AU/ACSC/GALE/AY09

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

CYBERMAD: SHOULD THE UNITED STATES ADOPT A MUTUALLY ASSURED DESTRUCTION POLICY FOR CYBERSPACE?

by

David A. Gale, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: John T. Ackerman, PhD

Maxwell Air Force Base, Alabama

April 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2009	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
CYBERMAD: Should The United States Adopt A Mutually Assured Destruction Policy For Cyberspace?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Command And Staff College Air University Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Cyberspace has grown in importance to the United States (US), as well as the rest of the word. As such, the impact of cyberspace attacks have increased with time. Threats can be categorized as state or non-state actors. This research paper looks at state actors. It asks the question, should the US adopt a mutually assured destruction (MAD) doctrine for cyberspace? In order to answer this question, this research used a parallel historical case study. The case study was the USs nuclear MAD doctrine of the 1960s. What was the answer? The question is better left to the politicians. As with nuclear strategies, statesmen must decide if the MAD strategy for cyberspace is acceptable or unacceptable. If it is acceptable, they must decide the threat thresholds. In other words, when will the US pull the trigger. If US statesmen decide to purse a CyberMAD policy, they must ensure that the capability exists, that the US has the will to carry through on it, and that the opponent fears the consequences. Without these three criteria, the credibility of the threat is reduced, thus, the deterrence effect is reduced. Finally, regardless of the strategy the US chooses, one item is clear. The US can either choose to defend, or to defend and deter. The first option is purely defensive in nature. The second is defensive and offensive in nature. The US already has the capability to destroy cyberspace, but does it have the will? Politicians will need to answer this question.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**33**	

Disclaimer

Contents

Abstract

Cyberspace has grown in importance to the United States (US), as well as the rest of the word. As such, the impact of cyberspace attacks have increased with time. Threats can be categorized as state or non-state actors. This research paper looks at state actors. It asks the question, should the US adopt a mutually assured destruction (MAD) doctrine for cyberspace? In order to answer this question, this research used a parallel historical case study. The case study was the US's nuclear MAD doctrine of the 1960s. What was the answer? The question is better left to the politicians. As with nuclear strategies, statesmen must decide if the MAD strategy for cyberspace is acceptable or unacceptable. If it is acceptable, they must decide the threat thresholds. In other words, when will the US pull the trigger. If US statesmen decide to purse a CyberMAD policy, they must ensure that the capability exists, that the US has the will to carry through on it, and that the opponent fears the consequences. Without these three criteria, the credibility of the threat is reduced, thus, the deterrence effect is reduced. Finally, regardless of the strategy the US chooses, one item is clear. The US can either choose to defend, or to defend and deter. The first option is purely defensive in nature. The second is defensive and offensive in nature. The US already has the capability to destroy cyberspace, but does it have the will? Politicians will need to answer this question.

Introduction

In November 2008, an extraordinary event happened. Senior United States (US) military leaders briefed The President of the United States on a "severe and widespread" malware attack on Department of Defense (DOD) computers. They believed the attack originated from Russia. These leaders also believed the attack, "posed unusual concern among commanders and raised potential implications for national security."[1] Why? The attack affected DOD computers in Iraq, Afghanistan, and at United States Central Command (USCENTCOM). USCENTCOM is the headquarters overseeing US involvement in both countries. Additionally, the attack penetrated a classified network.[2] In short, the attack, believed to have originated in Russia, had an impact on US military operations in Iraq and Afghanistan. The impact was severe enough to warrant briefing the US President. Why is this event significant and how can the US prevent future cyber attacks?

Problem Background and Significance

In accordance with *The National Strategy to Secure Cyberspace*, "The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace."[3] This dependence leads to vulnerability. A successful attack on cyberspace can have a tremendous impact on America, including disruption of critical government and defense operations, loss of revenue, and loss of life. The strategy goes on to identify the primary concern as "organized cyber attacks."[4] Accordingly, the national strategy lists, "Prevent cyber attacks against America's critical infrastructures"[5] as a strategic objective. How should the US prevent cyber attacks?

Looking again to *The National Strategy to Secure Cyberspace*, a possible answer is provided. The strategy states, "deter those with the capabilities and intent to harm our critical infrastructures."[6] What is deterrence? In accordance with Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, deterrence is, "The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction."[7] Since deterrence is a state of mind, one must understand the mind of the actor who would organize a cyber attack. In general, this adversary can be a state or non-state actor. Since deterring one may not deter the other, the scope of this research will be limited to state actors only.

How do you deter a state actor in cyberspace? This research will use a parallel historical case study. Since the end result of deterrence is a "threat of unacceptable counteraction," this research will assess the feasibility of adopting the nuclear mutually assured destruction (MAD) doctrine of the Cold War. In other words, if America adopts a MAD doctrine for cyberspace (CyberMAD), will it deter potential state adversaries? This research aims to answer that question.

It is expected that this research will provide the warfighter with a credible doctrine to contribute to one of America's strategic cyberspace objectives: preventing a cyber attack by an adversarial state. Once the doctrine is accepted, it will allow warfighters to focus scarce resources on areas that will strengthen the doctrines' credibility. On the other hand, the answer to the research question may be no. If this is the result, it is expected that this research will provide insights into what will or will not deter state actors from attacking America. Again, this will allow warfighters to focus their efforts in the area of cyberspace deterrence.

Research Question

Should the US adopt a mutually assured destruction doctrine for cyberspace?

