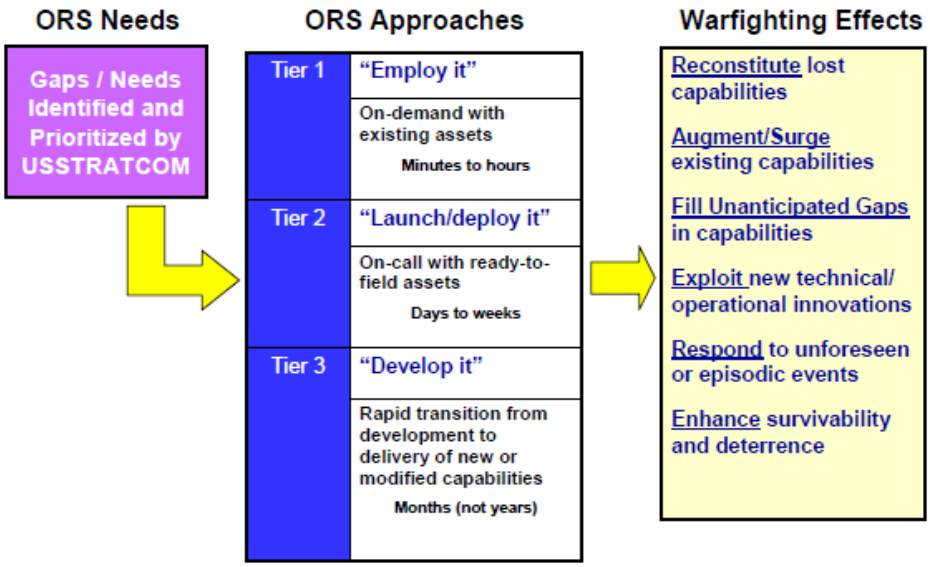


Figure 7- ORS Concept [46]

Conceptually, Tier 1 involves leveraging existing capabilities to meet a combatant commanders needs. An example might be re-tasking a remote sensing satellite to provide reconnaissance photos. [47] Tier 2 involves replacing a damaged satellite or providing capability via small launchers within weeks. Tier 3 is predicated on deploying a new satellite to fill a capability gap within one year. [47] STRATCOM will help to identify gaps and needs in the space structure and prioritize COCOM requests for space capabilities.

Developing the ORS office to develop contingency plans that help the US contest over the space domain have some effect over adversary decision making. But concrete examples, such as building and funding a project like the Chile works contribute to the adversary perception that the US is serious about space operations and mission success.

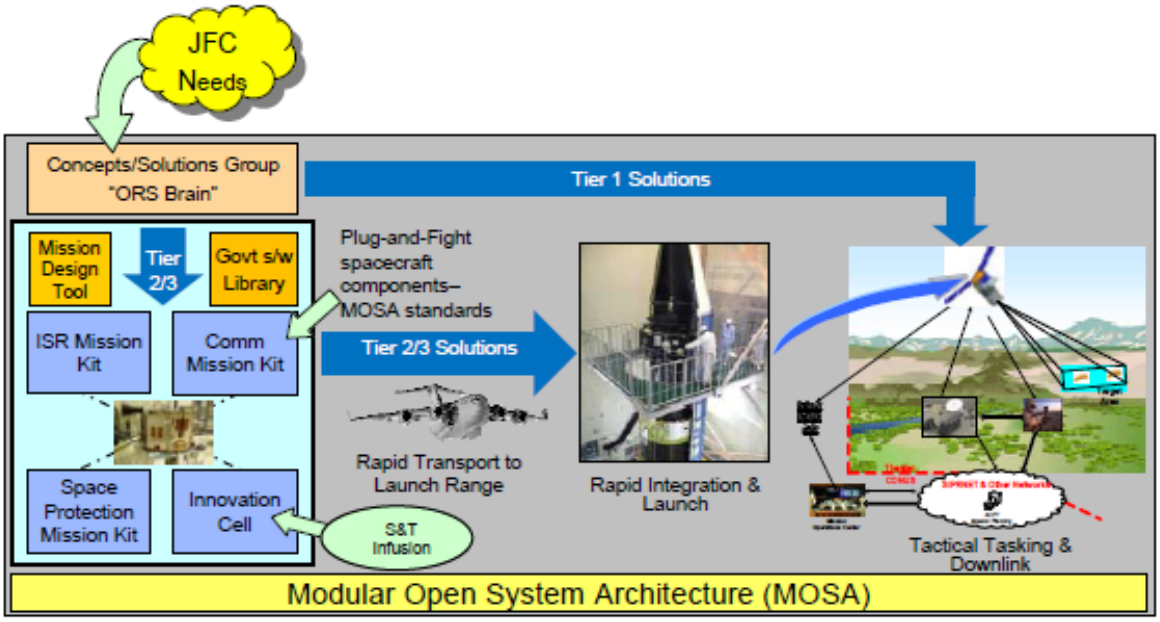


Figure 8- Implementation of the ORS Concept [46]

Rapid Satellite development and launch capability communicates to our adversary that despite their efforts to destroy or degrade our space capabilities, we have the resolve, and ability to replace those space assets. The adversary calculation is influenced by the fact that any satellite destruction will not achieve their desired ends. This impacts their decision to even attempt to destroy or degrade the satellite in the first place. It might even influence their desire to pursue a destructive anti-satellite program. If the enemy doesn't develop anti-satellite capabilities, could you attribute it to this practical implementation of deterrence policy? Not necessarily. This is one of the characteristics of a wicked problem- "there is no immediate and no ultimate test of a solution to a wicked problem." [48] Just because it is wickedly difficult to solve a problem like deterrence doesn't mean the steps that are taken to approach a solution are not worth doing. Ultimately with an

open-ended issue like deterrence, one must decide how much energy or effort can be afforded to be dedicated to its solution.

GPS

Much research goes on to develop navigation systems that are not dependant on GPS. This is important to demonstrate to our adversaries that the denial of GPS will not have the desired effect of stopping our military capability to wage war. In, fact it might have the consequence of making our attacks less precise. For example, if GPS guided munitions were not able to be used, it might result in the use of more dumb bombs. A GPS denied environment would not have affect on our will to conduct attacks, but might just change the means by which those attacks are prosecuted. This in turn might threaten greater damage to enemy civilians and infrastructure, as the result of the enemy leadership decision to deny GPS. This decision then reflects the enemy leadership decision to place more of their populace and infrastructure in peril, without gaining substantial advantage. Not a logical course of action, unless you thought that the US could not operate in a GPS-denied environment. Thus, the United States military must demonstrate its ability to deny this logic to the enemy. It does this by training without GPS and demonstrating its ability to "fight-through" a GPS denied environment. It also does not put all weapons and weapons systems into the GPS guidance basket. It must continue to work on developing the navigation technologies to operate without GPS and develop plans that assume no space superiority as the baseline position. By these means, the enemy's calculations on the advantages gained by denying GPS use to the US will be frustrated.

Creating Cyberspace Response Capabilities

What is the cyberspace equivalent of the Operationally Responsive Space (ORS) office? There is no direct corollary, but the cyberspace domain lends itself to several parallels.

Continuity of Operations (COOP) plans facilitate the ability to fight through an attack. As perfect copies of information can be created and hosted on servers anywhere around the globe, cyberspace's unique benefits are clearly evident. Most military organizations have some sort of plan to back-up information and can revert to this information in case of an attack or compromise. Perhaps not as well planned for are large-scale disasters like Hurricane Katrina which ripped through the southern US in 2005. Were there geographically separated copies of the most critical mission information stored across the US? Not every potential risk can be foreseen, but as planners anticipate the likely outcomes of contesting over the cyberspace domain, they must be ready with contingency plans to deal with potential attacks. Developing strategies and plans that span disaster and attack recovery will entail breaking down complex systems and understanding cyberspace interdependencies. In addition, these plans should be practiced, exercised and updated frequently. COOP contributes to cyberspace deterrence by allowing the US to continue operations and missions in the face of opposition, thus frustrating the adversary's attack and calling into question his judgment for the initiation of the attack.

The report from the CSIS Commission on Cybersecurity for the 44th Presidency summarizes the philosophy of COOP: "We will never be fully secure in cyberspace, but much can be done to reduce risk, increase resiliency, and gain new strengths." [5]

Cyber Superiority denies adversary benefit

General Kevin Chilton said "I think the most difficult challenge that we have today will be the challenge of continuing to operate our networks when we come under attack." [36]

The assumption of leaders, planners and warfighters needs to be opposition in cyberspace not complete domination. This fundamentally alters how the United States organizes, trains, and equips its forces and how the US fights its wars and battles. There are implications for both services who organize, train and equip, and COCOMS who lead the fight. If the adversary believes that there is advantage to conducting cyber attacks against the US, they will attempt to use this asymmetric means to offset our clear military advantages. These cyber attacks could be very wide-spread, attacking large segments of the civilian and the nation's critical infrastructure. The ability to fight through the attack communicates to the adversary that your actions in cyberspace will not lead to significant advantage. This serves as a deterrent to wide-spread cyber attack. How can you communicate this message? You have to prove it. Prove it through training, education, and technology that permits one to conduct the fight without cyber superiority. You prove it by exercising without the advantage of cyberspace. For the Air Force, this means that missions can be planned without flight planning software. Aircraft are generated without the advantages of cyberspace. Sorties are launched from airfields without computer support. Missions are flown and executed without turning on GPS for the entire mission. The command and control of aircraft is conducted with degraded or turned off computer systems. Turn NIPR, SIPR or JWACS off and let the CAOC

practice its mission. If you don't believe that the US Air Force can complete its mission without one or all of these things, the enemy won't think so either. You make his decision calculus very easy- the advantage to deny the United States cyber superiority is so great- they will be immobilized, that the adversary can do nothing else but develop cyber attack capabilities and use them as widely and often as possible to deny the US cyber superiority.

Cyber Operations in a contested environment

> *"You can think about technical means to power through denial of service. But if they can get inside our heads by getting inside our machines and becoming us, the impact that they can have on military operations can be dramatic."*
> -General Kevin Chilton, Commander USSTRATCOM

One insidious problem when operating in a contested environment is not what the adversary can do to your physical and technical systems, though mitigating those effects is paramount; it is in how the adversary can affect the minds of your leadership and personnel. If the adversary can sow distrust in your information systems, the systems you rely upon to conduct operations, he can dramatically impact your operations. Imagine a cyber-savvy adversary capable of infiltrating an airborne network like link-16, who could generate false targets or direct weapons release on friendly aircraft. More realistically with today's capabilities, imagine an email from your commander directing you to do the opposite of what he told you in the staff meeting. Would you call to confirm his order, or trust the system we rely upon for communication every day? According to General Chilton, "As soon as you've created that cognitive doubt, one ounce of doubt, you begin to impact combat operations." [49] Obviously this has ramifications for the effectiveness

of cyberspace deterrence. We have grown to rely upon the fact that whatever the computer says is right. This is a problem that requires the US to invest more in good network hygiene, identifying critical mission areas, anticipating sophisticated attacks upon those areas, and practicing and training to fight-through such attacks. In contrast, this problem also provides an opportunity when seeking to impose cost or emphasize the benefits of restraint to an adversary. If an adversary has come to rely upon cyberspace this creates dependencies that the US can exploit- particularly with regard to leadership seams. As these seams are also vulnerable to attack in an adversary system, one benefit of an adversary's restraint in cyberspace is that the US does not corrupt the data in their systems. The US would refrain from changing orders from leadership to followers as a consequence of adversary restraint. Holding as adversary's information at risk provides serious incentive to refrain from conducting attacks against the United States.

