


March 2015

Cyber Deterrence: Is a Deterrence Model Practical in Cyberspace?

Nathaniel Youd

United States Air Force, nathaniel.youd@edu.edu

Follow this and additional works at: <https://digitalcommons.unomaha.edu/spaceanddefense>

 Part of the [Asian Studies Commons](#), [Aviation and Space Education Commons](#), [Defense and Security Studies Commons](#), [Eastern European Studies Commons](#), [International Relations Commons](#), [Leadership Studies Commons](#), [Near and Middle Eastern Studies Commons](#), [Nuclear Engineering Commons](#), [Science and Technology Studies Commons](#), and the [Space Vehicles Commons](#)

Please take our feedback survey at: https://unomaha.az1.qualtrics.com/jfe/form/SV_8cchtFmpDyGfBLE

Recommended Citation

Youd, Nathaniel (2015) "Cyber Deterrence: Is a Deterrence Model Practical in Cyberspace?," *Space and Defense*: Vol. 8: No. 0, Article 7.

DOI: 10.32873/uno.dc.sd.08.01.1122

Available at: <https://digitalcommons.unomaha.edu/spaceanddefense/vol8/iss0/7>

This Article is brought to you for free and open access by DigitalCommons@UNO. It has been accepted for inclusion in Space and Defense by an authorized editor of DigitalCommons@UNO. For more information, please contact unodigitalcommons@unomaha.edu.

Cyber Deterrence: Is a Deterrence Model Practical in Cyberspace?

Nathaniel Youd

2014 Gen. Larry D. Welch Writing Award, USSTRATCOM, Junior Division

After reconsidering massive retaliation versus escalation dominance concepts from nuclear deterrence, escalation dominance, investing in capability to respond proportionally at each level of cyber attack, may be the most practical and effective military strategy for strengthening cyber deterrence.

The past several decades have revolutionized the way we communicate and how modern states wage war.¹ Today it is nearly impossible for most people around the world to go more than a few minutes without their lives being directly impacted by technology and information systems. From the moment a person wakes up to a digital alarm clock, turns on the news and coffee, and takes a shower, every aspect of their lives relies on technology in some way. The growth of the Internet of Things in the coming years will only increase the impact of technology on all aspects of daily life. The information technology revolution has not only influenced the lives of consumers and corporate America but has revolutionized the way wars are fought. The era of the general on the battlefield or the admiral at sea disconnected from higher leadership is gone.

Today a general is more likely to direct the war effort from an operations center surrounded by hundreds if not thousands of digital information streams, from satellite imagery, UAV footage, and information about every troop's digital location, down to real-time audio and video from individual soldiers on the battlefield. While this revolution in military affairs (RMA) and the strategic advantages it gives modern militaries is still fiercely debated, there is little doubt that it has a profound impact on the lethality of modern armed forces and their ability to conduct operations around the globe.

While the technological revolution has shaped modern life and war fighting, it has also created new vulnerabilities that did not exist in earlier conflicts. Although there is still a diverse academic debate about the potential impact and scope of cyber warfare, there is general agreement that a successful attack on information technology systems would have a profound effect on modern social, economic, and military capabilities. In 2012, Secretary of Defense Leon Panetta echoed the warning of several national security scholars when he suggested that a digital "Pearl Harbor" could serve as a wake-up call to the threats of cyberspace.²

It is difficult to quantify and evaluate the potential consequences large-scale cyber attacks could have on a modern state, but there is a growing consensus that such attacks would have a profound impact on daily life and severely limit modern war fighting capability. Academics, policy makers, and strategists agree that future wars will not be limited to conventional or nuclear forces but differ in their analyses of the effect cyber threats will have on information technology systems, as well as the appropriate tactical and strategic responses to mitigate such threats. Regardless of who is right, states must begin to adopt policies and strategies for dealing with cyber threats and even deterring aggression in cyberspace. One of the pressing questions in cyber strategy is how to effectively implement a deterrence strategy in the cyber domain. This paper will explore the practicality of cyber

¹ Nathaniel Youd, USAFA Class of '13, is a First Lieutenant in the United States Air Force and a recent graduate of the Columbia University School of International and Public Affairs. The views expressed here are his own.

² Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, Department of Defense Press Release, October 11, 2012.

deterrence and will focus on applying traditional deterrence concepts to the cyber domain.