Research Argument

The US should adopt a CyberMAD doctrine to deter adversary states. Why? First, the US economy and national security are fully dependent upon cyberspace. Second, as evidenced by the recent global economic crisis, globalization has led to economic interdependence. This interdependence is enabled by cyberspace. Therefore, similar to a nuclear weapons exchange, the loss of cyberspace would be devastating to not only the US, but also most other states. The nuclear MAD doctrine is credited with preventing the Cold War from turning hot, since neither side could expect to survive a full scale nuclear exchange. Although the loss of cyberspace might not rise to this level, the doctrine still applies. If the US can credibly vow to destroy cyberspace, thus destroying world economies, the US can deter an adversary from launching an attack. Critics may correctly argue that CyberMAD's deterrent effect is limited, since it will not deter non-state actors. However, nuclear MAD doctrine never deterred non-state actors. Critics will also argue that the lack of attribution will limit CyberMAD. Although true, it allows us to focus on developing the capability. We should not throw out the doctrine. We should develop the capability.

Background

Cyberspace Defined

What is cyberspace? Asking multiple people to answer this question will result in multiple answers, all of which will be slightly different. As a starting point, author William Gibson is credited with coining the term cyberspace in an early 1980's novel. He used the term to describe "the network of computers through which the characters in his futuristic novels travel."[8] As another example, *The National Strategy to Secure Cyberspace* states, "Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work."[9] Finally, DOD's definition for cyberspace is "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."[10] Although the definition is bound to continually change as cyberspace is further explored, this research paper will keep with the DOD definition provided above.

Cyberspace's Importance to US National Security

Although it is difficult to quantify how important cyberspace is to US national security, cyberspace's importance can be demonstrated through examples. In accordance with *The National Strategy to Secure Cyberspace*, America depends on cyberspace for military, government, and business operations.[11] For military operations, a recent event directly highlights DOD's dependence on cyberspace. Discussed in the introductory section, the event was a cyber attack on USCENTCOM and US forces operating in Iraq and Afghanistan. The impact was severe enough to warrant briefing the US President. Also in the introductory section,

the US government's dependence was noted. The US President acknowledged the importance of cyberspace to US national security by signing *The National Strategy to Secure Cyberspace* in 2003. Furthermore, *The National Strategy to Secure Cyberspace* directly states that cyberspace is essential to US national security and that, "recent events have highlighted the existence of cyberspace vulnerabilities and the fact that malicious actors seek to exploit them."[12] As for business operations, senior DOD officials have acknowledged that "80 percent of U.S. commerce goes through the Internet."[13] The three examples above provide a sense of how important cyberspace is to US national security, but is cyberspace important to the rest of the world, or only the US?

Cyberspace's Importance to Other States

A global state-by-state analysis is not included as part of this research project; however, the assumption is made that a majority of the world's states are either directly or indirectly dependent upon cyberspace. Furthermore, it is assumed that some of the world's states are more dependent than others. Again, this is hard to quantify, but several examples will be provided as evidence of this dependence.

First, is an acknowledgement by The President of the United States. According to *The National Strategy to Secure Cyberspace*, "The United States and world economy increasingly depend upon global markets and multinational corporations connected via information networks."[14] This statement provides an example of how cyberspace is growing in importance to the world economy.

Beyond an acknowledgement by the US President, an indication of world state dependence on cyberspace comes from comScore, a global Internet information provider. In a December 2008 press release, the company stated that China surpassed the US as the "largest

online audience in the world."[15] The US Department of Commerce states that over three percent of US retail sales occur over the Internet. In the third quarter of 2008, this equated to over 34 billion dollars.[16] In comparison, China Tech News reported that "Chinese Internet auction and e-commerce website Taobao.com has announced that its trade value in 2008 reached CNY99.96 billion, making it one of the largest comprehensive shopping platforms in China." This was an increase of 131 percent over 2007.[17] China's business dependence on cyberspace may not be as great as the US's, but this example shows that China's dependence is rapidly increasing. Are there examples beyond US and Chinese cyberspace dependence?

A third example comes from the cyber attacks on the countries of Estonia and Georgia. The 2007 attack on Estonia was hailed as, "the first known incidence of such an assault on a state."[18] The attack, believed to have originated in Russia, impacted Estonia's government, press, economy, and businesses.[19] In 2008, a similar attack was launched against the country of Georgia. Again, believed to have originated in Russia, the cyber attack affected the Georgian government and business sectors.[20] Why is this significant? In world gross domestic product, The World Bank, in 2007, reported that Estonia was ranked 86 out of 185 and Georgia was ranked 115 out of 185[21] As can be seen, both countries are ranked around the middle of the world; however, both suffered impacts due to cyber attacks.

A fourth example provides evidence that the world's states are also indirectly dependent on cyberspace. The example is the current world economic crisis. Although the crisis affects some states more than others, there is no doubt that it is affecting most states. In a recent Foreign Affairs article, Roger Altman discussed how the crisis was the "worst in over 75 years."[22] In the article, he discussed how China may "suffer a lesser blow," but goes on to state that China will suffer some pain.[23] Additionally, he states, "Much of the rest of the world,

however, has been hard hit by the crisis."[24] Even if states do not directly depend on cyberspace, they do depend on the world economy and the world economy depends on cyberspace.

The President of the United States has acknowledged that the US and world economy dependence on cyberspace. Is he right? Chinese economic dependence on cyberspace continues to grow. Two countries, in the middle to lower half of world's gross domestic product, felt the impact of cyber attacks to government and business. Finally, the world's economies are linked. Although states vary in direct dependence on cyberspace, they are all dependent on the world economy and the world economy is dependent on cyberspace. As can be seen from the above examples, the world's states are either directly or indirectly dependent on cyberspace.