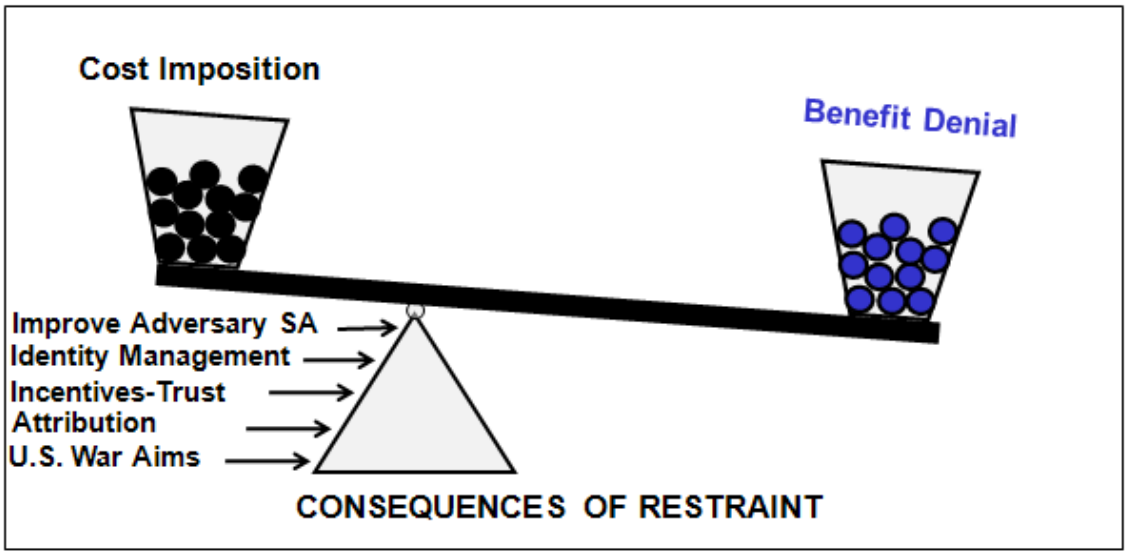


Figure 9- Influencing the Cyberspace "COR" Fulcrum

Objective: Encourage Restraint

Ways and Means which move the "Consequences of Restraint" Fulcrum have the potential to enhance the effectiveness of imposing costs and denying benefits to an adversary. Tailoring cyberspace deterrence policies which capitalize on this advantage creates unique opportunities. Three potential ways to influence the "Consequences of Restraint" Fulcrum in cyberspace are: Attribution, Identity Management (IM) and moderating the trust relationships of cyberspace. Another method by which the "Consequences of Restraint" fulcrum can be influenced is by formulating military plans and operations with consideration for adversary cyber attack capabilities, much as we formulate plans with consideration for nuclear capable foes. With each of these influencing concepts, deterrence strategy can influence the consequences of restraint fulcrum positively or negatively.

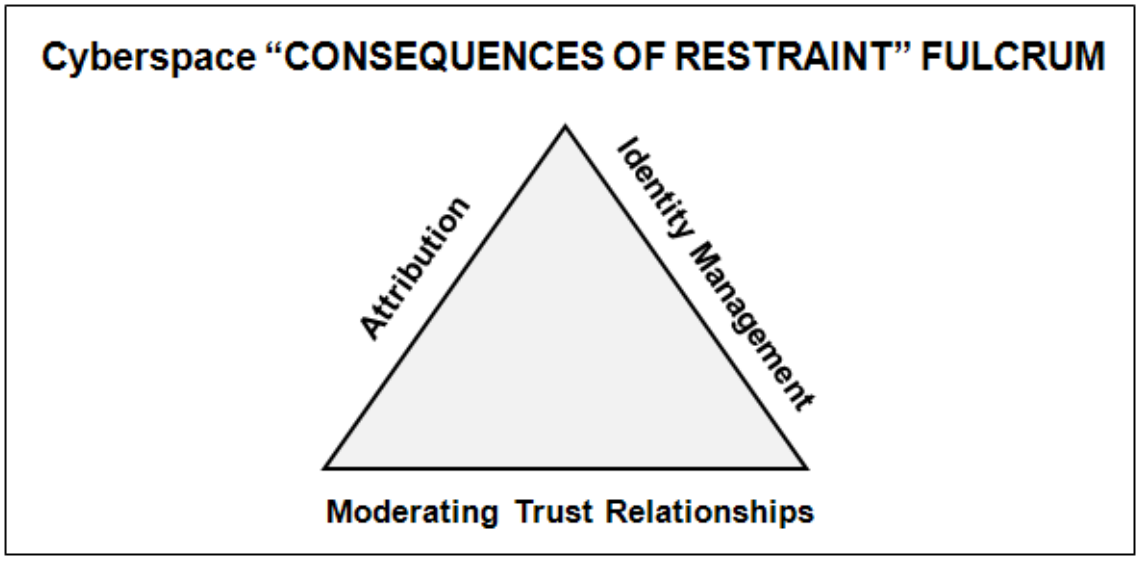


Figure 10- Cyberspace "COR" Fulcrum

Attribution

> *The most significant deterrence challenge posed by the threat of cyberspace attack is the perceived difficulty of attributing such attacks to a specific attacker, be it a state or nonstate actor.* –General Kevin Chilton and Greg Weaver [50]

Determining the source of a cyber attack is a difficult but not insurmountable obstacle. Attributing cyber attacks and intrusions to their source is critical to deterrence strategy. A working definition for attribution is "*determining the identity or location of an attacker or an attacker's intermediary*." [51] Cyber attribution is difficult for several reasons: it cannot be accomplished by purely technological means; cyber attacks cross jurisdictional boundaries and require trust and assistance to achieve attribution; the goal of open or anonymous communication across the internet is stymied by attribution. [52] Additionally, discerning the difference between a system failure and a cyber attack can be problematic. Attributing cyber attacks will require the development of procedures that are not currently in place.

First a requirement must be defined. Perhaps this requirement would be defined like: "Be able to identify the source of a cyber attack/intrusion within 10 minutes." (The number here is arbitrary, it could be 10 minutes or it could be 24 hours. It is based on what must be done with that information as input into the conflict planning and management process.)

Next the procedures to provide attribution must be developed. There are several alternatives to help provide attribution. In their research "Role and Challenges for Sufficient Cyber Attack Attribution," Dr Jeffrey Hunker, Bob Hutchinson and Jonathon

Margulies present nine techniques to help gain attribution.[12] These include techniques like Hash-based IP traceback or Hacking back.

Table 3- Technical Attribution Approaches [52]

Technique	Description
Hash based IP traceback	Routers store a hash (relatively unique, compressed representation created by a one-way function) of each packet across the network; attribution is done by tracing back the hash across network routers.
Ingress filtering	Require that all messages entering a network have a source address in a valid range for that network entry point. This limits the range of possible attack sources.
ICMP return to sender	Reject all packets destined for the victim; return rejected packers to their senders.
Overlay network for IP traceback	An overlay network links all ISP edge routers to a central tracking router; hop-by-hop approaches are used to find the source.
Generating trace packets using control messages (e.g., iTrace)	Periodically (e.g., 1 in 20,000 packets) a router sends an ICMP traceback message to the same destination address as the sample packet. The destination (or designated monitor) collects and correlates the tracking information.
Probabilistic packet marking	A router randomly determines whether it should embed information about the message's route into a given message. The defender can then use a set of messages to determine the route.
Hackback	Insert querying functionality into a host, specifically without the permission of the owner. If an attacker controls the host, this may alert the attacker and make the information less reliable.
Honeypots	Decoy systems that are only accessed by attackers capture information for attribution.
Watermarking	A passive technique that brands a file as belonging to a rightful owner.

Each attribution technique has draw-backs and situations where it simply won't work. For example, in Hash-based IP traceback, it would be necessary to keep a log of every packet that passes through a particular node on the internet. In addition to requiring

[12] These techniques were adopted from seventeen techniques offered in the Institute for Defense Analysis by David A. Wheeler and Gregory N. Larsen. [51]

excessive amounts of storage space the logs would be a target to attackers trying to cover their tracks. [52] Hackback could involve breaking into a machine or series of machines to work one's way back to the source of the attack. [52] There are certainly legal ramifications to employing this technique. No one technique will work in every possible situation. Those pursuing a cyberspace deterrence strategy will need to have the ability to use a variety of techniques, or combination of techniques, to determine attribution. Determining attribution will shift the "consequences of restraint" fulcrum point away from imposing costs, making cost imposition easier and more effective.

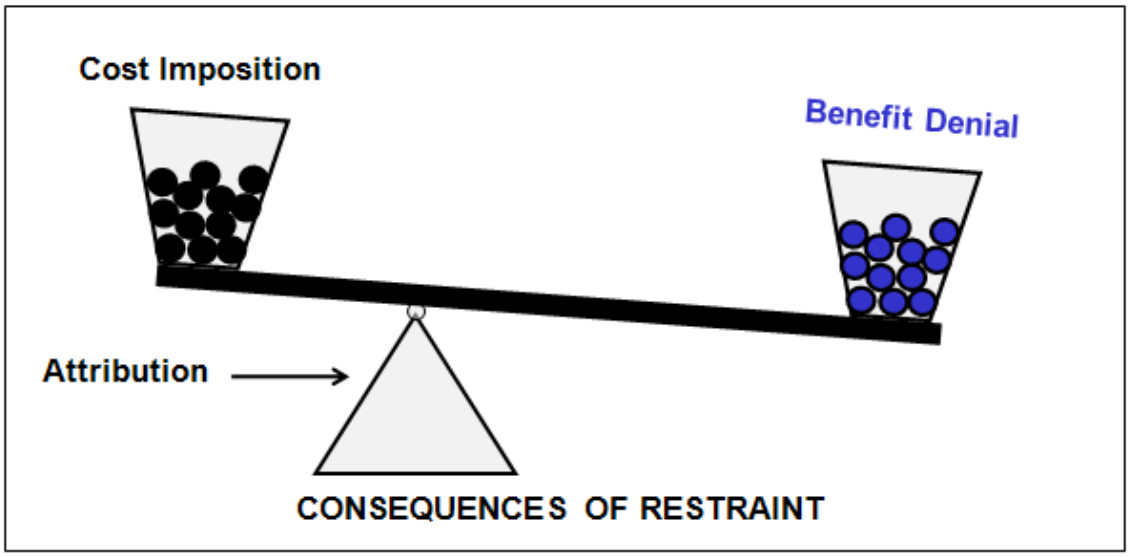


Figure 11- Attribution's effect on the "COR" fulcrum

For ease of examination we will look at the scenario of an attack that takes place through the internet. As cyberspace encompasses systems beyond the internet, planning consideration must be given to other cyberspace information systems that are vulnerable to adversary attack or exploitation. Most attacks on the United States critical infrastructure and military infrastructure performed through the internet will have to

transit some portion of the domestic cyberspace infrastructure. Interagency coordination and civilian ISP cooperation is critical. Some might argue that an adversary will just try to obscure the source of an attack by spoofing their address. Just because one spoofs their IP address, it does not mean that the attack cannot be traced.

According to the CISCO technical notes:

> The only reliable way to identify the source of an attack is to trace it back hop-by-hop through the network. This process involves the reconfiguration of routers and the examination of log information. Cooperation by all network operators along the path from the attacker to the victim is required. Securing that cooperation usually requires the involvement of law enforcement agencies, who [sic] must also be involved if any action is to be taken against the attacker. [53]

This is a slow and manual process, which could be complicated by a variety of factors including: multiple sources of spoofed packets, crossing jurisdictions/ national boundaries and reliance on upstream router personnel. [54] Obviously this drives the necessity of procedures which are exercised regularly and creates a requirement for legally mandated assistance to the government. The government cannot rely upon the patriotism or goodwill of commercial industry to aid in attribution, for there is little cost incentive for commercial industry to do so. Because the government receives hundreds of attacks per day [55], it would pose a strain to implement attribution standards without driving the development of tools that move the manual process of attribution to a more manageable procedure. This is necessary because today's probe, could be tomorrow's attack vector. Attribution is hard. But the hundreds of "attacks" the United States

receives everyday provide ample opportunity to practice the attribution techniques and procedures and overcome policy inertia. Attribution is a key component in assessing the effectiveness of a cyberspace deterrence policy, focusing that policy on specific actors, and imposing appropriate costs.

Encouraging Restraint through Identity Management and Trust

> *The experience of the Department of Defense was that intrusion into DOD networks fell by more than fifty percent when it implemented Common Access Card (CAC)"*
> - Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency [5]

Trust is fundamental to the successful operation of a decentralized system, such as that composed by the internet in the cyberspace domain. The US government and military, largely hierarchically-organized and centralized, struggle to bring order to the seeming chaos of the decentralized wilds of the cyberspace domain. This struggle reveals itself best in statements like General Chilton's when he says:

> Every Soldier, Sailor, Airman, Marine in the military is on the front line of cyber warfare every day. If you think about the guards who guard your bases, who stand there at the gate and make sure only the right people come in and keep the wrong people out -- that's everybody who has a computer on their desk in these domains today. They are part of the front line of defense and in fact they're engaged in cyber operations that matter every day, whether they know it or not. [36]

The gate guard is specialized in his task- he guards gates. This is how a centralized system works. Some parts of the organization focus on guarding gates, others focus on personnel issues, others operate airplanes or tanks. By specializing, the centralized organization can achieve great synergies, but if one section is removed (for instance the pilots that fly the planes) then the organization falters in its purposes and missions. In a

decentralized system- no one is in charge. Everyone bears some responsibility for the success or failure of the mission, but cutting off one person will not bring mission failure. Others will step in to fulfill the missing person's responsibilities. Thus, when General Chilton argues that every Soldier, Sailor, Airman and Marine is responsible for cyber warfare he is applying a decentralized paradigm to a centralized organization. This paradigm is a definite shift in perspective for how things have been traditionally done in the military. Accomplishing this blending of decentralized and centralized is going to require what General Chilton terms a change in culture. If the military is to organize and fight network centered warfare and develop network centered deterrence strategies, they are going to have to be prepared for a change in culture. In order to construct a hybridized system, combining decentralized and centralized elements, the US will have to feel out its way forward. Sometimes going forward will mean modifying centralized concepts to fit a decentralized system. Other times it will mean abandoning an centralized concept to accept a decentralized way of doing things. This will be the hardest for the US military to adapt to. One example is that the US military will need to be able to accept that the answers to some questions in a decentralized system are unknowable.