The concept of cyber deterrence is based on the idea that a state or non-state actor can deter a cyber-attack through conventional or non-conventional means, whether through defensive measures, the threat of cyber counterattack, or the potential threat and use of conventional or even nuclear forces. Cyber deterrence is mostly based on prior theories of nuclear and conventional deterrence but faces unique challenges due to the unconventional nature of the cyber domain. The main challenges with cyber deterrence and the academic arguments posed focus on whether or not cyber deterrence should center on retaliation or prevention; the problems that exist with attribution; the debate about rational or proportional response; and the implications of conflict escalation from cyberspace to conventional conflict domains. Each of these issues presents unique challenges for dealing with cyber deterrence and implementing a capable, communicable, and credible cyber deterrence strategy.

DETERRENCE THEORY

In order to understand the applications of deterrence in the cyber domain, it is important to first understand the main concepts behind deterrence theory. These concepts, although most successfully applied to the use of nuclear weapons, have been debated for centuries and can be applicable to all war fighting domains and types. Clausewitz characterized all warfare as “politics by other means,”³ and Sun-Tzu claimed “the supreme art of war is to subdue the enemy without fighting.”⁴ While these classical war theorists wrote long before the advent of modern information technology systems or nuclear weapons, their ideas directly apply to deterrence theory.

The essence of deterrence is to raise the cost of fighting in order to “subdue the enemy without

³ Carl von Clausewitz, *On War*, Michael Howard and Peter Paret, eds. and trans. (Princeton, NJ: Princeton University Press, 1976).

⁴ Sun-Tzu, *The Art of Warfare*, Roger Ames, trans. (New York: Ballantine Books, 1993).

fighting.” Thomas Schelling’s seminal work on deterrence theory, *Arms and Influence*, summarized the core elements of deterrence by claiming that the power to hurt is bargaining power. These two elements – the power to hurt, and the power to bargain – can be applied to any conflict and are the basis of any successful deterrence strategy.⁵ Without either element, deterrence strategies cannot succeed.

The key strategies, requirements, and challenges were summarized and applied to cyberspace by Kenneth Geers in his 2010 article in *Computer Law and Security Review*. Geers argues that there are two ways to approach deterrence: one is denial, or the ability to prevent a potential adversary from obtaining capabilities, a more defensive strategy; the other is punishment, or the ability to make the consequences of a certain action so costly that the adversary will not undertake the action. Geers further describes Schelling’s three requirements of any successful deterrence strategy – capability, communication, and credibility – and applies them to denial and punishment strategies.⁶ Capability is the actor’s ability to prevent or punish an adversary; communication is accurately conveying that capability to the adversary; and credibility is whether the adversary believes the threat.⁷

Martin Libicki described the aims and methods of deterrence and discussed their application to the cyber domain in his RAND study, *Cyberdeterrence and Cyberwar*. He claims “the aim of deterrence is to create disincentives for starting or carrying out further hostile action. The target threatens to punish bad behavior but implicitly promises to withhold punishment if there are no bad acts or at least none that meet some threshold.”⁸ According to Libicki, effective

⁵ Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

⁶ Kenneth Geers, “The Challenge of Cyber Attack Deterrence,” *Computer Law & Security Review*, 26 no. 3 (2010), 298.

⁷ Schelling.

⁸ Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Project Air Force, 2009), 28.

punishment is a key part of an effective deterrence strategy.

James Lewis further expanded on the requirements of deterrence strategy, noting “the concept of deterrence rests on a series of assumptions about how potential opponents recognize, interpret and react to threats of retaliation. The fundamental assumption is that a correct interpretation by opponents will lead them to reject certain courses of action as too risky or too expensive.”⁹

For state actors these assumptions typically hold true. If it is assumed that a state is a rational actor, then for a deterrence strategy where one state communicates its capability to deny or punish an adversary in a credible manner, the adversary state will respond and bargain (so long as the threat is clearly communicated and credible). While this assumption holds true for state actors, it is difficult to apply to sub-state and non-state actors, as such actors typically focus on cyber crime and cyber terrorism, not state-versus-state cyber warfare. Therefore, the aim of this paper is to analyze the practicality of cyber deterrence on a state level. The paper will make no attempt to apply cyber deterrence to sub-state and non-state actors.

United States Air Force Major General Susan Helms, in her review of a large-scale deterrence exercise conducted by the Air Force, summarized some of the underlying problems with deterrence in any domain. She stated that deterrence must be planned and conducted before any hostilities occur or appear imminent, and that, “an effective deterrence strategy is not one that is defined by actions within one domain, or one area of responsibility, or one nation.”¹⁰ She also reinforced Geers and Lewis’s assertions that

deterrence “must not be invisible”¹¹ or that it must be communicated to the adversary that is being deterred.¹² General Helms also commented on the need for deterrence strategists to understand the adversary’s perspective and that effective deterrence strategies are continually evolving.