Cyberspace Threats

It has been established that the US and the world's states, directly or indirectly, are dependent on cyberspace; however, dependence is only bad if there is a threat. What are the threats to cyberspace? The threats range from state actors to non-state actors. According to the US Computer Emergency Readiness Team, cyber threats include national governments, terrorists, industrial spies, organized crime groups, and hackers.[25] As stated in *The National Strategy to Secure Cyberspace*, the actors' intent and full capabilities are not known, but the "tools and methodologies" are known and are becoming increasingly sophisticated.[26] Is this correct?

In 1979, engineers developed the first computer "worm." The worm was designed for peaceful purposes and is considered the "ancestor of modern worms – destructive computer viruses that alter or erase data on computers, often leaving files irretrievably corrupted."[27] Seven years later, one of the first personal computer viruses was created by a programmer in Pakistan.[28] In 2002, the largest ever denial-of-service attack was launched against the Internet. Although the

Internet survived the attack, it called into question the security of the Internet.[29] As discussed above, Russia was accused of launching a denial-of-service attack against Estonia in 2007. A year later, Russia was accused of launching a denial-of-service attack against Georgia. Similar to the Estonia attack, the impact to Georgia was significant.[30] From 1979 to 2008, cyberspace threats mutated peaceful endeavors into, what appears to be, state on state cyberspace attacks. It's hard not to notice the trend.

Finally, *The National Strategy to Secure Cyberspace* states that organized cyber attacks "capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security" are the main threat to the US.[31] Additionally, the strategy states that a great deal of technical sophistication is necessary to launch this type of attack.[32] In other words, the greatest threat to the US is from technically sophisticated and organized actors. Although hackers, organized crime groups, and terrorists potentially fit this description, the most likely actor will be the one with the greatest resources. A state actor fits the bill. In fact, in a 2008 DOD report to the US Congress, *Military Power of the People's Republic of China*, states, "In the past year, numerous computer networks around the world, including those owned by the U.S. Government, were subject to intrusions that appear to have originated within the PRC. These intrusions require many of the skills and capabilities that would also be required for computer network attack. Although it is unclear if these intrusions were conducted by, or with the endorsement of, the PLA or other elements of the PRC government, developing capabilities for cyberwarfare is consistent with authoritative PLA writings on this subject."[33] As far as state actors are concerned, it appears China can be added to the list with Russia.

Scope of Research

The scope of this research is limited to a theoretical exploration of the US adopting a cyber mutually assured destruction strategy for deterrence. The US adoption of the nuclear mutually assured destruction strategy of the 1960s is used as a historical parallel case study to develop the theoretical cyber mutually assured destruction strategy; however, four points need to be addressed in order to scope the research.

To begin, the purpose of this research is not to determine if deterrence is effective or if the US nuclear mutually assured destruction strategy of the 1960s was effective. Numerous noteworthy authors, such as Lawrence Freedman, have examined these issues in depth. The results of the examinations are mixed. Since this research does not aim to answer these questions, two assumptions are made. First, the assumption is made that deterrence, if properly implemented, is effective. Second, the assumption is made that the US nuclear mutually assured destruction strategy was effective at deterring the Soviet Union and keeping the Cold War cold.

Second, potential threats to cyberspace are numerous; however, they can be classified into state and non-state actors. A strategy aimed at deterring one may not deter the other. Since US nuclear deterrent strategies were aimed at state actors, most notably the former Soviet Union, this research is limited to examining a theoretical cyberspace deterrence strategy aimed at state actors. As such, this research is not intended to address the cyber deterrence of terrorists, hackers, organized criminal groups, or actors hired as proxies by a state.

Third, this research will not examine the issue of attribution. It is acknowledged that an error free cyberspace attribution capability does not exist; however, this research assumes that the US does have the capability to attribute cyberspace attacks to a specific state or non-state actor.

Fourth, this research does not examine the policy issue of execution thresholds. As with the nuclear mutually assured destruction strategy, the US will need to define when an opponent has crossed the cyber mutually assured destruction threshold. The US will need to send a clear message as to what actions will trigger retaliation by the US.

In summary, the scope of this research is limited to a theoretical exploration of the US adopting a cyber mutually assured destruction strategy for state actor deterrence based on the US nuclear mutually assured destruction doctrine of the 1960s. Assumptions have been made that deterrence is effective, the nuclear mutually assured destruction strategy of the 1960s was effective, the US has the capability to attribute cyberspace attacks to specific states and non-state actors, and that policy makers will determine execution thresholds.

Deterrence

Deterrence Defined

What is deterrence? In accordance with Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, deterrence is, "The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction."[34] This definition is in line with the deterrence definition of author Lawrence Freedman. In his book *Deterrence*, he states, "deterrence is concerned with deliberate attempts to manipulate the behavior of others through conditional threats."[35] Combining the two definitions, deterrence is a deliberate attempt to cause an adversary not to act through the use of credible and conditional threats that an adversary believes to be unacceptable. In the context of this research paper, this is the definition for the term deterrence. Now that deterrence has been defined, how does one know it is working?