For instance when General Chilton asked how many computers were on the DoD network it took over 45 days to get the answer, an answer he wasn't even sure was right. This problem is only going to multiply as IPv6 comes on-line and more and more devices are networked. General Chilton would like to apply a centralized system approach- accounting for equipment, to a decentralized system. His vision is that just as we have 100% accountability for how many M-16 rifles are in the army, we should have 100%

accountability for how many devices are connected to a network. [36] It may be possible for the military to create a hybrid system of centralized and decentralized as it approaches warfare and deterrence in the cyber domain, but perhaps it would be better to focus on not trying to answer questions that are ultimately unknowable. If you can't count and account for everything that is hooked up to your network, then other approaches to securing the network must be explored. Exploiting the characteristics of a decentralized system will be pivotal in developing concepts that will help secure it. Two concepts that have implications for fighting in cyberspace and worth building deterrence strategy around are attribution and trust. These concepts are bridged by a third concept- Identity Management (IM). IM isn't the only bridging concept, but it holds great potential for helping to secure cyberspace and contribute to deterrence policy.

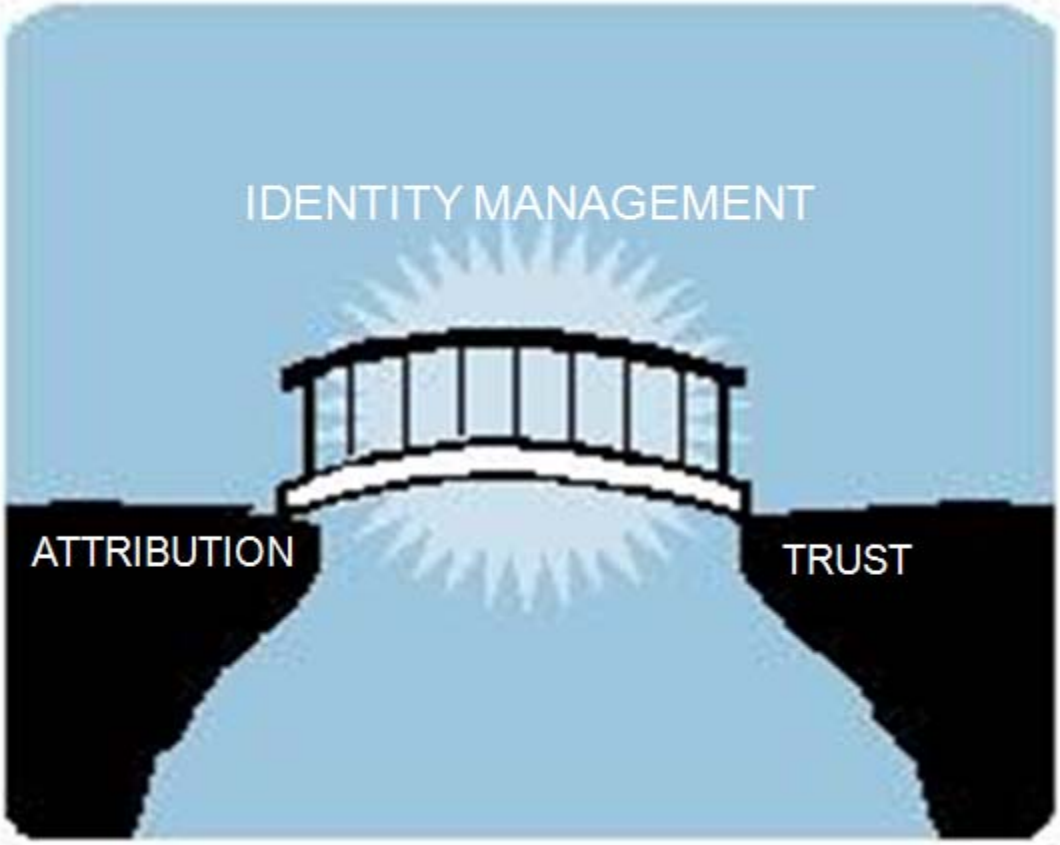


Figure 12- Identity Management Bridge

As the CSIS Commission on Cybersecurity for the 44th Presidency indicated intrusion into DoD networks fell 50% with the introduction of the Common Access Card (CAC). General Chilton also recognized the importance of identification management when he spoke in 2008:

> Identification management is very critical to defending our networks. The CAC PKI card was an important first step and we need to do more than that. Knowing who is on our network at all times and knowing what and what machines are on our networks are vitally important to the way that we move forward to defend it. [49]

In fact, identity management seemed like such a good idea that the Bush administration mandated it in Homeland Security Presidential Directive 12 (HSPD-12).

HSPD-12 mandated that the US government would implement a common identification standard. The DoD started the adoption of the CAC in 1999 and in 2007 over 13 million cards had been issued. [56] Unfortunately, the rest of the government is having difficulty keeping up with HSPD-12 instructions and deadlines. Background checks for federal government employees with less than 15 years of service and new identity cards with fingerprint data were to be completed by 27 October, 2007. No agency met the deadline. [56] In an attempt to push the agencies to compliance, the Office of Management and Budget started to require quarterly progress reports. As of October of 2008, only 29% of employees and contractors (1,593,191) had received their new identification cards. [57] "By leveraging the capabilities of HSPD-12 identity credentials, agencies can achieve greatly enhanced physical and cybersecurity while obtaining the benefits of government-wide interoperability," stated Karen Evans the Administrator of the Office of Electronic Government and Information Technology at the Office of Management and Budget. [57]

Identity management will be of greater and greater importance in the future. In a way, identity management allows for some degree of understanding an individual's documented attributes. IM is normally issued by a government agency and documents certain attributes of an individual- their age, eye color, membership in the DoD. The government agency is responsible for ensuring you are you- normally through a birth certificate and social security number (which is based upon a birth certificate). Thus the government agency is affirming that the attributes listed can be trusted. At its heart, identity management is fundamentally about linking attribution and trust.

Identity management will be of greater and greater importance in the future. Microsoft will introduce in 2010 the Lifecycle Manager "2" to replace their Microsoft Identity Lifecycle Manager (ILM) 2007. Microsoft's vision is to provide a way in which people can collaborate within the bounds of internal and external regulations, business policy and process, and security. In a way, identity management allows for some degree of attribution. But as the goals of the Microsoft project indicate, what is at the heart of identity management is trust.

Who do you trust to have access to your information? Who do you trust to join your network? Have the systems they are using implemented the correct patches and security updates? Could you even tell if they hadn't? Decentralized systems, like those found in the cyberspace operate best when those who join are trusted. But cyber-adversaries seek to take advantage of trust and wreak havoc in those same systems. How can cyber adversaries be deterred from taking advantage of trust? Identity Management will be part of the solution as it reduces some of the anonymity currently found in cyberspace. IM attempts to confirm the identity of those you allow into your system by tying their virtual presence with their physical identity and attributes. Potential adversaries will have to overcome the hurdle of proving they have the required attribute, membership in the DoD circle of trust for example, in order to gain access to systems. Another potential concept which will contribute to deterrence in cyberspace involves moderating trust relationships. Those who seek to do harm in the man-made environment of the cyberspace, can be disconnected. A break in trust can result in shutting out or disallowing the cyber adversary access.

Broken Trust

If an individual was to misuse their permissions in a DoD computer system, the DoD could revoke their privileges. If that individual's CAC was somehow compromised by an adversary that CAC's privileges could be revoked and the card replaced. But moderating trust relationships holds promise for application of cyberspace deterrence strategy in potentially greater ways.

In November of 2008, a US based web hosting firm that was accused of being responsible for more than 75% of the junk email sent out across the globe was disconnected. [58] McColo, whose servers were located in San Jose, California was effectively blacklisted out of service.

Known as "peering," Internet Service Providers (ISPs) connect with each other to exchange Internet traffic. [59] Several computer security researchers were able to detail how McColo contributed to cybercrime and spam. They convinced those with whom McColo connected to "de-peer" the company. This meant that the 40 websites that hosted child pornography were simply disconnected from the rest of the internet. [59] Botnet masters, whose command and control servers were hosted from McColo, no longer had control of their legions or computers. Spam decreased 50-80 % overnight. This is a powerful idea that can contribute greatly to deterrence.

What is interesting about this scenario is that it wasn't the government who forced McColo out of business. It was a conglomeration of people that formed with a common interest- to protect the internet community. It was a call to responsibility for the "Internet community [to] act in accordance with the ACM (Association of Computing Machinery)

code of ethics, e.g. avoiding harm to others." [60] Their philosophy is that it is the "Internet security community's responsibility to blow the whistle. While we do not take the actions to "stop" the cyber-criminals, we do urge those who provide connectivity or peering to consider this report and their role." This philosophy gets at the same change in culture that General Chilton spoke about- decentralized organizations/participants rallying around a common cause- in this case the proper and responsible use of the internet. Engendering support for cybersecurity from all participants in cyberspace will require a shift in the way the military educates and trains its personnel. Adapting the approach of the internet security researchers responsible for bringing down McColo may have even greater success in developing cyberspace deterrence strategy. When nation-states or adversary actors cannot be deterred from their undesirable activities in cyberspace, the US can work to convince others to disconnect the adversary from the system.

This powerful idea can be instrumental in shifting the "consequences of restraint" fulcrum. Nation-States who participate in upholding the standards and laws of right conduct in cyberspace will be granted access- they will be trusted. Those who assist in attribution and in identifying criminal and war behaviors will be rewarded with continued connectivity, maybe even favored connectivity. Adversaries who do not observe the norms and rules of the cyber community will be disconnected. All participants will have a responsibility to monitor the community and enforce the rules. It is incumbent upon the United States to participate in the decisions that are made across the globe as norms and practices are established. The US must provide leadership by example in this area to gain success.

US military contributions to encouraging adversary restraint

> *We are pursuing a future force that will provide tailored deterrence of both state and non-state threats (including WMD employment, terrorist attacks in the physical and information domains, and opportunistic aggression) while assuring allies and dissuading potential competitors.*
> -2006 National Security Strategy [61]

Updating JOPES

The joint operational planning process used by the DOD, the Joint Operation Planning and Execution System (JOPES) is sufficient and robust enough to account for this new domain: cyberspace. Certainly, some terminology must be agreed upon, and some new processes, plans and cyber-doctrine must be coordinated, but the JOPES planning process is robust enough to handle planning for cyberspace operations. In fact, JOPES cyberspace planning implements deterrence in three ways. The first two are well supported, but the third requires an expansion of JOPES planning considerations.

First, STRATCOM, as part of the Unified Command Plan, organizes and plans for operations in cyberspace. They do this with a global perspective. They must also coordinate with the geographic commands to ensure the appropriate use and defense of cyberspace. They contribute to cyberspace deterrence planning through both a cyberspace specific plan and cyberspace planning in their deterrence plan. Hopefully, these two interrelated plans are complementary and synergistic in their effect and integration. They contribute to deterrence primarily through focused operations that impose cost to the adversary, and communications which seek to influence the adversary's leadership and decision making processes.

Second, planners must deal with the integration of all of those different service implementations of cyberspace technology. They must plan for and manage the man-made structure that creates cyberspace in the geographic commands. This is typically a "6" function. Who do you call when the computer won't work? The six. The implementation and management[13] of the infrastructure contributes to deterrence in the Responsive Infrastructure leg of the new triad. The cyberspace infrastructure which supports the US military makes the military more lethal and effective. The infrastructure is adaptable and can be configured to changing circumstances or mission requirements. It is robust in its implementation and resists the manipulations of the adversary. The capability of our cyberspace infrastructure, implemented through our joint planning process, gives our adversary pause when considering attacks through cyberspace.

The final way in which military planners might influence cyberspace deterrence is through the development and implementation of traditional military plans. The practical implementation of cyberspace deterrence strategy must be written into JOPES, so that planners consider the risks and inter-dependant nature of cyberspace. I would propose that cyberspace needs its own category in the plan development activities.

---

[13] Management functions or good "hygiene" practices might also be described as defense in many quarters. Things like ensuring compatibility of new software on the system, and patching computers with anti-virus updates. Practically speaking these are maintenance/hygiene issues and do not in and of themselves, compose an active defense as defined in *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms*.