To be effective at the strategic level, deterrence must be viewed through the lens of how your adversary views the geopolitical world. Deterrence is not static; effective deterrence strategies will morph under conditions of crisis, and the level of uncertainty about your adversary’s decision process must be actively tracked and accounted for, or else you risk serious miscalculation and unexpected deterrence failure.¹³

Only by incorporating these elements can an effective deterrence strategy be formulated and successfully implemented in any domain.

Nuclear Deterrence

Although there are fundamental differences between nuclear, cyber, and other forms of deterrence, it is important to understand the context and application of nuclear deterrence in order to apply it to other domains. Nuclear deterrence represents the most widely researched and arguably the most successful implementation of deterrence theory in history and therefore demands careful analysis before attempting to establish a new deterrence strategy in cyberspace. Mike McConnell, the former director of the National Security Agency (NSA) and Director of National Intelligence (DNI) in a 2010 *Washington Post* article summarized some of the key elements of Cold War deterrence and attempted to relate

⁹ James A. Lewis, *Cross-Domain Deterrence and Credible Threats* (Washington, DC: Center for Strategic and International Studies, 2010), 1.

¹⁰ Susan J. Helms, “Schriever Wargame 2010: Thoughts on Deterrence in the Non-Kinetic Domain,” *High Frontier: The Journal for Space and Cyberspace Professionals* 7, no. 1 (November 2010), <http://www.afspc.af.mil/shared/media/document/AFD-101116-028.pdf> (accessed January 25, 2012), 12-13.

¹¹ General Helms’s claim holds true for most historical examples but fails to explain Israel’s nuclear weapons program and uncommunicated deterrence strategy. The Israeli program may provide a useful case study for future applications of cyber deterrence, where states are unable to communicate a credible threat without compromising their capability.

¹² *Ibid.*, 13.

¹³ *Ibid.*

them to cyber warfare. “During the Cold War, deterrence was based on a few key elements: attribution (understanding who attacked us), location (knowing where a strike came from), response (being able to respond, even if attacked first) and transparency (the enemy’s knowledge of our capability and intent to counter with massive force).”¹⁴ These same elements summarize the main requirements and weaknesses with cyber deterrence. Attribution and location are essential to any deterrence strategy, as are response capability, and transparency, but each of these elements present unique problems when applied to the cyber domain.

While there are many similarities between nuclear deterrence and cyber deterrence, there are several important differences that present unique challenges in the cyber domain. First, nuclear deterrence during the Cold War was not as simple as many outside observers believe in today’s post-Cold War world. There was a fierce debate between academia and policy makers, particularly during the 1950s and 1960s, about how to best implement a nuclear strategy. These discussions went through several evolutions of counter force versus counter value doctrine and eventually led to an American policy of assured destruction, which served as the basis for the theory of Mutually Assured Destruction.¹⁵

Second, nuclear deterrence typically relies on the use of nuclear weapons to deter another state from using nuclear weapons.¹⁶ While such a strategy was unpleasant and difficult to contemplate, it did not require an escalation in conflict. Once nuclear war began, it would theoretically be easier for a decision maker to respond in kind with nuclear retaliation. This assumption may not hold true in cyberspace. In order for states to retaliate against a cyber-aggressor they may need to resort to conventional attacks in order to maintain proportionality and limit the attacks’ effect, or if

¹⁴ Mike McConnell, “To Win the Cyber-War, Look to the Cold War,” *The Washington Post*, February 28, 2010.

¹⁵ Lawrence Freedman, *The Evolution of Nuclear Strategy*, Third Edition (New York: Palgrave Macmillan, 2003).

¹⁶ Helms, 13.

the initial aggressing state has little cyber infrastructure to hold at risk.

As the Department of Defense concluded in a working study on the ‘Essential Elements of a Deterrence Strategy for Cyberspace,’ “the best response to an attack through cyberspace in many cases will not involve a reciprocal attack back through cyberspace.”¹⁷ This assumption makes it difficult to apply conventional understanding of nuclear deterrence to cyberspace because it is hard to predict how decision makers will actually behave in critical moments of cyber warfare.

The third critical difference between nuclear deterrence and cyber deterrence is reflected in the fact that while nuclear deterrence strategy eventually led to the adoption of nuclear arms control measures and limitation treaties, it is unlikely that a similar international agreement on cyber disarmament will be reached. Nuclear deterrence only holds because most current nuclear powers declare their nuclear weapons capabilities and are assumed to behave rationally. Furthermore, the United States and Russia have signed several treaties limiting the development and deployment of nuclear weapons in order to maintain peace and stability in the hope of avoiding war. These treaties form the basis for various confidence building measures between states that help limit the likelihood of miscommunication and inadvertent escalations.