Deterrence Effectiveness Criteria

In order to determine deterrence effectiveness criteria, the assumption is made that deterrence actually works. As author Colin Gray stated, "There is absolutely no way in which the success of deterrence can be assured, ensured, or guaranteed."[36] The reason for Gray's statement is that the adversary gets to decide if they are deterred; however, with the assumption that deterrence does work, how can its effectiveness be measured? As stated earlier, deterrence hinges on the existence of a credible threat. Credibility is the key word. How does an actor achieve deterrence credibility? Gray lists some attributes that enhance the deterrence effect. They are, "impressive capabilities, a track record of promises kept, a steadiness and clarity in policy statement, and so forth."[37] Additionally, Peter Jakobsen appears to agree. In his article *Reinterpreting Western Use of Coercion in Bosnia-Herzegovina: Assurances and Carrots Were*

Crucial, he states that threat credibility "depends on capability and will."[38] Although the case study is not relevant to this research, the author's understanding of a credible threat substantiates Gray's. Jakobsen reached his conclusions by analyzing when coercion and deterrence worked and when they didn't. Gray's and Jakobsen's terminology are not the same, but Gray's attributes of "a track record of promises kept" and "a steadiness and clarity in policy statement" are what Jakobsen describes as "will." The final criterion that needs to be added to this discussion is from the DOD definition of deterrence. That criterion, as stated in the definition, is "fear of the consequences." In the context of this research paper, capability, will, and fear, will be used as the criteria to measure deterrence effectiveness. Each will briefly be discussed.

First is capability. A threat that cannot be fulfilled will not deter. Therefore, an actor wishing to deter another has two options. First, they can develop the capability and demonstrate it to their opponent. It must exist and be known. Second, since deterrence is a state of mind, an actor wishing to deter may deceive their opponent by creating the perception that the capability does exist.

Second is will. The target of deterrence must believe that their opponent has the will to carry through on the threat. As Jakobsen states, "A coercer with a capacity to implement his threat must also signal his willingness to do so. The key to success is to convince the opponent that the threat will be executed automatically if compliance is not forthcoming."[39] Although Jakobsen is referring to coercion, the same holds true for deterrence. In other words, the target of deterrence must perceive that their opponent has the will to follow through on the threat.

Third is fear. As the DOD definition of deterrence alludes to, the target of deterrence must fear the consequences of the communicated threat. As Jokobsen discusses, "The aim is to influence the intentions of the opponent by convincing him that it would be too costly to resist

the coercer's demands."[40] In other words, the opponent must value what is threatened. If not, deterrence will not work.

In summary, the assumption is made that deterrence works. Additionally, three criteria will be used to measure the effectiveness of deterrence. The first criterion is capability. The capability must exist, or exist in the mind of the opponent, to execute the threat. Second is will. The opponent must believe that the actor issuing the threat has the will to carry through on the threat. Finally, is fear. The opponent must fear the threat or value what is being threatened.

Nuclear Mutually Assured Destruction versus Cyber Mutually Assured Destruction

General Descriptions

Understanding cyberspace and deterrence, should the US adopt a mutually assured destruction doctrine for cyberspace? Why mutually assured destruction? In order to answer this question, a brief understanding of the development of nuclear mutually assured destruction (NuclearMAD) is necessary. What follows is a brief overview of NuclearMAD, followed by a theoretical overview of CyberMAD.

Nuclear Mutually Assured Destruction (NuclearMAD). How did NuclearMAD develop and what is it? In his book *Nuclear Deterrence – Does it Deter?*, Honoré Catudal chronicles the development of US nuclear deterrent strategies. US deterrent strategies began with city busting. Catudal describes the 1947 policy of city busting as, "Deterrence of attack on U.S. vital interests rests on drastic threat of atomic destruction. Supported by plans to use SAC bombers to destroy largest Soviet urban-industrial base."[41] In this quote, SAC is the US's Strategic Air Command. Of note, city busting developed as a strategy prior to the Soviet Union's development of a nuclear bomb in 1949.[42] Once the Soviets developed an atomic bomb, the nuclear race was on. Catudal notes that the US reaction was to begin development of a hydrogen bomb.[43] The Soviets quickly followed with development of their own hydrogen bomb.[44] The race for gaining or maintaining nuclear superiority continued until the mid-1960s. At this point, the US accepted Soviet parity and adopted the NuclearMAD strategy. Catudal describes NuclearMAD as, "Deterrence now rests on both sides to destroy each other after they have been attacked."[45] The US strategy was no longer based on a race for superiority, but an acceptance of the fact that a nuclear exchange would devastate both states, regardless of who struck first.

Cyber Mutually Assured Destruction (CyberMAD). Theoretically, CyberMAD is based on two ideas. First, the US does not have superiority in cyberspace. Why? The US does not control cyberspace. In fact, no state can. As discussed early in this paper, cyberspace is a global domain. Additionally, *The National Strategy to Secure Cyberspace* acknowledges that governments control only a small portion of their critical cyberspace infrastructure.[46] Cyberspace parity is a result of the fact that no state can achieve superiority. Second, the impact of cyberspace attacks has reached a critical point. As noted above, the US and the world's states, are dependent on cyberspace. Additionally, threats to cyberspace are increasing in sophistication and impact. Although the level of damage caused by current cyberspace attacks may not rise to the level of a nuclear exchange, they do have the potential to cause great harm to the world's governments, economies, and militaries. Up to now, the US has primarily focused on defense. A theoretical CyberMAD is based on offense, but how should the US develop a credible CyberMAD strategy?