Figure 13- JP 5-0 Plan Development Activities

A model for how cyberspace planning might be considered is found in nuclear planning. However, cyberspace planning must go beyond nuclear in some respects. For example, in plan or order development per CJCSM 3122.01 (JOPES) specific attention is paid to nuclear strike. JP 5-0 states:

> Commanders must assess the military as well as political impact a nuclear strike would have on their operations. Nuclear planning guidance issued at the CCDR level is based on national-level political considerations and is influenced by the military mission. Although USSTRATCOM conducts nuclear planning in coordination with the supported GCC and certain allied commanders, the supported commander does not effectively control the decision to use nuclear weapons. [62 pp. III-45]

Due to risks associated with cyber-escalation, commanders should assess the military, political, and economic impacts of a cyber strike against the adversary. JOPES should include a specific cyber planning considerations section modeled after the nuclear section. Cyber planning differs from nuclear, in that supported commanders may control

the decision to use cyber weapons against the adversary. This fundamentally alters the way a commander must view the use of cyber attacks against a cyber-capable foe. The supported commander must consider how to conduct cyberspace activities in such a way as to deter escalation and aggression from the adversary. A commander's planning is further altered just by facing a cyber-capable foe.

In seeking to prevent attacks against the critical infrastructure of the United States including the cyberspace infrastructure, a commander must analyze all military actions for the potential of spawning a critical attack against the homeland. If a given objective of a campaign against an adversary is regime change, the adversary leadership may be left with the belief that all cyber-restraint should be discarded. Our objectives might be tailored in such a way as to lead the adversary closer to using cyber attacks against the homeland or cyberspace infrastructure, not further away. It is then imperative that commanders consider the cyber capabilities of an adversary, or friendly third parties that the adversary may be aligned with, as they formulate their campaign objectives and choose courses of action (COAs).

PHASING MODEL					
SHAPE Phase 0	**DETER Phase I**	**SEIZE INITIATIVE Phase II**	**DOMINATE Phase III**	**STABILIZE Phase IV**	**ENABLE CIVIL AUTHORITY Phase V**
PREVENT PREPARE	CRISIS DEFINED	ASSURE FRIENDLY FREEDOM OF ACTION/ ACCESS THEATER INFRASTRUCTURE	ESTABLISH DOMINANT FORCE CAPABILITIES/ ACHIEVE FULL-SPECTRUM SUPERIORITY	ESTABLISH SECURITY RESTORE SERVICES	TRANSFER TO CIVIL AUTHORITY REDEPLOY

Figure 14- Phasing Model

Because cyberspace is a cross-cutting domain, it also cuts across every phase of a campaign. Cyberspace deterrence has a place in each phase of a campaign. Commanders must leverage other planning structures Many lessons can be learned from how the US implements deterrence of WMD attack against US forces and the homeland.

Planners must take into account the specific cyber capabilities of an adversary and account for the friendly cyber vulnerabilities and mission critical areas in each phase of a campaign. In reality, the US will always be conducting some form of cyberspace deterrence- whether in Phase 0- shaping operations including deterring aggression and promoting peace and stability, or Phase III- Dominating operations across a full spectrum of options. Cyberspace operations may need to be planned, organized and controlled in a more fluid fashion than the military is used to thinking. Depending on one's point of view, if what separates Phase I- Deter from Phase III- Dominate is the use of force, then cyberspace deterrence which imposes cost to the adversary could easily move from Phase I to Phase III and back again within a day. This fluidity points to the fact that we are in a continuous struggle in cyberspace. This is a struggle in which the control of cyberspace deterrence operations, spanning multiple phases of conflict, will be critical to success. If you, the reader, can conceptualize the imposition of cost as part of deterrence operations

in any phase of conflict, then this understanding will probably be of greater assistance to you as you come to think of cyberspace deterrence campaign organization.

Cyber adversaries not only conduct operations against the United States each day, they are actively preparing the future battlefield. Deterring cyber-aggression against the US military or US critical infrastructure is a monumental task if the adversary believes there is much to be gained by these attacks. The work of US deterrence strategy is to encourage restraint, thus making US cost imposition and denial of benefits more successful. Let me postulate a hypothetical scenario for you. As the United States is deploying its forces and building up combat strength somewhere in the world to take on an adversary, that adversary would likely look for ways in which they could disrupt the deployment of US forces.

> Adversaries also could use cyber attacks to attempt to slow or disrupt the mobilization, deployment, combat operations, or resupply of US military forces. Attacks on logistic and other defense networks would be likely to exploit heightened network vulnerabilities during US deployment operations, complicating US power projection in an era of decreasing permanent US military presence abroad. [63]

If the adversary perceived that the US had a weakness in terms of a dependency on cyberspace and the internet to conduct its deployment of troops and equipment, what would keep them from attacks on the internet or other US critical infrastructure? Cyberspace deterrence policy must address the fact that the benefits of this type of adversary action (disrupting the US ability to deploy or resupply its forces) are so great that encouraging restraint may be extremely difficult.

US military dependence on commercial infrastructure has made the commercial side of US society a viable military target to adversaries. Deterring aggression against

commercial companies or privately owned assets with arguments of discrimination and the rules of war will likely not be successful. A center of gravity for our military resides in the commercial companies and infrastructure upon which we rely. Adversaries recognize this center of gravity and prepare actively to contend against the US in cyberspace.

> China's ambitions extend to crippling an enemy's financial, military and communications capabilities early in a conflict, according to military documents and generals' speeches that are being analysed by US intelligence officials. Describing what is in effect a new arms race, a Pentagon assessment states that China's military regards offensive computer operations as "critical to seize the initiative" in the first stage of a war. [31]

Deterrence policy must enumerate the benefits of restraint so that adversaries are convinced that attacking US critical infrastructure is not in their best interests, even in a military conflict. US leadership must recognize the vulnerabilities associated within the modern communications infrastructure and when confronting a cyber-capable foe, be prepared to accept the risk of a possible attack against the critical infrastructure of the United States

IV. Key Policy Tradeoffs and Research Findings

Imposing Costs Risks Retribution

> *Robust information assurance and securing vital networks must be our first priority. Our people play an important role in preventing unauthorized access to the critical systems in cyberspace. The cyber security training provided to our service men and women, and the civilian and contractor workforce is inadequate and must be improved.*
> - Lieutenant General Keith Alexander, Commander Joint Functional Component Command for Network Warfare [64]

One of the key policy tradeoffs to implementing a cyberspace deterrence strategy is that by imposing cost the US might illicit an escalated response which it is unprepared to handle. By his own admission, Lt General Alexander acknowledges the inadequacy of cyber training. In fact, before the House Armed Services Committee- subcommittee on Terrorism, Unconventional Threats and Capabilities, he stated that there are "issues with training, equipping and tactics, techniques and procedure. I would like to say our networks are secure but that would not be correct." [19] Because US cyberspace systems are so vulnerable to counter-attack, this poses a unique deterrence challenge. How does one impose cost on an adversary to deter cyber-aggression when their own systems are so vulnerable to cyber attack or their people untrained to fight? Because the US is not prepared to be on the receiving end of a cyber-response, they are not yet ready to impose some costs on cyber actors. The fear is that imposing cyber costs on an adversary could escalate cyber attacks not deter them. This fear actually limits US freedom of action. If the US were ever to strike back (impose cost), despite greater capabilities, they would limit how hard they hit an adversary. This is because the US feels that its cyber hygiene (defense) is so poor that we could not withstand the counter-punch.

The risk of escalating cyber attacks must be faced and mitigated. Withholding imposition of cost in cyberspace only emboldens the cyber adversary, and invigorates his manipulation of cyberspace to his benefit. Deterrence policy that does not hold cyber actors accountable for their actions and impose cost is anemic and counterproductive. Like a three-legged stool, the "Defense" leg and "Responsive Infrastructure" Leg of the new deterrence triad uphold the "Strike" leg and enable effective cyberspace deterrence strategy. Taking inspiration from Arthur Lykke Jr.'s Ends-Ways-Means stool [65], the stool that supports cyberspace deterrence strategy will not be balanced without all three supporting deterrence categories as found in the new triad. Eliminating, or diminishing strike, from the equation results in an ineffective deterrence posture.

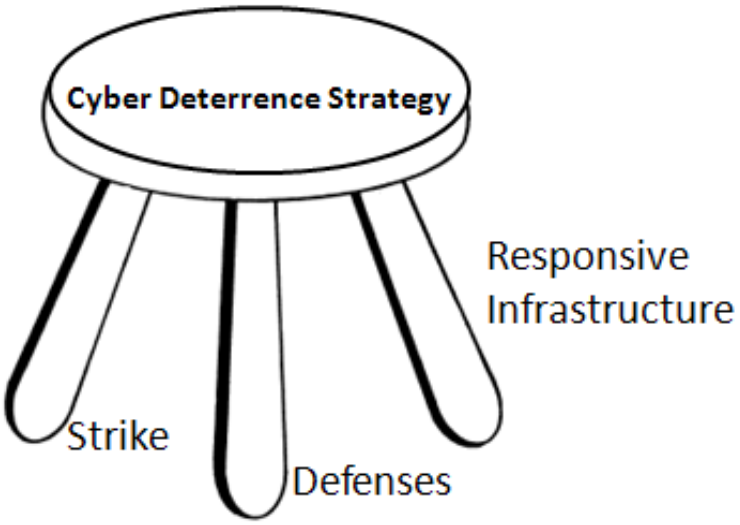


Figure 15- Cyberspace Deterrence Model

One possible way to mitigate this policy tradeoff is to impose asymmetric costs. In the instance that an attack against the US cyber infrastructure or an attack conducted

through cyberspace does take place, the US could impose costs through other channels such as economic or diplomatic. These costs then would seek to deny benefit or impose cost to the adversary leadership in another venue not associated with cyberspace. This venue might even be something that the adversary holds dearer than his own cyber infrastructure or those things reachable in cyberspace. It would serve as a means of imposing costs that might not lead to an escalation of retaliatory, or tit for tat, cyber attacks. Ultimately however, for cyberspace deterrence to work, cost imposition must also take place in domain of cyberspace. In order to communicate to a cyber adversary the value you place on the cyberspace and your willingness to defend in that domain, you must be willing to impose cost in cyberspace.

The day of full accountability and a fully prepared defense in the cyberspace is a long way off. Waiting until some nebulous decision point for the defense to be ready before you implement a cyberspace deterrence strategy that imposes costs will never come. Speaking about cyber security, Senate Commerce Committee Chairman John D. Rockefeller IV (D-W.Va.) stated: "It's not a problem that will ever be completely solved. You have to keep making higher walls." [66] Of course the walls are only one aspect that enables successful deterrence. “If we try to defend our networks like we do a castle, we will never be successful,” reported Lt General Alexander to Congress. “We have to defend it on the network globally. That also means we need an early warning system between networks automatic tipping and cueing at network speed to defeat future threats like some of the robot networks that are out there.” [19] Efforts to improve the security of the systems of cyberspace must be continued to enhance deterrence efforts, but the

imposition of cost upon the adversary should not be predicated upon implementation of better cybersecurity.

There is no historical track record to guide strategy developers on the application of imposing costs in cyberspace. The first application of cyberspace deterrence cost imposition is critical. The US has to get it right, because it will set a precedent and establish the root from which all other applications of cyberspace cost imposition springs. The application should be well documented and shared with the world so as to send a clear message where the US stands and what it is prepared to do to defend cyberspace.

Greater Freedom of Action Through Deterrence

> *Maintaining freedom of action in cyberspace in the 21st century is as inherent to US interests as freedom of the seas was in the 19th century, and access to air and space in the 20th century*
> Lieutenant General Keith Alexander, Commander Joint Functional Component Command for Network Warfare [67]

A key research finding is that the issuance of a declaratory cyberspace deterrence policy is the cornerstone for successful deterrence efforts. One of the key policy tradeoffs is that by announcing a cyberspace deterrence policy, this will restrict the United States' freedom of action or maneuver. No matter how carefully crafted a policy is to try ensure that the US is not restricted, some restrictions will inevitably result. But, is this any different than the ways in which US cyber policy is restricted today? The US restricts its application of cyber intelligence gathering based on law and geography. The Department of Defense pays considerable attention to the application of United States Code Title 50, Title 10 and Title 18 in order to ensure that activities conducted in cyberspace are consistent with the laws of the nation. The application of the laws and

principles of warfare, such as proportionality and discrimination, are debated and consensus is drawn as to what is appropriate application of power in cyberspace. In a democracy, true freedom of action never exists; it is always limited by what is allowed in society. In fact, establishing a declaratory cyberspace deterrence policy may actually increase the freedom to act. Major General William Lord, commander of the Air Force Cyber Command (provisional) noted that “It's easier for us to get approval to do a kinetic strike with a 2,000-pound bomb than it is for us to do a non-kinetic cyber activity." [68]

The US needs to take the lead, as in nuclear deterrence, to establish the standards of conduct for cyberspace. Despite imposing some limits to the United States’ freedom of action in cyberspace, establishing a cyberspace deterrence policy will provide greater benefit to the United States. These benefits include the ability to establish the standards of right conduct in cyberspace. Upholding these standards will give the US justification for imposing costs in cyberspace and provide rationalization to support those decisions. The benefit of reducing unwanted cyber adversary behavior is certainly worth the tradeoff to limiting freedom of action in cyberspace. For example, if the standard of conduct is that any break-in to a US critical infrastructure electrical system computer is deemed unacceptable, perhaps the US would be justified in hacking back to the adversary system. Perhaps this would even condone imposing cost in the form of destruction of adversary computers. The US would also be able to hold the leadership of the nation-state from where the attack came responsible for the preparation of an attack against the electrical grid. In this example, the restriction to the US freedom of action comes in the form that the US would not target enemy electrical systems with hostile programs or destruction. Vice Admiral Carl V. Mauney, Deputy Commander, USSTRATCOM is

correct when he says, “Cyberspace has become a warfighting domain like land, sea, air, space. And in light of growingly astute cyber enemies, it’s in our interest to maintain freedom of action,” [14] Almost counter-intuitively, increasing freedom of action may mean willing submission to some restrictions as laws and norms are applied to this new domain, because it removes fear of action and allows costs to be imposed in a cyberspace deterrence strategy.