This problem led the Department of Defense to conclude that cyber attacks are “an unrealistic candidate for traditional arms control” because “it is difficult to prove or disprove that an adversary has a cyber-attack capability, making any sort of ‘cyber disarmament’ intrinsically unverifiable.”¹⁸

Finally, cyber weapons are based on dual-use technology. While there are some technological similarities between nuclear weapons programs and peaceful civilian nuclear programs, there are also clear distinctions between the two that are easily discernable to weapons inspectors and other

¹⁷ Department of Defense, “Essential Elements for a Deterrence Strategy for Cyberspace,” 3.

¹⁸ *Ibid.*, 8.

experts. Furthermore, there are a limited number of states that possess the resources necessary to independently develop nuclear weapons, and the countries that have these resources would be unable to quickly convert civilian programs into weapons programs without attracting international attention. Even the most advanced non-nuclear states would require months (if not years) to successfully convert from one program to the other, therefore making it much easier for current nuclear powers to monitor the limited number of nuclear-capable states and then react if such a conversion were to be initiated.

These issues lead to the conclusion that the attempt to draw extensive similarities between nuclear and cyber deterrence is not a reliable or correct approach to implementing a successful cyber deterrence strategy. It may be necessary to apply lessons learned from other types of weapons to questions concerning cyber deterrence and cyber weapons in order to gain a more complete understanding of the potential approaches and challenges of implementing a cyber-deterrence strategy.

APPLYING DETERRENCE THEORY TO THE CYBER DOMAIN

Although most academic research on deterrence deals with nuclear deterrence, there is a growing field of research on the practicality of applying nuclear deterrence strategy to the cyber domain. These writings present conflicting views on the practicality of the synergy between the two modes of war fighting but both share common background. General Helms stated that one of the most important conclusions drawn from a set of deterrence exercises conducted at Schriever Air Force Base was that “some lessons about deterrence from the Cold War era do not necessarily translate to the space and cyber realm.”¹⁹ Even if Cold War lessons of deterrence do not directly apply in the cyber domain they provide a useful framework for reference in addressing the problem of cyber deterrence and attempting to establish a functioning cyber deterrence strategy.

¹⁹ Helms, 12.

One of the key issues with cyber deterrence is establishing what types of threats should be deterred and how to deter them. The simplest division of cyber threats places them into three categories: nation-state threats, terrorist threats, and criminal threats. Terrorist and criminal cyber threats, while dangerous and costly, do not pose as serious of a national security threat to the United States as nation-state threats, and existing counter terrorism and law enforcement mechanisms are more appropriate to face the threat than the Department of Defense. Furthermore, responsibility for dealing with terrorist and criminal cyber threats has been primarily delegated to the Department of Homeland Security and the Department of Justice rather than the Department of Defense. As such, the Department of Defense and United States Cyber Command’s (USCYBERCOM) focus centers around threats posed by nation-states. Therefore, the primary focus of a cyber-deterrence strategy is the Department of Defense’s efforts to deter nation-state threats in cyberspace.

As nation-state threats are the focus of deterrence strategy, they need to be analyzed in more detail. State-based threats can be further divided into cyber espionage and cyber attacks. Cyber espionage threats are primarily focused on collecting information through cyberspace while cyber attacks are designed to damage information and systems and potentially cause physical harm.²⁰ In theory, cyber espionage threats should be handled similarly to traditional espionage threats through robust defensive and counter intelligence programs. Despite the theoretical virtues of such a division it is difficult to implement in practice due to the difficulty in distinguishing between cyber espionage and attack threats. Oftentimes, the capability for

²⁰ Although there have not been many examples of cyber attacks causing physical harm to date, many influential policy makers, most notably Richard Clarke in his book, *Cyber War: The Next Threat to National Security and What to Do About It*, continue to project the potential for cyber engagements escalating to cause physical damage. Thomas Rid disagrees with Richard Clarke’s assessment and claims “Don’t fear the digital bogeyman. Virtual conflict is still more hype than reality.” Thomas Rid, “Think Again: Cyberwar,” *Foreign Policy*, March 1, 2012.

implementing a cyber attack is the same as for a cyber-espionage threat, and the only difference is the intent of the actor. Furthermore, there is the potential that a cyber-espionage threat could be misinterpreted as preparation for a cyber attack and could elicit a military response.