Strategy Comparison versus Deterrence Criteria

In order to develop a theoretical CyberMAD strategy, an analysis of NuclearMAD will be presented according to the deterrence criteria outlined above. This analysis will provide a case study for what the CyberMAD strategy should contain in order to provide a credible deterrent effect. To recap, three criteria will be used to measure the effectiveness of deterrence. The first criterion is capability. The capability must exist, or exist in the mind of the opponent, to execute the threat. Second is will. The opponent must believe that the actor issuing the threat has the will to carry through on the threat. Finally, fear. The opponent must fear the threat or value what is being threatened.

Criteria One – Capability. As stated above, the capability must exist, or exist in the mind of the opponent, to execute the threat. Did the US have the capability to follow through on the NuclearMAD threat?

For the purpose of this discussion, the exact quantities of warheads and delivery mechanism are not necessary. The threat was assured destruction, even after a first strike by the Soviet Union. In other words, the US needed to have the capability to retaliate, as well as destroy, the Soviet Union even if the Soviet Union launched a nuclear first strike. This second strike capability is the mutual component of the term mutually assured destruction. Therefore, two components are necessary. First, the US must possess the capability to destroy the Soviets through the use of nuclear weapons. A technological breakthrough that added to the credibility of the threat was the hydrogen bomb. Catudal noted the breakthrough while discussing the hydrogen bomb. He states, "As a result of the discovery of the fusion bomb, a *single* modern strategic nuclear weapon could have a million times the yield of the high explosive strategic bombs of World War II or one hundred to a thousand times the yield of the atomic bombs that destroyed Hiroshima and Nagasaki, killing some 250,000 people."[47] Furthermore, Freedman notes that US strategic planners, in 1968, knew that the US could destroy 50 percent of the Soviet population and almost 80 percent of Soviet industry; however, the destruction of only 20 percent of the population and 50 percent of industry was thought to be adequate to assure the destruction of the Soviet Union.[48] In other words, the US did not need to completely annihilate 100 percent of the Soviet's population and industry. A lesser percent would suffice, and the US's nuclear arsenal could exceed that lesser percent. Second, the capability must be able to survive and retaliate a first strike initiated by the Soviets. What drove the US to desire a second strike capability? The Soviet launch of Sputnik, an artificial satellite in 1957, was the

beginning.[49] Following the launch, the US discovered that the Soviets had tested an intercontinental ballistic missile (ICBM). As ICBM technology matured, the Soviets could hit US targets within 30 minutes of launch.[50] The US needed to respond. They did so by ordering that US bombers, armed with nuclear weapons, would remain airborne at all times, ready to attack the Soviets.[51] This policy eventually matured into the nuclear triad concept. The US would have land, air, and maritime based nuclear weapons at the ready. As can be seen, the US did possess the capability to assure destruction, even after a first strike.

Using the above analysis as a parallel case study, in order for CyberMAD's capability to be credible, CyberMAD must be able to assure destruction of cyberspace with a second strike component. Does the US possess this capability? The US can certainly choose to employ its nuclear arsenal to destroy cyberspace. Additionally, the US can employ its conventional military instrument of power. For example, the US can kinetically attack key cyber nodes throughout the world. Attacking these key nodes could potentially destroy cyberspace. For a non-kinetic approach, the US could use directed energy or electro-magnetic pulse weapons. As with the conventional example above, these weapons could be developed and used to non-kinetically destroy key cyber nodes. What about cyberspace weapons? Does the US have the capability to destroy cyberspace through the use of cyberspace weapons? At this point in time, it is unknown if the US has this capability, thus three possibilities exist. If the US possesses the capability, they can demonstrate it. If not, the US can develop it. Finally, the US can work on deceiving the world into believing the capability exists. How hard would it be to develop the capability? The answer to that question is unknown; however, a clue was provided by an attack on cyberspace in 2002. According to Krebs, "A denial-of-service attack hits all 13 of the 'root' servers that provide the primary roadmap for almost all Internet communications."[52] Although Internet

safeguards prevented major impacts, Krebs notes that the event raised questions about the security of the Internet's core infrastructure.[53] What about second strike capability? Since this is a theoretical concept, the US would need to develop a second strike capability. The development can mirror the nuclear triad concept with cyberspace attack capabilities physically located in the air, maritime, and land domains; however, the capability could take on a new form within the cyberspace domain.

Criteria Two – Will. For the second criteria, the opponent must believe that the actor issuing the threat has the will to carry through on the threat. Did the US effectively communicate the NuclearMAD threat to the Soviets?

To begin, the US did attempt to communicate its will to the Soviets. As Freedman states, while describing the US's attempt to communicate its will to the Soviets, "The annual posture statements were written with great care and meant to be read with equal care by both allies and adversaries."[54] Furthermore, he notes that it was very important to the US administration to communicate a clear and unambiguous message to the Soviets.[55] Although the US attempted to clearly articulate that they had the will to carry through on the threat, there is a better question to ask. How well did the Soviets receive the message? This is a better question to ask since deterrence is a state of mind. The opponent gets to decide if they are deterred or not. One example of how the message was received by the Soviets is based on the Soviet reaction to it. Catudal notes, while describing the strategy's critics' reactions, "the Soviets are vehemently opposed to such a strategy which would, in effect, make the U.S.S.R. dependent on the goodwill and designs of the United States."[56] Furthermore, in Catudal's description of the Soviet views on deterrence, he focuses on whether or not the Soviets accepted the US NuclearMAD deterrence

strategy.[57] In order to accept or reject the policy, it can be assumed that the Soviets did receive and understand the message. They didn't need to like it.