In order to preserve as much freedom of action as possible, some ambiguity in the cyberspace deterrence must be communicated to the cyber adversary. Ambiguity preserves the ability of the US to impose cost, without unnecessarily limiting US options in cyberspace. It also helps to prevent against the tendency of an adversary to push up against red lines. In the air force, we draw red lines on the concrete around the aircraft parked on the ramp. If someone crosses that red line, the security police will most likely put that person face down on the concrete and detain that person until their identity and intentions are confirmed. Air Force bases use warning signs to indicate that deadly force is authorized on the base and in situations where “red lines” are crossed.

If clear red-lines are established in cyberspace, adversaries may attempt to exploit them by conducting actions that are just short of the red-line. They would try to get away with as much as possible. The risk is that the adversary may inadvertently cross a red-line when not intending, and thus risk an escalation or exchange. The other risk is in secret, or non-enunciated, red-lines. Some ambiguity is a good thing, but one of two things will happen. The adversary will keep probing and poking and conducting undesired cyber activities until something provokes a reaction- a cost is imposed. This

will cause them to stop and change their behavior. The other likelihood is that they will poke and probe until they map out all of the rules, or red-lines, and they stay away from those activities or are able to disguise those activities that the US deems undesirable. Opponents are savvy and have purpose behind their cyber activities. Although cost imposition is an important element of deterrence strategy, the US must provide a situation where restraint in cyberspace is encouraged and reaps acceptable benefit to an adversary. Simply imposing costs by breaking adversary computers or sending false information in adversary exploitation attempts will not necessarily be successful to deter unwanted behavior unless it is combined with attempts that reinforce the benefits of adversary restraint. One such means of encouraging restraint will reside in the US lead of establishing laws and norms for acceptable behavior in the globally connected domain of cyberspace. As General Chilton reported to Congress:

> Deterrence in any area involves a couple things. One, a position needs to be taken on -- a policy position, if you will. So you have to be able to look at somebody in the eye and say, "If you do this, then." And then whatever the "then" is has to be credible, both credible internally, but most important, credible in the individual's eye who you are trying to deter. [16]

Slower is Faster

> *The discussion we're going to enter into . . . is what is the role and responsibility of DHS and [what are] the legal and operational frameworks for sharing classified threat signatures with industry at* ***network speed*** *so that it is defensible.*
> Lieutenant General Keith Alexander, Commander Joint Functional Component Command for Network Warfare [64]

The catch phrase of the times is “net-speed” or “network speeds.” In the quote above, Lieutenant General Alexander is speaking about building the technical and legal frameworks to allow an anti-virus signature to be rapidly shared to protect US networks. Having rapid response capabilities that allow one to inoculate against emerging threats certainly contributes to deterrence and could be categorized in the “Responsive Infrastructure” or “Defense” legs of the new triad. However, deterrence inherently resides in the minds of people and is focused at influencing the actions of people. As such the necessity of operating at net-speeds is removed from the calculus of deterrence in some regards.

Figure 16- A-10 Air-to-Air Refueling

When I flew fighters, one of the times we would use the phrase “slower is faster” was when we were attempting to hook up to the tanker for an in-flight refueling. Certainly there are pressures to be expeditious. Sometimes people are low on gas, or there isn’t much time before one needs to be somewhere else to conduct a mission. If you try to go too fast- rush the tanker for example, the boom operator will just pull the refueling boom back into the airplane and you will have to reset and start the process all

over again. In the case of cyberspace deterrence strategy development and execution, the planner must appreciate where taking it slower is the more efficient means of implementing the strategy.

Efforts are best served by prior planning, and exercising what-ifs. The time of crisis is not the time to formulate plans and strategies to deal with a crippling cyberspace attack against the nation's critical infrastructure. Sometimes, when people hear a person like Lieutenant General Alexander or General Chilton representing a concept like operating at "network speeds", they only hear we must operate in cyberspace as fast as the network communications will allow. But when dealing with a concept like formulating and executing a cyberspace deterrence strategy, a concept focused on human beings, one must be willing to accept that "slower is faster." Some things that contribute to deterrence, sharing anti-virus signatures for instance, or developing attribution techniques for another, certainly lend themselves to "network speed" solutions. Overall though, shaping and tailoring effective deterrence strategies will be a human process completed at human speeds.

Findings

According to the DO JOC: Joint military operations and activities contribute to the "end" of deterrence by affecting the adversary's decision calculus elements in three "ways":

- Impose Costs
- Deny Benefits
- Encourage Adversary Restraint [4]

This research looked at combining these "ways" of deterrence towards the "end" of "Deterring cyber attack on the United States critical infrastructure**."** To be successful cyberspace deterrence strategy and a declaratory statement must first be issued from the office of the President of the United States. The president must declare what is important, and then explain the lengths to which the United States will go to protect its critical infrastructure against a cyber attack. The United States must be ready to impose costs to cyber adversaries. Defenses and Responsive Infrastructure as a means of implementing cyberspace deterrence strategy are incomplete without the complementing means of Strike. In addition, to declaratory policy, and maintaining a robust force prepared to impose cost across the spectrum of policy options, the United States must seek to deny safe havens to cyber adversaries and garner international support for norms and laws that are favorable to the US position

As the United States seeks to deny the adversary benefit to their actions, some traditional ways of conducting deterrence operations may not directly translate to cyberspace. Right now, "Detect and Preempt" is not a viable deterrence strategy in cyberspace. Garnering deterrence lessons from other domains such as space or concepts in other established mission areas like WMD holds great promise. As such, denying the

adversary the benefit of their actions by proving the US ability to fight through a cyber attack will serve as great deterrent to potential adversaries. As the US military plans for future conflict with cyber-capable foes, it must consider how its actions will be perceived by that enemy. JOPES planning should be updated to provide planning considerations for appropriately dealing with cyber-capable foes that could potentially attack the critical infrastructure of the United States. With some modifications, many of these considerations could be modeled after the already present nuclear sections in the JOPES planning process.

A balanced deterrence strategy contains all three elements in the DO JOC model; efforts to encourage restraint have the potential for the largest gains. Factors in cyberspace which contribute to moving the "consequences of restraint" fulcrum include: attribution, identity management, and incentivizing trust. Application that addresses these means will serve to make US attempts to impose costs and deny benefits to the adversary more effective and multiply the effect of those efforts.

Future Research

Deterrence is a "wicked problem." [2][14] Cyberspace Deterrence is even more "wicked". One of the characteristics of a "wicked problem" is that there is no stopping rule. Thus, there is plenty of room for future research. Some of the other areas ripe for future research include answering the following questions:

Deterrence Modeling

One area for future research is using operations research techniques to assess and compare deterrence strategies. [69] Determining the best model to analyze or formulate deterrence strategies is difficult. The author of this research spent much time looking at the use of Value Focused Thinking and Attack Trees and how these operations research techniques might contribute to analyzing deterrence options. Future research efforts could easily be spent looking at applying these tools to specific STRATCOM Deterrence policies, but this research would unfortunately be classified.

Playing into the adversary's hand

What are the goals, including the cyber goals, of our adversary? Does our cyberspace deterrence policy play into their hand? Do they want to bleed us dry, thus further investment serves only to weaken us? Is stealing technology to further their technical and economic ends an indication of this strategy?

International Cooperation

How do cyberspace deterrence strategies contribute to Assurance? By creating international support relationships does the United States increase the risk of getting pulled into a cyber conflict?

How could this risk be mitigated? Ambiguity might lessen the assurance effect, but it also decreases the risk.

What assures one ally may frighten another. How are assurance-messages crafted and tailored for allies in this domain?

---

[14] For a description of wicked problems see Dr. Tom Ritchey's research **"**Wicked Problems**:** Structuring Social Messes with Morphological Analysis**" at** http://www.swemorph.com/wp.html

As we view other nation-states as potential actors to engage with assurance policies, should the DOD view other departments/industry/civilians as agents that need assurance? Should the DoD focus communications to other agencies in our own government in order to implement a deterrence/assurance strategy?

Conceiving of responses outside of the cyber box

US government responses to cyber attack should include asymmetric responses (ie non-cyberspace). The US government should plan to use kinetic responses to a cyber attack. Although each situation is unique, perhaps a Response Option (RO) methodology should be examined for its merits. This RO could take the form of standardized cyber or non-cyber cost impositions in response to adversary actions that are not compliant with the US view of acceptable cyberspace behavior.

Too Big to Fail

When the US insurance industry started tanking, the phrase for the US Congress became that these companies were "too big to fail." In fact some companies bought more bad debt to make themselves too big to fail. This principle shows a potential deterrence strategy, by having too many interconnections with other potential cyber adversaries we make our relationship too big to fail. For example: If China is too important a partner, ie owns too much US debt, why would they risk attacking the US critical infrastructure and the subsequent failure of the economic relationship? Intricate Global partnerships and ties decrease the likelihood of an overwhelming cyber attack against the US.

Drawbacks to this strategy include issues with elements of society that may not answer to the leadership of a country but have great capability. For example Chinese hackers that may not answer to Chinese leadership, or correspondingly the Russian Mob, which may not take orders from the Russian leadership. Deterring these groups may require a differently tailored strategy.

Information assurance and secure networks

Information assuarance and securing networks contributes to deterrence by denying the adversary benefit of their actions and contributing to effectiveness of US opreations. Lieutenant General Keith Alexander laid out these truths in his congressional testimony when he wrote:

> Robust information assurance and securing vital networks must be our first priority. Our people play an important role in preventing unauthorized access to the critical systems in cyberspace. The cyber security training

> provided to our service men and women, and the civilian and contractor workforce is inadequate and must be improved.
>
> Secondly, the defense of our networks must be accountable to the highest levels, and managed as such. It is imperative that all commanders enforce measures to ensure the readiness of networks managed by personnel under their purview. Our adversaries are taking advantage of this lack of assiduousness and discipline that ultimately costs hundreds of millions of dollars in lost information and work hours.
>
> Finally, we must leverage the power of automated security protocols to effectively manage these threats we face every day. For example, deploying a host based security system will provide a level of security that potentially will operate at the speed of the network, and centrally update systems to a trusted baseline. [64]

Documenting and understanding the role of information assurance and network security contributions to overall deterrence strategy is a great undertaking. Better understanding these contributions and the limitations of information assurance will be important as strategies are assessed for their effectiveness at deterring attack.

Appendix A

One key factor necessitating a change in the way the United States approaches deterrence is the emergence of a multi-polar world. During the cold war the world was nominally bi-polar with the Soviet Union and the United States facing each other down. In this environment the concept of nuclear deterrence and Mutually Assured Destruction (MAD) was developed to keep us from the unthinkable and undesirable outcome of military hostilities- escalation to nuclear war. The new threat environment is composed of a variety of state and non-state actors who pose significant threat to the interests of the United States, particularly through and in cyberspace. The management of the relationships with these emerging cyber powers will help to shape future security strategies and changes the face of deterrence in this new age.

The traditional view of deterrence

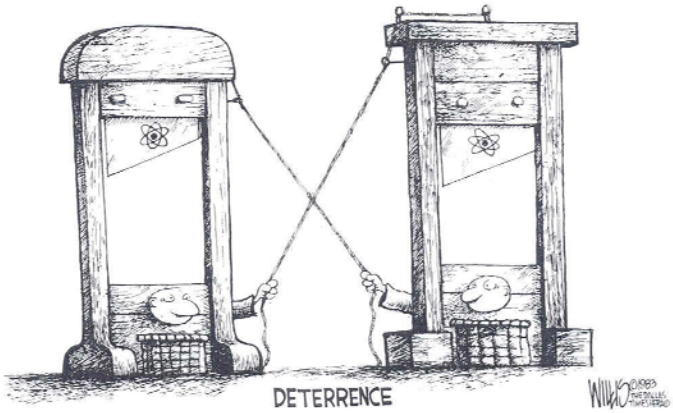


Figure 17- Deterrence by Punishment Focus

JP 1-02 defines deterrence as: "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." [40 p. 161] This view of deterrence focuses on punishment, or imposing cost to an adversary's actions that outweigh the benefits he might receive.