In order to apply Cold War lessons about deterrence to the cyber realm, there are several steps that the United States must take. Former NSA Director and Director of National Intelligence Mike McConnell argues that in order for cyber deterrence to work, America must express its intent to use deterrence, it must translate intent into capabilities, and the ability to “signal” an opponent about potentially risky behavior must be developed.²¹ Although McConnell argues that the technology exists, there are many potential challenges with cyber deterrence that must be addressed to make it a viable defensive strategy.

Prevention or Retaliation

The two main schools of thought on how to use deterrence in any domain advocate retaliation (punishment) or prevention (denial). Former Deputy Defense Secretary William Lynn said that, “we cannot rely on the threat of retaliation alone to deter attacks; deterrence must be based on denying the benefits of the attack.”²² Kenneth Geers applied this to cyberspace by stating “this means improving defenses, so that launching an effective attack becomes more difficult and expensive, and improving resiliency, so that effects of an attack can be mitigated.”²³

Although Secretary Lynn advocated the use of denial in deterring cyber-attacks, most scholars agree that prevention is not sufficient in the cyber domain and that a more aggressive retaliation approach to cyber deterrence must be pursued. Geers argues:

Denial is unlikely due to the ease with which cyber attack technology can be acquired, the

immaturity of inter-national legal frameworks, the absence of an inspection regime, and the perception that cyber attacks are not dangerous enough to merit deterrence in the first place. Punishment is the only real option, but this deterrence strategy lacks credibility due to the daunting challenges of cyber attack attribution and asymmetry.²⁴

Defense in cyberspace is further complicated by the decentralized nature of the Internet and the vast amount of data transmitted. According to a 2011 Cisco report, in 2010 there were 1.84 devices connected to the web per person in the world, and by 2020 Cisco predicts that number will reach 6.58 devices per person.²⁵ Cisco also estimates that by 2015 just less than one zettabyte of data will be transmitted annually over networks.²⁶

The mass connectivity of devices, the large amount of data transmitted on a daily basis, and the decentralized nature of packet-based communication systems make it nearly impossible to implement a defensive strategy that is one hundred percent effective, and the cost of securing network systems to prevent all attacks would be unsustainable. However, the difficulty of implementing a defensive or denial strategy for cyber deterrence does not mean that states should ignore defense.

Defense can be useful in limiting cyber terrorism and cyber crime but is not likely to prevent a well-funded nation-state or state-sponsored actors from compromising digital systems. States should continue to invest in cyber security and defensive systems but must recognize that, barring a

²⁴ Ibid., 10.

²⁵ David Evans, “The Internet of Things: How the Next Evolution of the Internet Is Changing Everything,” Cisco Internet Business Solutions Group, 2011, 3.

²⁶ Arik Hesseldahl, “Cisco: The Internet Is, Like, Really Big, and Getting Bigger,” All Things D, June 1, 2011. (This is approximately the amount of data that would fill 250 billion DVDs. (Cisco, “Visual Networking Index IP Traffic Chart”))

²¹ McConnell.

²² Geers, 6.

²³ Ibid.

significant technological breakthrough, well-funded nation-state actors will be able to penetrate secure information systems, necessitating a punishment response.

Although the United States and many other nations have the capabilities to punish potential cyber aggressors, there are several other challenges to pursuing this type of strategy. Geers goes on to state:

The trouble with a punishment strategy, however, is that governments are always reluctant to authorize the use of military force (for good reason). Deterrence by punishment is a simple strategy but one that demands a high burden of proof: a serious crime must have been committed, and the culprit positively identified. The challenge of cyber attack attribution, described above, means that decision-makers will likely not have enough information on an adversary's cyber capabilities, intentions, and operations to respond in a timely fashion.²⁷

Furthermore, "Deterrence by punishment is a strategy of last resort."²⁸ States are typically reluctant to use any kind of military force unless there is a clear cause to do so. In addition, deterrence by punishment in the cyber domain faces the problem of identifying the attacker. Without the capability to attribute an attack, deterrence by punishment strategy becomes ineffective.

A punishment strategy is also difficult to implement based on political and moral concerns. Without clear attribution of an attacker, punishment could be perceived as an overreaction or could be misdirected at an innocent third party. The consideration of the use of non-cyber forces to respond to a cyber attack would further

compound these concerns. The United States will require a high burden of proof before responding to a cyber attack with conventional force, and decision makers will struggle with the question of using conventional force to respond to a cyber attack. These questions could limit the credibility of a punishment strategy that is one of the essential elements of implementing any successful deterrence strategy.