Again, using the above example, to increase the effectiveness of CyberMAD's deterrence effect, the US will need to send clear and unambiguous messages to state actors. They must clearly articulate that the US will destroy cyberspace if an actor decides to disrupt US government, business, or military capabilities. Of course, the US must also clearly articulate tolerance thresholds. As *The National Strategy to Secure Cyberspace* discusses, US opponents may only conduct cyberspace espionage activities; however, those activities may be in preparation for a severe cyberspace attack against the US.[58] In other words, the US must articulate what constitutes a cyberspace attack and how severe it must be before the US responds by destroying all of cyberspace. Beyond tolerance thresholds, the US must also articulate the state versus non-state actor issue. State actors may use non-state actors as proxies to conduct cyberspace warfare against the US. In fact, *The National Strategy to Secure Cyberspace* states, "The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all."[59] Maybe absolute attribution is not necessary. In parallel with the *National Strategy for Combating Terrorism*, one of the US's short-term priorities for action is to, "Deny terrorists control of any nation they would use as a base and launching pad for terror."[60] The US can adopt a less than 100 percent attribution policy. The state may not be directly responsible, but actors within that state are. If it is known that the US will destroy cyberspace regardless of whether the attacker is a state or not, it might encourage legitimate states to police their own borders. The key point is that that US must make it known that they are willing to destroy cyberspace if the

pain becomes too intense. Beyond developing the capability and articulating its willingness to execute the threat, the US must also create fear.

Criteria – Fear. The last criterion is fear. Does the opponent fear the threat or value what is being threatened? In other words, one can have the capability to execute the threat and have clearly communicated the threat to their opponent, but their opponent may not care.

Did the Soviets value what was threatened? To begin, the US was threatening the survival of the Soviet Union. As stated above, the US believed destroying 20 percent of the population and 50 percent of industry would accomplish the task. At one point, the US estimated it could destroy 50 percent of the population and 80 percent of industry. Three points are presented to show that the Soviet Union feared the threat of state survival. First, is the Soviet Union's entry into a nuclear arms race with the US. If the Soviets were not fearful, why did they feel a need to achieve parity or even superiority in the nuclear arena? It started with the atomic bomb, then the hydrogen bomb. From there the race became one of numbers and delivery mechanism, only to end in a stalemate. The Soviets feared the potential of these new weapons and sought to acquire them for their own use. The second point is the signing of the Anti-Ballistic Missile Treaty in 1972. Catudal notes that the treaty was an accepted "state of mutual vulnerability" between the US and the Soviets. Each state would hold the other hostage.[61] If the Soviets did not fear the exchange of nuclear weapons, why did they sign the treaty? Finally, the Cuban Missile Crisis provides another example of Soviet fear. In 1962, Nikita Khrushchev, the Soviet Union's Premier, made the decision to position short range nuclear missiles in Cuba.[62] His decision led the US and Soviets to the brink of nuclear war. Although the crisis was resolved, an indication of Soviet fear was later provided by Khrushchev in his memoirs. During the crisis, he suggested that he and some government officials go to the opera. He wrote in his

memoirs, “I suggested to other members of government: ‘Comrades, let’s go to the Bolshoi Theater this evening. Our own people as well as foreign eyes will notice, and perhaps, it will calm them down. They’ll say to themselves if Khrushchev and our other leaders are able to go to the opera, at a time like this, then at least tonight we can sleep peacefully.’ We are trying to disguise our own anxiety, which was intense.”[63] Khrushchev’s statement shows that the Soviet Union did fear the threat of US nuclear weapons employment. These three points show that the Soviets accepted the threat, countered it, and entered into the mutually assured destruction strategy.

Fear is the reason a CyberMAD doctrine is best targeted towards state actors. Looking at the cyberspace threat actors, states have the most to lose from a CyberMAD strategic doctrine. Non-state actors, such as terrorists, industrial spies, organized crime groups, and hackers, may have nothing to lose. In fact, the anarchy caused by the destruction of cyberspace may assist these actors. As discussed earlier, both the US and other states, directly or indirectly, depend on cyberspace. For some states, such as the US, government, military, and business operations would be devastated. Other countries may not directly suffer the same devastation, but they will suffer. Will they fear CyberMAD? A rational person may answer yes; however, as discussed above, deterrence cannot be guaranteed. Why? Deterrence is a state of mind. The opponent gets to decide if they are deterred or not. If the US does adopt CyberMAD, the US must also articulate the impact to the world should the US execute CyberMAD. As with NuclearMAD and the Soviet Union, the world’s states must fear the threat of cyberspace destruction. If they don’t, the strategy will not work.

In summary, if the US adopts CyberMAD, the US should develop the strategy based on the lessons learned from NuclearMAD in order to provide a credible deterrent effect. The

strategy should contain the three criteria of capability, will, and fear. The capability must exist, or exist in the mind of the opponent, to execute the threat. The opponent must believe that the US has the will to carry through on the threat. Finally, the opponent must fear the threat or value what is being threatened.

Conclusion

Conclusions

Should the US adopt a mutually assured destruction doctrine for cyberspace? In order to answer the question, this research needed to prove three points. It had to prove how important cyberspace is to the US, how important it is to the world, and how threats to cyberspace are growing in intensity and impact. In other words, it had to show that the destruction of cyberspace is feasible, and that the consequences of the destruction of cyberspace would be unbearable for the US and the world. Did the research prove these three points?