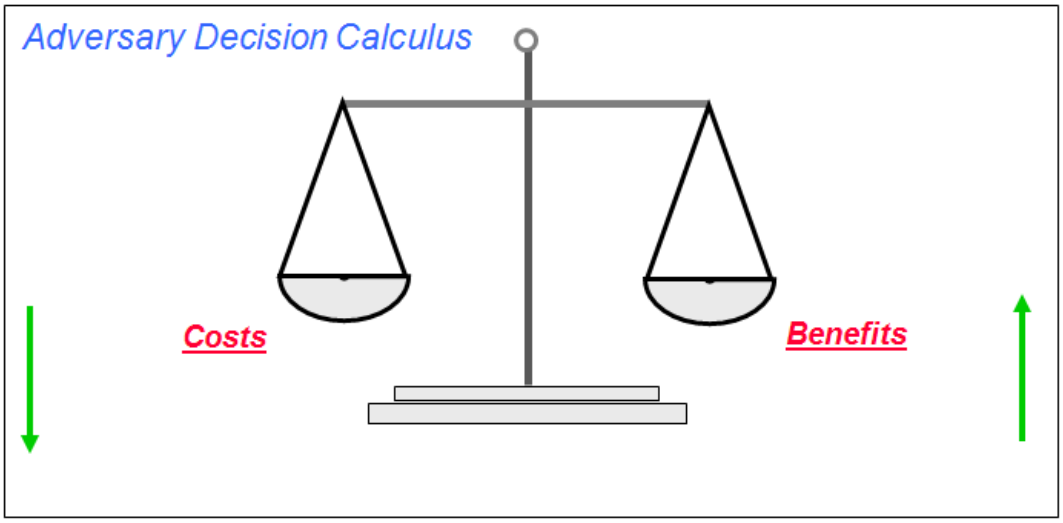


Figure 18-Traditional View of Deterrence

In the traditional view of deterrence (as defined in the most current JP 1-02 dictionary), there is an assumption of a fixed fulcrum. The formula for computing deterrence looks like:

$$\text{Deterrence}_{\text{them}} = \text{Costs}_{\text{them}} - \text{Benefits}_{\text{them}}$$

This model is focused then on weighing only the benefit of adversary action against the cost of adversary action. One of the problem's with this model is that if there was no unacceptable cost to your adversary then you would have the problem of the 'Undeterrable' Actor.

The Joint dictionary then goes on to define **deterrent options** as **"**A course of action, developed on the best economic, diplomatic, political, and military judgment, designed to dissuade an adversary from a current course of action or contemplated operations. (In constructing an operation plan, a range of options should be presented to effect deterrence. Each option requiring deployment of forces should be a separate force module.)" Although focusing deterrence across the Range of Military Operations as well as the DIME this definition aligns itself with the traditional view of deterrence.

The new deterrence definition from DO JOC is **"**Deterrence operations convince adversaries not to take actions that threaten US vital interests by means of decisive influence over their decision-making. Decisive influence is achieved by credibly threatening to deny benefits and/or impose costs while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome."

A brief review of physics- the power of the fulcrum

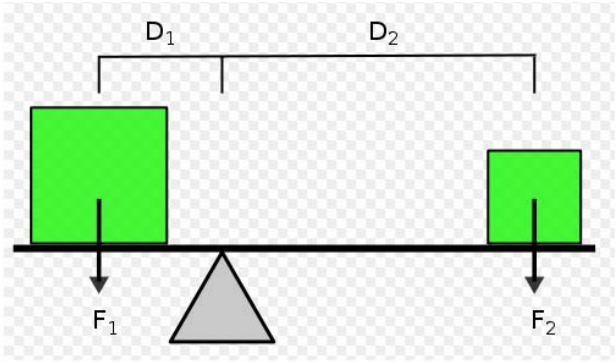


Figure 19- Lever principles [70]

Using Newton's laws of motion, one can compute the principles involved in leverage. The amount of work done is computed by Force times the Distance. In the above figure, if $F_1D_1 = F_2D_2$ then all forces are balancing and the lever is in static equilibrium. The point you apply the force is called the effort. The effect of applying this force is called the load. If we move the fulcrum of the lever system we change the equation by which we compute the force required to lift a weight. For example, if we balance a one gram feather on one end of the lever with a one kilogram weight on the other, the feather will need to be 1000 times further from the fulcrum point than the one kilogram weight. [71]

Why this physics review? It reveals the power of the idea of the fulcrum point. In the traditional deterrence model, the fulcrum point was fixed and the only concern was the mass of the cost compared to the mass of the benefits. Now with a movable fulcrum point: the consequences of restraint, you have a powerful multiplier to more effectively develop deterrence policies. Although all three areas of deterrence calculation are

important, the inclusion of these consequences of restraint is what makes the DO JOC methodology different from traditional deterrence formulation and calculation.

The DO JOC model of deterrence

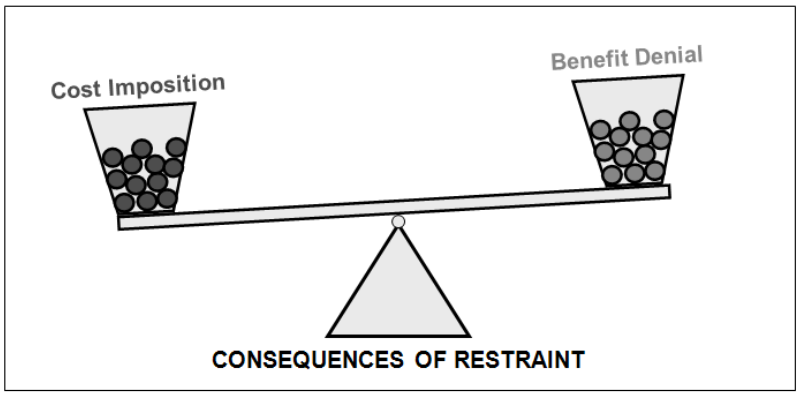


Figure 20- DO JOC model of deterrence [1]

Deterrence is successful, in the DO JOC model, when the perceived costs incurred by an adversary ($mass_1$) outweigh the perceived benefits ($mass_2$) in regard to the consequences of restraint (fulcrum).

Deterrence fails in this model when an adversary perceives that the benefit of taking an action outweighs the costs, and the adversary takes the actions which are contrary to US interests.

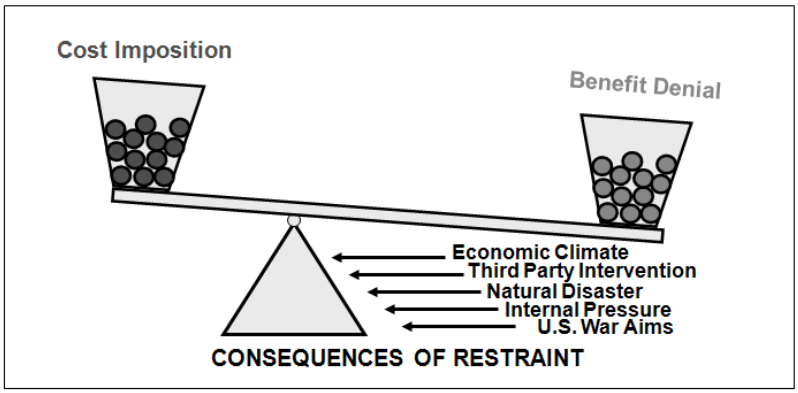


Figure 21- Consequences of Restraint

The difference of the DO JOC from the old model is the consequences of restraint. "Given an otherwise favorable situation, forces exist that may cause an adversary to act contrary to US interests. Increasing adversary consequences of restraint can (over time) result in deterrence failure. These factors influence the capabilities the US must employ to maintain/restore deterrence." [1] Obviously, if the physics upon which the model is based hold true, then deterrence efforts will have their greatest effect when they move the fulcrum so as to make the costs more effective than the benefits.

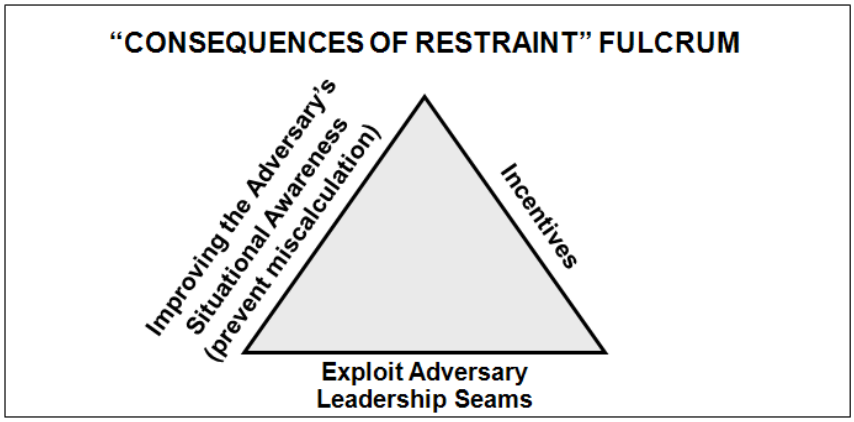


Figure 22- COR Fulcrum

The elements of the consequence of restraint fulcrum are not well established or agreed upon, but the authors of the SD JOC feel it includes at a minimum- Improving the Adversary's Situational Awareness, Providing Incentives to the adversary, and Exploiting Adversary Leadership seams. [1] When analyzing cyberspace, attribution, identification and exploiting the trust relationships of the internet should be considered in the ways that these concepts affect the "consequences of restraint" fulcrum.

The new Triad

Another emerging idea, and a way that deterrence has changed from the Cold War era, is in the concept of the New Triad. In January of 2002, President George W Bush, announced a new strategic triad in the Nuclear Posture Review (NPR). This new triad is based on: nuclear and precision non-nuclear strike forces; passive and active defenses; and a revitalized defense infrastructure. [15]

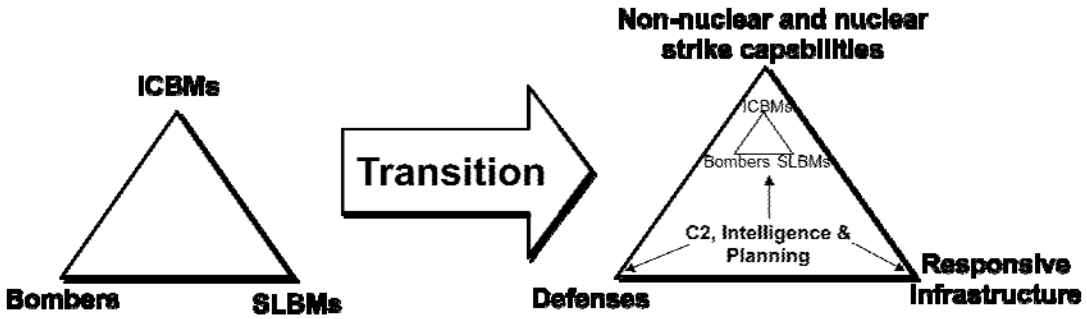


Figure 23- New Triad

In the new triad, deterrence is bolstered through the US ability to respond with tailored means to aggression. Although conceived originally for nuclear deterrence, the new triad can stand in nicely on other deterrence efforts- including cyberspace.

Cyberspace deterrence efforts can be categorized into the Strike, Defense and Responsive Infrastructure legs. One drawback to the new construct is that it doesn't account for the adversary's consequences of restraint. This can be found in the DO JOC construct of describing deterrence strategy. When combining the new triad with the DO JOC concept of deterrence, you have an able means of both categorizing US deterrence efforts in the new triad, and describing deterrence effects focused on an adversary with the DO JOC.

Appendix B

Table 4- Critical Infrastructure Sectors

Sector	Description
Agriculture	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production.
Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions, including clearing and settlement.
Chemicals and hazardous materials	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical industry produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.
Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.
Dams	Comprises approximately 80,000 dam facilities, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.
Drinking water and water treatment systems	Sanitizes the water supply through about 170,000 public water systems. These systems depend on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.
Emergency services	Saves lives and property from accidents and disasters. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.
Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. This sector is divided into electricity and oil and natural gas.
Food	Carries out the postharvesting of the food supply, including processing and retail sales.
Government	Ensures national security and freedom and administers key public functions.
Government facilities	Includes the buildings owned and leased by the federal government for use by federal entities.
Information technology	**Produces hardware, software, and services that enable other sectors to function.**
National monuments and icons	Includes key assets that are symbolically equated with traditional American values and institutions or U.S. political and economic power.
Nuclear reactors, materials, and waste	Includes 104 commercial nuclear reactors; research and test nuclear reactors; nuclear materials; and the transportation, storage, and disposal of nuclear materials and waste.
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The United States Postal Service and other carriers provide the services of this sector.
Public health and healthcare	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. This sector consists of health departments, clinics, and hospitals.
Telecommunications	**Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.**
Transportation	Enables movement of people and assets that are vital to our economy, mobility, and security, using aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.