Attribution

Michele Markoff, a senior policy adviser in the State Department's Office of the Coordinator for Cyber Issues, succinctly summarized the importance of attribution in deterrence strategy when she said, "classic deterrence policy fails in the absence of attribution." She went on to state, "attribution, the ability to determine who is attacking you, is difficult but not impossible in cyberspace."²⁹

Although the Department of Defense is working to improve its ability to attribute attacks, its attribution system is still not perfect and the Defense Department is assuming that following a large scale attack it will be forced to operate in a degraded environment, which will further hinder its ability to properly attribute attacks.³⁰

Cyber attribution is also hindered by attribution challenges that are unique to the cyber domain. While it is easy to identify a conventional or nuclear attacker, identifying a cyber attacker is much more difficult. James Lewis stated that, "since we know the identity of an attacker in perhaps only a third of cyber incidents, and since a skilled attacker will disguise their identity to appear as someone else, the United States could easily attack the wrong target."³¹ These uncertainties make it difficult to make a credible threat necessary for deterrence outside of conventional or nuclear conflict.³²

General Helms summarized these problems.

²⁹ William Jackson, "Cyberspace: A Battlefield Where the Old Rules Don't Apply," *Government Computer News*, 1.

³⁰ *Ibid.*

³¹ Lewis, 1.

³² *Ibid.*

²⁷ Geers, 9.

²⁸ *Ibid.*, 6.

We are all aware of the challenges of attribution, and yet the measure of your deterrence campaign's success or failure depends on it. Without confidence of attribution, how do you credibly assure an adversary in a pre-crisis environment that you intend to respond? How do you mitigate the risk of a third party exploiting the ambiguity to create or escalate the crisis? How can you assess the success of meeting your deterrence objectives and adjust your adversary-focused campaign accordingly, if you are not confident about attribution?³³

The questions General Helms posed accurately reflect the main problems with cyber deterrence and provide an excellent roadmap for what the United States needs to do to implement a successful deterrence strategy.

It may be possible that a cyber attack will be accompanied by kinetic action or other events in the international system that will help with attribution of a cyber attack.³⁴ For instance the 2007 cyber attacks on Estonia coincided with a diplomatic dispute between Russia and Estonia, suggesting that the attacks originated in Russia, although it remains difficult to determine if the attacks were state-sponsored or perpetrated by groups sympathetic to Russia that were not sponsored by the Russia government. A similar situation occurred in 2008 during the Russia-Georgia War. During this conflict the attacks on Georgia's internet infrastructure were most likely coordinated by Russia's Foreign Military Intelligence agency (GRU) and Federal Security Service (FSB), but the evidence is still not concrete and may not have been definitive enough to justify a counterattack on Russian targets were

it not for the kinetic actions taken by Russia against Georgia.³⁵

Overreliance on external events could also provide its own set of difficulties as other actors could seek to exploit a difficult international situation or further confuse the situation by launching additional attacks.³⁶ Third party actors could exploit a tense international situation through cyber attacks or conduct attacks that, as a result of false attribution, could escalate the conflict.

Some of these dilemmas could be mitigated through robust intelligence collection efforts. If the United States is unable to attribute an attack through cyber forensics, it may be able to attribute the attack through intelligence sources. It is important to bear in mind, though, that reliance on such systems would require real-time coordination between the intelligence community and military authorities, which is not always seamless.

The current construct and close relationship between USCYBERCOM and NSA likely makes such coordination practical but may become more difficult as NSA comes under increased scrutiny following recent leaks and when USCYBERCOM and NSA become more independent from each other in the near future. The commander of USCYBERCOM and the Director of NSA most likely will become separate positions following General Keith Alexander's retirement in the Spring of 2014.³⁷

Capability, Communication, and Credibility of Cyber Deterrence

The final difficulty with cyber deterrence is the question of rationality and proportionality of response. James Lewis argues that in order for the United States to make a credible threat of retaliation, it needs to expand its options into

³³ Helms, 14.

³⁴ Department of Defense, "Essential Elements for a Deterrence Strategy for Cyberspace," 8.

³⁵ John Leyden, "Russian Spy Agencies Linked to Georgian Cyber-Attacks: Follow the Bear Prints," *The Register*, March 23, 2009.

³⁶ Department of Defense, "Essential Elements for a Deterrence Strategy for Cyberspace," 8.