To begin, this research has shown that cyberspace is important to US national security. *The National Security Strategy to Secure Cyberspace*, a document signed by the US President, has shown how important cyberspace is to US military, government, and business operations. A recent attack impacted military operations in Iraq and Afghanistan. Additionally, 80 percent of US commerce operates over the Internet. In 2008, this equated to 34 billion dollars.

Second, this research has shown that cyberspace is important to other states. Directly or indirectly all states are dependent on cyberspace. *The National Security Strategy to Secure Cyberspace* highlights this importance. States' dependence on cyberspace is increasing. Chinese e-commerce, in one company, increased over 100 percent from 2007 to 2008. Two countries, ranked in the mid to lower half of world gross domestic product, have suffered from cyberspace attacks. Furthermore, the current world economic crisis has shown how interdependent state governments are on cyberspace.

Third, this research has shown that threats to cyberspace have increased in number and impact. What started as a peaceful endeavor has mutated into a malicious endeavor. The sheer number of attacks has increased. The impact of the attacks has increased. Finally, the trend

appears to indicate movement from non-state actors to state actors. In conclusion, this dependence on cyberspace has created vulnerability. The increases in the number and impact of cyberspace attacks have reached an unacceptable point.

The research has shown that the destruction of cyberspace is feasible, and that the consequences of the destruction of cyberspace would be unbearable for the US and the world. Beyond a doubt, the US must find a solution. The solution can be defensive in nature. It can also be offensive in nature. Should the US adopt a mutually assured destruction doctrine for cyberspace? Although this research paper focused on a cyberspace capability to back the doctrine, the US does have the capability to execute the CyberMAD threat. The US can use NuclearMAD's capabilities to carry it out or the US can use conventional kinetic and non-kinetic capabilities to carry it out. It is unknown, at this time, whether the US can carry it out through cyberspace alone, but the US can carry it out. Therefore, the question is probably better answered by politicians. As with NuclearMAD, they'll be the ones to answer the tough questions. Does deterrence work? Did the NuclearMAD strategy of the 1960s deter the Soviet Union? Is the impact of CyberMAD's destruction acceptable or is it immoral? If it is acceptable, when will the US pull the trigger? In the context of this research paper, the question cannot be answered, but the capability does exist. With this said, if the US does chose to pursue a CyberMAD strategy, several recommendations are offered.

Recommendations

If US policy makers choose to adopt a CyberMAD strategy, several recommendations are offered. These recommendations are designed to increase the effectiveness of the deterrent strategy.

Recommendation One. The capability must exist. Although politicians will decide what the execution threshold is and what the threat response is, the US will need to ensure it has the capability to execute the threat or to deceive its potential adversaries. Additionally, it must be able to withstand and retaliate against a first strike by an adversary. The capability can be nuclear, kinetic, or non-kinetic.

Recommendation Two. The US must clearly articulate its willingness to carry through on the threat. As with NuclearMAD, great care must be taken to communicate the message. The message must also articulate what the execution threshold is and what the response will be.

Recommendation Three. The US must ensure that what is threatened is valuable to the opponent. Today, the US is likely to suffer more than others; however, globalization has led to economic interdependence. Other states may not suffer directly, at least not as much as the US, but they would suffer through indirect effects. The US must ensure they target this strategy at appropriate actors. Non-state actors may not fear the destruction of cyberspace. In fact, some may welcome it.

Recommendation Four. The US must determine how to deter non-state actors. As alluded to in the third recommendation, CyberMAD is directed toward state actors; however, non-state actors must also be deterred. These actors can range from terrorist groups to organized crime. This leads to the fifth and final recommendation.

Recommendation Five. The US must continue work on attributing cyberspace attacks to the appropriate actors. As stated above, the US can lower the standard for attribution, but ultimately, the US will desire a 100 percent attribution capability. Achieving this capability will allow the US to avoid executing CyberMAD erroneously. A non-state actor, disguised as a state

actor, may attempt to provoke the US to execute the strategy. Perfect attribution can potentially avoid such a scenario.

Final Thoughts

Regardless of the strategy the US chooses, one item is clear. The US can either choose to defend, or to defend and deter. The first option is purely defensive in nature. As can be seen from the research, it is not working. The second is defensive and offensive in nature. It may work. The US already has the capability to destroy cyberspace, but does it have the will? Politicians will need to answer this question.

Notes

[1] Barns, "Cyber Attack", 1.
[2] Ibid., 1.
[3] President, *National Strategy to Secure Cyberspace*, iii.
[4] Ibid., viii.
[5] Ibid., viii.
[6] Ibid., ix.
[7] JP 1-02, *Military and Associated Terms*, 162.
[8] Krebs, "History of Computer Viruses and Attacks", 2.
[9] President, *National Strategy to Secure Cyberspace*, vii.
[10] JP 1-02, *Military and Associated Terms*, 141.
[11] President, *National Strategy to Secure Cyberspace*, iii.
[12] Ibid., 1.
[13] Doyle, "Elevate Status of Cyberspace Command", 1.
[14] President, *National Strategy to Secure Cyberspace*, 51.
[15] comScore, "Global Internet Audience," 1.
[16] US Census Bureau, "Quarterly U.S. Retail Sales," 1.
[17] China Tech News, "Taobao.com Trade Value," 1.
[18] Traynor, "Russia Accused of Cyberwar", 1.
[19] Ibid., 1.
[20] Danchev, "Russia vs Georgia Cyber Attack", 1.
[21] World Bank, "World Development Indicators," 1.
[22] Altman, "The Great Crash, 2008", 2.
[23] Ibid., 11.
[24] Ibid., 13.
[25] US Computer Emergency Readiness Team, "Cyber Threat Source Descriptions," 1.
[26] President, *National Strategy to Secure Cyberspace*, 6.
[27] Krebs, "History of Computer Viruses and Attacks", 2.
[28] Ibid., 2.
[29] Ibid., 3.
[30] Danchev, "Russia vs Georgia Cyber Attack", 1.
[31] President, *National Strategy to Secure Cyberspace*, viii.
[32] Ibid., viii.
[33] DOD, *China Military Report*, 3-4.