Source: GAO report Internet Infrastructure-DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan (June 2006), as taken from Homeland Security Presidential Directive 7 (Dec 17, 2003)

Bibliography

[1] Okey, Hal, LCDR USN., "DTIC." *Strategic Deterrence (SD) Joint Operating Concept (JOC) Version 2.0.* [Online] [Cited: 02 17, 2009.] www.dtic.mil/futurejointwarfare/strategic/sd_joc.ppt.

[2] Ritchey, Tom., "Wicked Problems Structuring Social Messes with Morphological Analysis." *swemorph.com.* [Online] 2005-2008. [Cited: 05 25, 2009.] http://www.swemorph.com/wp.html.

[3] Department of Defense., "Joint Publication 1 Doctrine for the Armed Forces of the United States Incorporating Change 1." *dtic.mil.* [Online] March 20, 2009. [Cited: 05 27, 2009.] http://www.dtic.mil/doctrine/jel/new_pubs/jp1.pdf.

[4] —. "Deterrence Operations Joint Operating Concept." *dtic.mil.* [Online] Dec 2006. [Cited: 05 25, 2009.] www.dtic.mil/futurejointwarfare/concepts/do_joc_v20.doc.

[5] CSIS Commission on Cybersecurity for the 44th Presidency., "Securing Cyberspacefor the 44th Presidency." *DIME: Information as Power.* [Online] Dec 2008. [Cited: 05 04, 2009.] http://www.carlisle.army.mil/DIME/documents/CSISCyber%20Report%20Final.pdf.

[6] Government Accountability Office- Statement of David Powner., "Critical Infrastructure Protection- Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies." [Online] 10 31, 2007. [Cited: 05 20, 2009.] http://homeland.house.gov/SiteDocuments/20071031154933-23969.pdf.

[7] —. "National Cybersecurity Stategy: Key Improvements Are Needed to Strengthen the Nation's Posture." *GAO.* [Online] 03 10, 2009. [Cited: 05 20, 2009.] http://www.carlisle.army.mil/DIME/documents/Powner%20Testimony.pdf.

[8] Miller, Robert A. and Lachow, Irving., "Strategic Fragility: Infrastructure Protection and National Security in the Information Age." [Online] Jan 2008. [Cited: 05 20, 2009.] http://www.ndu.edu/CTNSP/defense_horizons/DH59.pdf.

[9] Government Accountability Office., "Internet Infrastructure- DHS Faces Challenges in Developing a Join Public/Private Recovery Plan." [Online] June 2006. [Cited: 05 20, 2009.] http://www.gao.gov/new.items/d06672.pdf.

[10] , "The National Strategy to Secure Cyberspace." [Online] February 2003. [Cited: 05 20, 2009.] http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

[11] Mauney, Vice Admiral Carl V., "Space Weapons in the 21st Century." *USSTRATCOM.* [Online] 01 29, 2009. [Cited: 05 06, 2009.] http://www.stratcom.mil/speeches/19/.

[12] Saydjari, O. Sami., "Addressing the Nation’s Cyber Security Challenges: Reducing Vulnerabilities." *US House of Representatives Committee on Homeland Security.* [Online] 04 25, 2007. [Cited: 05 06, 2009.] http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf.

[13] Georgia Tech Information Security Center., "Emerging Cyber Threats Report for 2009." *DIME: Information as Power.* [Online] 10 15, 2008. [Cited: 05 04, 2009.] http://www.carlisle.army.mil/DIME/documents/CyberThreatsReport2009[1].pdf.

[14] Walsh, David., "Greater cooperation needed to defeat cyber enemies." *Defense Ssytems.* [Online] 01 30, 2009. [Cited: 05 06, 2009.] http://defensesystems.com/articles/2009/01/30/cooperation-needed-to-defeat-cyber-enemies.aspx?s=ds_040209.

[15] Russell, James and Wirtz, James J., "A Quiet Revolution: The New Nuclear Triad." *Center for Contempory Conflict.* [Online] May 2002. [Cited: 05 20, 2009.] http://www.ccc.nps.navy.mil/si/may02/triad.asp.

[16] Chilton, Kevin P. General., "House Armed Services Committee Testimony." *USSTRATCOM.* [Online] 3 17, 2009. [Cited: 05 02, 2009.] http://www.stratcom.mil/speeches/21/.

[17] Obama, Barack., "REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE." *whitehouse.gov.* [Online] 05 29, 2009. [Cited: 06 03, 2009.] http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

[18] Brafman, Ori and Beckstrom, Rod., *The Starfish and the Spider.* New York : Penguin Group, 2006.

[19] Fulghum, David A., "Cyber Plans, Missing and Missed." *Ares: A Defense Technology Blog* . [Online] 05 06, 2009. [Cited: 05 20, 2009.] http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckScript=blogScript&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog%3A27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3Aa3068a83-f1e6-4f73-8a9c-713d90c1e1f7.

[20] Gorman, Siobhan., "Electricity Grid in U.S. Penetrated By Spies ." *WSJ.* [Online] 04 08, 2009. [Cited: 05 04, 2009.] http://online.wsj.com/article/SB123914805204099085.html.

[21] RSS., "U.S. Under Siege from Chinese, Russian Cyber-Attackers." [Online] 04 08, 2009. [Cited: 05 22, 2009.] http://www.newsmax.com/headlines/cyberattacks_power_grid/2009/04/08/201226.html.

[22] UNH Media Relations., "Who Are The Greatest Cyber Attack Threats To The United States?" *UNH Media Relations* . [Online] 01 25, 2007. [Cited: 05 22, 2009.] http://www.unh.edu/news/cj_nr/2007/jan/lw25cyber.cfm.

[23] Marks, Paul., "Pentagon readies its cyberwar defences ." *New Scientist.* [Online] 03 16, 2009. [Cited: 05 04, 2009.] http://www.newscientist.com/article/mg20126994.600-pentagon-readies-its-cyberwar-defences.html.

[24] Thomas, Timothy L., "Deterring Information Warfare: A New Strategic Challenge." [Online] Winter 1996-97. [Cited: 05 04, 2009.] http://www.carlisle.army.mil/USAWC/PARAMETERS/96winter/thomas.htm.

[25] Bunn, M. Elaine., "Can Deterrence Be Tailored?" *Strategic Forum* . [Online] Jan 2007. [Cited: 05 04, 2009.] http://www.ndu.edu/inss/Strforum/SF225/SF225.pdf.

[26] Report to the President's Commision on Critical Infrastructure Protection., "DIME: Information as Power." *Toward Deterrence in the Cyber Dimension.* [Online] 1997. [Cited: 05 04, 2009.] www.carlisle.army.mil/DIME/documents/173_PCCIPDeterrenceCyberDimension_97.pdf -.

[27] Canaves, Sky., "China Denies Hacking U.S. Electricity Grid." *WSJ: China Journal.* [Online] 04 09, 2009. [Cited: 05 04, 2009.] http://blogs.wsj.com/chinajournal/2009/04/09/china-denies-hacking-us-electricity-grid/.

[28] Wheatley, Gary F. and Hayes, Richard E., "Information Warfare and Deterrence ." *Institute for National Strategic Studies.* [Online] Dec 1996. [Cited: 05 04, 2009.] http://www.fas.org/irp/threat/cyber/docs/iwd/index.html.

[29] Chertoff, Michael Secretary of Homeland Security., "Remarks by Secretary Michael Chertoff at the Cyber Strategic Inquiry 2008." *Homeland Security.* [Online] 12 19, 2008. [Cited: 05 14, 2009.] http://www.dhs.gov/xnews/speeches/sp_1229714843263.shtm.

[30] Koerner, Brendan I., "From Russia With LØpht." *Legal Affairs.* [Online] 04 30, 2002. [Cited: 05 04, 2009.] http://www.legalaffairs.org/printerfriendly.msp?id=286.

[31] Reid, Tim., "China’s cyber army is preparing to march on America, says Pentagon." *TimesOnline.* [Online] sep 8, 2007. [Cited: 05 04, 2009.] http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece.

[32] , UN-backed anti-cyber-threat coalition launches headquarters in Malaysia. *UNESCO.* [Online] 03 24, 2009. [Cited: 05 04, 2009.] http://portal.unesco.org/ci/en/ev.php-URL_ID=28464&URL_DO=DO_TOPIC&URL_SECTION=201.html.

[33] UN News service., "Progress in disarmament will free up resources for development, says Ban." *UN News CENTRE.* [Online] 02 18, 2009. [Cited: 05 04, 2009.] http://www.un.org/apps/news/story.asp?NewsID=29947&Cr=disarmament&Cr1.

[34] Denning, Dorothy., "Reflections on Cyberweapons Controls." [Online] Fall 2000. [Cited: 05 04, 2009.] www.cs.georgetown.edu/~denning/infosec/cyberweapons-controls.doc.

[35] Department of Defense., "Ballistic Missile Defense Program." *fas.org.* [Online] 07 13, 2001. [Cited: 05 04, 2009.] http://www.fas.org/spp/starwars/010713-D-6570C-001.pdf.

[36] Chilton, Kevin P., General., "Speech: 2009 Cyberspace Symposium." *USSTRATCOM.* [Online] 04 07, 2009. [Cited: 05 01, 2009.] http://www.stratcom.mil/speeches/23/.

[37] Elder, Robert Lieutenant General, USAF., "NDIA 2007 DIB Infrastructure Protection Symposium." *NDIA.* [Online] 04 11, 2007. [Cited: 05 14, 2009.] proceedings.ndia.org/7030/Elder.pdf.

[38] US Air Force., "Air Force Fact Sheets- Airpower in Operation Desert Storm." *About.com.* [Online] [Cited: 05 14, 2009.] http://usmilitary.about.com/library/milinfo/affacts/blairpowerinoperationdesertstorm.htm.

[39] American Forces Press Service., "The Operation Desert Shield/Desert Storm Timeline." *defenselink.* [Online] aug 08, 2000. [Cited: 05 14, 2009.] http://www.defenselink.mil/news/newsarticle.aspx?id=45404.

[40] Department of Defense., "Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms." *Joint Electronic Library.* [Online] October 17, 2008. [Cited: 04 15, 2009.] http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

[41] 8AF/PA., "Flying and Fighting in CYBERSPACE." *afcyber.af.mil.* [Online] [Cited: 05 27, 2009.] http://www.afcyber.af.mil/shared/media/document/AFD-071213-047.pdf.

[42] Department of Defense., *Quadrennial Roles and Missions Review Report.* s.l. : Department of Defense, January, 2009.

[43] Sakrisson, Ben Captain., "'Space as a contested environment' debuts." *Air Force Link.* [Online] 30 3, 2009. [Cited: 04 13, 2009.] http://www.af.mil/news/story.asp?storyID=123142047.

[44] GAO., "Military Space Operations: Planning, Funding and Acquisition Challenges Facing Efforts to Strengthen Space Control." *www.GAO.gov.* [Online] Sep 2002. [Cited: 04 13, 2009.] http://www.gao.gov/new.items/d02738.pdf.

[45] Holmes, Erik., "Lab to build special order satellites in days." *Air Force Times.* [Online] 02 20, 2009. [Cited: 4 13, 2009.] http://www.airforcetimes.com/news/2009/02/af_satellites_space_022009/.

[46] Wegner, Peter Dr., "Operationally Responsive Space: Meeting the Joint Force Commanders' Needs." *www.ResponsiveSpace.com.* [Online] 02 5, 2009. [Cited: 04 13, 2009.] http://www.responsivespace.com/ors/reference/ORS%20Office%20Overview_PA_Cleared%20notes.pdf.

[47] Magnuson, Stew., "'Responsive Space' Office Must Quickly Prove Itself, Proponents Say." *National Defense.* [Online] [Cited: 04 13, 2009.] http://www.nationaldefensemagazine.org/ARCHIVE/2007/DECEMBER/Pages/Responsive2407.aspx.

[48] Wikipedia., Wicked problem. *Wikipedia.* [Online] [Cited: 05 22, 2009.] http://en.wikipedia.org/wiki/Wicked_problem.

[49] Chilton, Kevin P. General., "Land War Net Speech." *US STRATCOM.* [Online] 08 21, 2008. [Cited: 05 14, 2009.] http://www.stratcom.mil/speeches/16/.

[50] Chilton, Kevin and Weaver, Greg., "Waging Deterrence in the Twenty-First Century." *Air University- Strategic Studies Quarterly.* [Online] Spring 2009. [Cited: 05 11, 2009.] http://www.au.af.mil/au/ssq/2009/Spring/chilton.pdf.