³⁷ Despite predictions of the split of NSA and USCYBERCOM, the commander has remained duell-hatted under Admiral Michael Rogers.

some other domain, but he also recognizes that such a response will escalate the conflict and present a new set of problems.³⁸ Matthew Crosston agrees that cyber-attacks can be easily viewed as an act of war and that attribution is essential because cyber-attacks can quickly lead to physical consequences.³⁹ A January 2013 report conducted by the Defense Science Board for the Department of Defense entitled “Resilient Military Systems and the Advance Cyber Threat” recognizes the potential for the escalation of cyber engagement in the future and recommends that the Department of Defense develop the capability to retaliate against a cyber attack with all elements of national power, suggesting that the United States needs to prepare to escalate a conflict beyond the cyber domain in order to maintain credible deterrence in cyberspace.⁴⁰

The most conventional logic is to respond to a cyber attack with a cyber counterattack of some kind. Assuming the attribution problems are overcome, a state can counterattack in cyberspace similarly to how it would counterattack in any other domain. The difficulty with a cyber counterattack arises with Schelling’s three requirements of a successful deterrence strategy: capability to retaliate, communication of intent to retaliate, and the credibility of the threat.⁴¹ Each of these elements presents a unique challenge in cyberspace, and they are not mutually exclusive.

The first retaliation difficulty in launching a cyber counterattack is maintaining the capability to respond. Cyber attacks are possible based on weaknesses in the system being attacked that allow the attacker to penetrate it. The

vulnerabilities to exploit are continuously changing as states patch security flaws and improve their defensive capability. Therefore, in order to maintain the ability to launch a cyber counterattack, the United States must continually search for weaknesses and develop exploits it can use against potential aggressors.

It may also be difficult to respond to a cyber attack if the attacker is not as reliant on cyber technology as the United States. A state’s cyber vulnerability increases as the country becomes more reliant on information technology systems. If a state is not reliant on information technology, it may not be as vulnerable to a cyber counterattack as the United States is to a first-strike attack. These problems could be compounded following a cyber attack, which could limit the ability of the United States to respond to a cyber first strike. To overcome this difficulty, the United States must develop reliable second-strike cyber capabilities that will function following a catastrophic cyber first strike.

These three difficulties lead to the conclusion that the United States may need to respond to a cyber attack with a counterattack using other instruments of national power. A cyber attack may warrant a response with the conventional means of military power. Although there is some agreement that a kinetic retaliation to a cyber attack can be warranted, there are still concerns about the justness of such an action and the potential for quickly elevating the severity of the conflict. James Lewis claimed:

Cyberspace poses a particular challenge for deterrence. State actors are engaged in harmful acts in cyberspace against the United States. However, military force is of limited utility in responding to or deterring actual cyber threats. A U.S. military response to espionage or crime would be a strange departure from international norms regarding the use of force. A retaliatory cyber attack (where the intention is to damage or to destroy, rather than exploit) or retaliation using a

³⁸ Lewis, 3.

³⁹ Matthew D. Crosston, “World Gone Cyber MAD: How ‘Mutually Assured Debilitation’ Is the Best Hope for Cyber Deterrence,” *Strategic Studies Quarterly* 5, no. 1 (Spring 2010): 106, <http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf> (accessed February 7, 2012).

⁴⁰ Department of Defense: Defense Science Board, “Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,” Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, DC, January 2013.

⁴¹ Schelling.

kinetic weapon for a cyber attack against countries that have not used force against us or against individuals with criminal rather than political aims, could easily be interpreted as an aggressive and unwarranted act by the international community. The result is to cast doubt on the credibility of a retaliatory threat, weakening any deterrent effect.⁴²

By this logic, regardless of justness of a retaliatory strike, the perception that the United States would not escalate a cyber-conflict into a kinetic fight limits the credibility of such a threat. Geers goes so far as to argue that a kinetic retaliatory attack may be more proportional than a cyber attack:

One important decision facing decision-makers in the aftermath of a cyber attack would be whether to retaliate in kind or to employ more conventional weapons. It may seem logical to keep the conflict within cyberspace, but a cyber-only response does not guarantee proportionality, and a cyber counterattack may lack the required precision.⁴³

Nevertheless, this assertion fails to address the political willingness of the United States to escalate the conflict and assumes that other states would believe America's threats.

Martin Libicki describes the escalation of conflict and defines what he refers to as the level of belligerence in conflict from least to most belligerent with respect to the use of diplomatic and economic force, cyber force, physical force, and nuclear force.⁴⁴ The United States and other nations are typically reluctant to elevate the level of belligerence from that of an attack suffered.