[34] JP 1-02, *Military and Associated Terms*, 162.
[35] Freedman, *Deterrence*, 6.
[36] Gray, "Deterrence in the 21st Century", 176.
[37] Ibid., 177.
[38] Jakobsen, "Assurances and Carrots", 4.
[39] Ibid., 4.
[40] Ibid., 3.
[41] Catudal, *Nuclear Deterrence – Does it Deter?*, 14.
[42] Freedman, *Evolution of Nuclear Strategy*, 60.
[43] Catudal, *Nuclear Deterrence – Does it Deter?*, 90.
[44] Ibid., 91.
[45] Ibid., 17.
[46] President, *National Strategy to Secure Cyberspace*, xii.
[47] Catudal, *Nuclear Deterrence – Does it Deter?*, 91.
[48] Freedman, *Evolution of Nuclear Strategy*, 234.
[49] Catudal, *Nuclear Deterrence – Does it Deter?*, 132.
[50] Ibid., 134.
[51] Ibid., 135.
[52] Krebs, "History of Computer Viruses and Attacks", 3.
[53] Ibid., 3.
[54] Freedman, *Evolution of Nuclear Strategy*, 235.
[55] Ibid., 235.
[56] Catudal, *Nuclear Deterrence – Does it Deter?*, 145.
[57] Ibid., 145.
[58] President, *National Strategy to Secure Cyberspace*, viii.
[59] Ibid., viii.
[60] President, *National Strategy for Combating Terrorism*, 16.
[61] Catudal, *Nuclear Deterrence – Does it Deter?*, 146.
[62] Ibid., 463.
[63] Ibid., 480.

Bibliography

Altman, Roger C. "The Great Crash 2008: A Geopolitical Setback for the West." *Foreign Affairs* 88, no. 1 (January/February 2009): 2-14.

Barnes, Julian E. "Cyber-attack on Defense Department Computers Raises Concerns." *Los Angeles Times*, 28 November 2008. http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28 (accessed 31 January 2009).

Catudal, Honoré. *Nuclear Deterrence – Does it Deter?* Atlantic Highlands, N.J.: Humanities Press International, Inc., 1986.

China Tech News. "Taobao.com Trade Value Reached CNY99.96 Billion in 2008." http://www.chinatechnews.com/2009/01/15/8515-taobao-trade-value-reached-cny9996-billion-in-2008/ (accessed 25 March 2009).

comScore. "Global Internet Audience Surpasses 1 Billion Visitors, According to comScore." http://www.comscore.com/press/release.asp?press=2698 (accessed 25 March 2009).

Danchev, Dancho. "Coordinated Russia vs Georgia Cyber Attack in Progress." *ZDNET*, 11 August 2008. http://blogs.zdnet.com/security/?p=1670 (accessed 9 September 2008).

Doyle John M. "Air Force to Elevate Status of Cyberspace Command." *Aerospace Daily & Defense Report*, 22 March 2007. http://www.military-quotes.com/forum/300151-post.html (accessed 31 January 2009).

Freedman, Lawrence. *Deterrence*. Malden, MA: Polity Press, 2004.

Freedman, Lawrence. *The Evolution of Nuclear Strategy*. New York, NY: Palgrave MacMillan, 2003.

Gray, Colin. "Deterrence in the 21st Century." In *Applied Warfare Course* coursebook, edited by Sharon McBride, 175-179. Maxwell AFB, AL: Air University Press, October 2008.

Jakobsen, Peter. "Reinterpreting Western Use of Coercion in Bosnia-Herzegovina: Assurances and Carrots Were Crucial." *The Journal of Strategic Studies* 23, no. 2 (June 2000): 1-22.

Joint Publication (JP) 1-02. Department of Defense Dictionary of Military and Associated Terms, 12 April 2001.

Krebs, Brian. "A Short History of Computer Viruses and Attacks." *The Washington Post*, 14 February 2005. http://www.washingtonpost.com/wp-dyn/articles/A50636-2002Jun26.html (accessed 9 September 2008).

Office of the President of the United States. *National Strategy for Combating Terrorism*. Washington, D.C. February 2006.

Office of the President of the United States. *The National Strategy to Secure Cyberspace*. Washington, D.C. February 2003.

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*, 17 May 2007. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (accessed 9 September 2008).

United States Census Bureau. "Estimated Quarterly U.S. Retail Sales: Total and E-commerce." http://www.census.gov/mrts/www/data/html/08Q3table1.html (accessed 25 March 2009).

United States Computer Emergency Readiness Team. "Cyber Threat Source Descriptions." http://www.us-cert.gov/control_systems/csthreats.html#nat (accessed 25 March 2009).

US Department of Defense. *Annual Report to Congress: Military Power of the People's Republic of China*. Washington, DC: Office of the Secretary of Defense, 2008.

World Bank. "World Development Indicators Database." http://siteresources.worldbank.org/DATASTATISTICS/Resources/GDP.pdf (accessed 25 March 2009).