[51] Wheeler, David A. and Larsen, Gregory N., "Techniques for Cyber Attack Attribution." *Institute for Defense Analyses.* [Online] Oct 2003. [Cited: 05 21, 2009.]

http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf.

[52] Hunker, Jeffrey, Hutchinson, Bob and Margulies, Jonathan., "Role and Challenges for Sufficient Cyber-Attack Attribution." s.l. : Institute for Information Infrastructure Protection, Jan 2008.

[53] , Characterizing and Tracing Packet Floods Using Cisco Routers ; Document ID: 13609. *CISCO website.* [Online] 05 27, 2005. [Cited: 03 30, 2009.] http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080149ad6.shtml#topic13.

[54] Whyte, David., Following the Journey of a Spoofed Packet. [Online] [Cited: 03 30, 2009.] http://www.scs.carleton.ca/~dlwhyte/whytepapers/ipspoof.htm.

[55] Surdu, Gregory Lt Colonel and Conti, John Colonel., "Army, Navy, Air Force, and Cyber—Is it Time for a Cyberwarfare Branch of Military?" *IAnewsletter Vol 12 No 1 Spring 2009 • http://iac.dtic.mil/iatac.* [Online] Spring 2009. [Cited: 03 30, 2009.] http://www.bucksurdu.com/Professional/Documents/IAN_12-1_conti-surdu.pdf.

[56] Aitoro, Jill R., "HSPD-12." *nextgov.com.* [Online] 02 10, 2008. [Cited: 05 25, 2009.] http://www.nextgov.com/the_basics/tb_20080610_8037.php.

[57] OMB communications., "OMB Reports Significant HSPD-12 Implementation Progress but Areas for Improvement Identified." *Office of Management and Budget.* [Online] 10 31, 2008. [Cited: 05 20, 2009.] http://www.whitehouse.gov/omb/pubpress/2008/103108_hspd12.html.

[58] Krebs, Brian., "Major Source of Online Scams and Spams Knocked Offline." *The Washington Post.* [Online] 11 11, 2008. [Cited: 05 25, 2009.] http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html.

[59] Kirk, Jeremy., "ISP Cut off From Internet After Security Concerns." *PC World.* [Online] 11 12, 2008. [Cited: 05 25, 2009.] http://www.pcworld.com/businesscenter/article/153734/isp_cut_off_from_internet_after_security_concerns.html.

[60] Armin, Jart (editor)., "McColo - Cyber Crime USA 2008 Version 2.0." *HOSTEXPLOIT.COM.* [Online] 2008. [Cited: 05 25, 2009.] http://hostexploit.com/downloads/Hostexploit%20Cyber%20Crime%20USA%20v%202.0%201108.pdf.

[61] Bush, George President of the United States., "The National Security Strategy of the United States of America." [Online] Mar 2006. [Cited: 05 22, 2009.] http://www.marforres.usmc.mil/docs/nss2006.pdf.

[62] Department of Defense., "Joint Publication 5-0: Joint Operation Planning." *JTIC.* [Online] Dec 26, 2006. [Cited: 05 11, 2009.] http://www.dtic.mil/doctrine/jel/new_pubs/jp5_0.pdf.

[63] Gershwin, Lawrence K. National Intelligence Officer for Science and Technology., "Cyber Threat Trends and US Network Security: Statement for the Record to the Joint Economic Committee." *National Intelligence Council.* [Online] 06 21, 2001. [Cited: 05 13, 2009.] http://www.dni.gov/nic/testimony_cyberthreat.html.

[64] Lieutenant General Keith Alexander, USA, Commander, Joint functional Component Command Netwrok Warfare Director, National Security Agency., "Statement for the Record Before the House Armed Services Committee Terrorism, Unconventional Threats, and Capabilities Subcommittee." *House armed services committee.* [Online] 05 05, 2009. [Cited: 05 11, 2009.] http://armedservices.house.gov/pdfs/TUTC050509/Alexander_Testimony050509.pdf.

[65] Lykke, Arthur F. Jr., "Chapter 13- TOWARD AN UNDERSTANDING OF MILITARY STRATEGY." *Air University.* [Online] [Cited: 05 22, 2009.] http://www.au.af.mil/au/awc/awcgate/army-usawc/strategy/13lykke.pdf.

[66] US Senate Committee on Commerce, Science and Transportation., "Bill Would Federalize Cybersecurity- Senate Proposal Would Affect Even Some Private Networks ." *US Senate Committee on Commerce, Science and Transportation.* [Online] 04 01, 2009. [Cited: 05 18, 2009.] http://www.commerce.senate.gov/public/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=6bdb9f79-80f9-409a-a084-9f5dac0bf692&Month=4&Year=2009.

[67] Agence France-Presse., "US military needs unified cyber command: NSA chief." *ABS CNS News.* [Online] 05 06, 2009. [Cited: 05 22, 2009.] http://www.abs-cbnnews.com/technology/05/06/09/us-military-needs-unified-cyber-command-nsa-chief.

[68] Paone, Chuck., "General calls for new thinking on cyberspace." *AF Print News Today.* [Online] 05 12, 2009. [Cited: 05 18, 2009.] http://www.af.mil/news/story_print.asp?id=123148876.

[69] McKenna, Pat., "The Deterrence Analytic Challenge." *ndu.edu.* [Online] [Cited: 05 25, 2009.] http://www.ndu.edu/CTNSP/HSCB/HSCB%20Deterrence%20-%20Dr%20Pat%20McKenna%20-%20The%20Deterrence%20Analytic%20Challenge.pdf.

[70] Iainf., Diagram showing the Lever Principle. *wikimedia.* [Online] 07 09, 2006. [Cited: 04 15, 2009.] http://commons.wikimedia.org/wiki/File:LeverPrincleple.svg.

[71] Wkipedia., Lever. *Wikipedia.* [Online] [Cited: 04 15, 2009.] http://en.wikipedia.org/wiki/Lever.

[72] US Strategic Command., "Joint Operating concepts." [Online] December 2006. [Cited: 02 17, 2009.] www.dtic.mil/futurejointwarfare/concepts/do_joc_v20.doc.

[73] Glaser, Charles L., Politcal Consequences of Military Strategy- Expanding and Refining the Spiral and Deterrence Models. *harrissschool.* [Online] July 1992. [Cited: 04 15, 2009.] http://harrisschool.uchicago.edu/faculty/articles/Glaser-WorldPolitics-1992.pdf.

[74] —. "Correspondence- Taking Offense at Offense-Defense Theory." *Harris School.* [Online] Winter 1998/1999. [Cited: 04 15, 2009.] http://harrisschool.uchicago.edu/faculty/articles/Glaser8.pdf.

[75] Goldman, Harriet G. and Woodward, John P. L., *Defending Against Advanced Cyber Threats.* s.l. : The MITRE Corporation, 2008.

[76] Thomas, Timothy L., "FMSO Special Study." *Dialectical Versus Empriical Thinking: Ten Key Elements of the Russian Understanding of Information Operations.* [Online] Sep 1998. [Cited: 05 04, 2009.] http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA434981&Location=U2&doc=GetTRDoc.pdf.

[77] , "National Strategy for Combatting Terrorism." [Online] 2006. [Cited: 05 04, 2009.] http://www.cbsnews.com/htdocs/pdf/NSCT0906.pdf.

[78] The Claremont Institute., The Stages of a Ballistic Missile's Flight. *missilethreat.com.* [Online] [Cited: 05 06, 2009.] http://www.missilethreat.com/overview/pageID.157/default.asp.

[79] Resende, Patricia., "U.S. Not Ready for Georgia-Style Computer Attacks." *newsfactor.com.* [Online] 08 15, 2008. [Cited: 05 18, 2009.] http://www.newsfactor.com/story.xhtml?story_id=61369.

[80] , "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection." [Online] 12 17, 2003. [Cited: 05 20, 2009.] http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

[81] Gertz, Bill., "China Bolsters For 'Cyber Arms Race' With U.S." *Early Bird: from The Washington Times.* [Online] 05 12, 2009. [Cited: 05 20, 2009.] http://ebird.osd.mil/ebfiles/e20090512676613.html.

[82] Wald, Charles F., "The Phase Zero Campaign." *ndupres s .ndu.edu.* [Online] 4th Quarter 2006. [Cited: 05 23, 2009.] http://www.ndu.edu/inss/press/jfq_pages/editions/i43/20%20JFQ43%20Wald.pdf.

[83] Durkac, Louis M., Colonel, USAF., "Effects-Based Operation Planning: "Convergent" Course of Action (COA) Development." *dodccrp.org.* [Online] 02 17, 2006. [Cited: 05 24, 2009.] http://www.dodccrp.org/events/2006_CCRTS/html/papers/229.pdf.

[84] Brewin, Bob., "NSA director calls for a cyberspace Monroe Doctrine." *nextgov.com.* [Online] 05 06, 2009. [Cited: 05 25, 2009.] http://www.nextgov.com/nextgov/ng_20090506_4087.php?oref=mostread.

[85] The Office of the President of the United States., "Cyberspace Policy Review." *whitehouse.gov.* [Online] 05 29, 2009. [Cited: 06 03, 2009.] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[86] Bradley, Jennife, Stork, Brian and Burnett, Mark., Deterrence Operations Joint Operating Concept. *Strategic Deterrence Assessment Lab.* USSTRATCOM, Omaha, Nebraska, 04 09, 2009.

Vita

Major Kevin Beeker entered the Air Force through the United States Air Force Academy in 1996 where he was awarded a B.S. in Computer Science.

Maj Beeker is a senior pilot and has flown the A/OA-10 Warthog and F/A-18 Hornet. He was selected to attend AFIT in 2008 and is currently completing the Cyber Warfare Intermediate Developmental Education program. Upon graduation he will be assigned to the US Strategic Command, Joint Functional Component Command for Network Warfare.

SF 298

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**			
1. REPORT DATE *(DD-MM-YYYY)* 18-06-09	**2. REPORT TYPE** Graduate Research Project		**3. DATES COVERED** *(From – To)* 15 May 2008 – 18 June 2009
4. TITLE AND SUBTITLE **Strategic Deterrence in Cyberspace: Practical Application**		**5a. CONTRACT NUMBER** N/A	
		5b. GRANT NUMBER N/A	
		5c. PROGRAM ELEMENT NUMBER N/A	
6. AUTHOR(S) **Kevin R. Beeker, Major, USAF**		**5d. PROJECT NUMBER** ENS 09-153	
		5e. TASK NUMBER: N/A	
		5f. WORK UNIT NUMBER N/A	
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)			**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/ICW/ENG/09-01
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Major William F. Dobbs (DSN: 425-8586, NIPR e-mail: william.dobbs@pentagon.af.mil) Headquarters, United States Air Force, Office of the Vice Chief of Staff, Quadrennial Defense Review Office 1670 Air Force Pentagon Washington, DC 20330			**10. SPONSOR/MONITOR'S ACRONYM(S)** **HAF/CVAQ**
			11. SPONSOR/MONITOR'S REPORT NUMBER(S): N/A
12. DISTRIBUTION/AVAILABILITY STATEMENT Unclassified//Cleared for Public Release			
13. SUPPLEMENTARY NOTES : None			

14. ABSTRACT

This research outlines practical steps that the United States can take to improve strategic deterrence in cyberspace. The unique character of cyberspace requires tailoring of traditional deterrence strategies to fit the domain. This research uses the Deterrence Operations Joint Operating Concept (DO JOC) and the New Triad as models for organizing deterrence operations. The DO JOC focuses on tailoring deterrence operations based on the actor; but deterrence operations must be also be tailored to the uniqueness of cyberspace. The effective tailoring of deterrence operations for cyberspace will require both the application of new ways and means and the tailoring of traditional deterrence concepts to fit this new domain. Practical application of cyber strategic deterrence involves: issuance of US declaratory cyber deterrence policy; removing sanctuaries for cyber adversaries; changing US and adversary mindsets and expectations for what is permitted in cyberspace; changes to military planning in order to conduct operations in consideration of adversary cyber capability; and appreciation of the key policy tradeoffs with respect to cyber deterrence implementation. Cyberspace deterrence should include all three ways of implementing a deterrence strategy: imposing costs, denying benefits, and inducing adversary restraint. Influencing the "Consequences of Restraint" fulcrum through attribution, identity management, and incentivizing trust holds great promise for cyberspace deterrence.

15. SUBJECT TERMS
Computer Network Operations, Force Presentation, Command and Control, Joint Doctrine, Cyberspace

16. SECURITY CLASSIFICATION OF: Unclassified/Releasable to Public			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
REPORT	ABSTRACT	c. THIS PAGE			**Robert F. Mills, PhD**
Unclass	Unclas s	Unclass		119	**19b. TELEPHONE NUMBER** *(Include area code)*(937) 257-3636x4527