This reflects the lack of credibility that the United States has when threatening to use nuclear weapons. Although most states believe that the United States will respond to a nuclear attack with nuclear action, they do not expect that the United States will respond to a conventional attack with nuclear weapons except for in certain limited circumstances. This is one of the important distinctions between cyber and nuclear deterrence. While a threat of nuclear retaliation for a nuclear attack is credible, the threat of nuclear retaliation for a kinetic attack or of kinetic retaliation for a cyber-attack may not be. In order for cross-domain deterrence to be used effectively, this view of American proportionality must be overcome.⁴⁵

The second difficulty of implementing a cyber deterrence strategy is the ability to credibly communicate the threat of retaliation. Geers claims that in order for a denial or punishment deterrence strategy to work in cyberspace, it needs to be clearly communicated to the potential aggressors.⁴⁶ The difficulty with communication of a cyber retaliatory strategy is that clear communication of the capability to retaliate can compromise the exploit potentially used to retaliate. Therefore, communication of capability to respond to an attack can compromise the capability to respond.

Developing a strong cyber counterattack force and demonstrating its ability to respond in several engagements, thereby clearly communicating to other potential aggressors that the state has the ability to respond to cyber threats without compromising specifics on how the state intends to respond, could overcome this problem. This difficulty can also be overcome by communicating the intention to respond to cyber attacks with conventional forces, which are easier to identify and more difficult to defend against specific threats.

⁴² Lewis, 1.

⁴³ Geers, 7.

⁴⁴ Libicki, 24.

⁴⁵ Crosston, 113.

⁴⁶ Geers, 298.

CONCLUSION

Cyber deterrence presents unique challenges and questions for traditional Cold War deterrence models. These issues require careful consideration by policy makers and strategists, as well as increased investment in cyber capabilities in order to respond to a variety of cyber threats. Cyber deterrence, like nuclear deterrence, requires multiple responses and actions depending on the situation and how the United States plans to respond. The best option is for the United States to develop multiple capabilities, cyber and non-cyber, in order to maintain its ability to respond regardless of the threat it faces. This approach is similar to Herman Kahn's concept of escalation dominance in nuclear war, which he defined as

[The] capacity, other things being equal, to enable the side possessing it to enjoy marked advantages in a given region of the escalation ladder... It depends on the net effect of the competing capabilities on the rung being occupied, the estimate by each side of what would happen if the confrontation moves to these other rungs, and the means each side has to shift the confrontation to other rungs.⁴⁷

The United States needs to develop and maintain the capability to be dominant at all levels of conflict escalation in order to deter potential aggressors. The United States currently possesses these capabilities at higher levels of conflict escalation but needs to develop and maintain its dominance in cyber warfare as well.

The United States has already invested significant resources into offensive and defensive cyber capabilities, and while the exact nature of these forces is not public knowledge, it is generally assumed that the United States maintains robust cyber forces that are as capable if not more capable than any other force in the world. This investment could explain why large-scale cyberwar, although predicted by pundits for

several years, has yet to materialize. The United States may already be perceived to possess strong enough cyber and conventional forces to maintain escalation dominance, which deters potential aggressors in cyberspace. If this is the case, the United States needs to continue to invest in these capabilities in order to maintain escalation dominance and prevent other states from developing asymmetric advantages that could be used against the United States.

These assumptions are all based on attempts to apply nuclear deterrence theory to cyberspace, which although feasible in theory may differ in practice. A more applicable similarity may be the relationship between chemical or biological weapons programs and cyber weapons. All three are dual-use technologies that are simple to develop from civilian technology, easy to conceal, and can be adapted to a diverse set of targets. The Department of Defense also suggests there are similar difficulties in use between biological and cyber warfare: both "have the potential challenge of gaining access to specific targets, yet both can be applied indiscriminately across a wide range of targets. Similarities between biological warfare and cyber attack also can include uncertainty about attack attribution, uncertain effectiveness, the persistence of damaging results, and unintended consequences."⁴⁸ These similarities present a new framework for potential analysis of cyber deterrence and may lead to different conclusions.

Overall, cyber deterrence presents many unique challenges, but applying traditional deterrence concepts to cyberspace can help to overcome the difficulties in implementing a successful deterrence strategy. The most difficult questions and debates do not center on the practicality of cyber deterrence but on the assertion that the threat of cyberwar may be overblown and that deterrence may not be necessary in cyberspace.

If cyberwar proves to be less likely than anticipated, the United States may need to increase its investment in lower-level cyber crime and cyber espionage threats and decrease its

⁴⁷ Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Praeger, 1965), 290.

⁴⁸ Department of Defense, "Essential Elements for a Deterrence Strategy for Cyberspace," 9.

emphasis on cyberwar. If this is the case, traditional modes of warfighting will prove more significant than cyber concepts. If cyberwar, however, proves to be the way of the future, cyber deterrence will prove indispensable in order to “subdue the enemy without fighting.”⁴⁹

⁴⁹ Sun-Tzu.