Strategy Research Project

Cyber Deterrence: An Old Concept in a New Domain

by

Lieutenant Colonel Michael J. Philbin
United States Army

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Cyber Deterrence:
An Old Concept in a New Domain

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Michael J. Philbin
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Richard A. Lacquement, Jr.
School of Strategic Landpower

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,998

14. ABSTRACT

Cyberspace is the newest domain recognized by the United States military. One question often asked is whether or not deterrence is possible in the cyber domain as it is in the physical domains (land, sea, air and space). Deterrence, simply put, is convincing an opponent that the potential value gained in an attack is not worth the cost or potential cost of the attack itself. Certain aspects of the cyber domain certainly affect this calculation such as the monetary cost of cyber operations, the ability to attribute an attack in cyberspace, or the ill-defined nature of permissible behavior in cyberspace. However, these attributes do not fundamentally change the nature of deterrence. To successfully deter, the US government must continue to invest in cyber, lead in developing international norms for behavior in cyber, and continue to bolster its domestic defenses.

15. SUBJECT TERMS
Cyber Policy, U.S. Defense

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*
UU	UU	UU	UU	32	

USAWC STRATEGY RESEARCH PROJECT

Cyber Deterrence:
An Old Concept in a New Domain

by

Lieutenant Colonel Michael J. Philbin
United States Army

Colonel Richard A. Lacquement, Jr.
School of Strategic Landpower
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Cyber Deterrence: An Old Concept in a New Domain
Report Date:	March 2013
Page Count:	32
Word Count:	5,998
Key Terms:	Cyber Policy, U.S. Defense
Classification:	Unclassified

Cyberspace is the newest domain recognized by the United States military. One question often asked is whether or not deterrence is possible in the cyber domain as it is in the physical domains (land, sea, air and space). Deterrence, simply put, is convincing an opponent that the potential value gained in an attack is not worth the cost or potential cost of the attack itself. Certain aspects of the cyber domain certainly affect this calculation such as the monetary cost of cyber operations, the ability to attribute an attack in cyberspace, or the ill-defined nature of permissible behavior in cyberspace. However, these attributes do not fundamentally change the nature of deterrence. To successfully deter, the US government must continue to invest in cyber, lead in developing international norms for behavior in cyber, and continue to bolster its domestic defenses.

Cyber Deterrence:
An Old Concept in a New Domain

> Every age had its own kind of war, its own limiting conditions and its own peculiar preconceptions.
>
> −Carl von Clausewitz, On War[1]

Cyberspace is the newest domain recognized by the United States military. As a nascent domain there are a number of papers on the implications of this new arena to military strategy. One question often asked is whether or not deterrence is possible in the cyber domain as it is in the physical domains (land, sea, air and space). There are some elements in cyberspace that impact deterrence in cyberspace. Once these challenges are overcome there is a difference in deterrence from other domains.

Deterrence Defined

There are multiple theories of deterrence and how deterrence works. The United States Military Strategy concept of deterrence states:

> Denying an aggressor the benefits of achieving its objectives can be just as effective as in altering its strategic calculus through the threat of retaliation. The most effective deterrence approaches make use of both techniques while also providing potential adversaries acceptable alternative courses of action.[2]

Thomas Schelling defines deterrence as "persuading a potential enemy that he should in his own interests avoid certain courses of activity."[3] Common amongst the theories is some form of cost benefit analysis. "…deterrence involves anything that prevents (or attempts to prevent) an actor from taking an action by influencing its decision making through its anticipation that the action will lead to a negative result…"[4] More simply put, the attacker determines that the cost of the attack outweighs the potential benefits from the attack. To successfully deter an attack the defender must understand the elements

that make up the cost to the attacker and the elements that make up his potential benefits.

Cost Elements

The cost of an attack is made up of the total of the value of the resources used in the attack and the potential penalties incurred by the attacker as a result of the attack. One can measure Potential penalties in capabilities of the defender to retaliate and the defender's credibility, or the belief that he can or will use his capabilities to retaliate against the attack. "Retaliation is a familiar concept: during or after an attack, the defender launches a counterstrike that imposes costs on the attacker…"[5]

The simplest way to measure the value of the resources used in attack is to measure them in monetary terms. For example terrorists spent between $400,000 and $500,000 to carry out their attacks on the United States on 9/11.[6] One way to drive up the costs of an attack is to build defenses that would drive up the monetary price of attack. Another way to look at the value of resources expended is the cost in terms of world opinion. "For example, if the United States punished the families of suicide bombers … such an approach would be morally repugnant to the United States (normatively counterproductive) and would have adverse effects on broader US goals (strategically counterproductive)."[7]

The other half of the cost equation is the potential penalties incurred as a result of the attack. For example, it was a reasonable expectation that if one state launched a nuclear strike the defending state would retaliate with its own nuclear strike. In other words what damage will be done when the defender retaliates against the attacker. Significant to this estimate is the attacker's belief that the enemy can and will strike back. An attacker who believes that his initial attack will be so devastating that the

defender cannot retaliate does not have to factor in the cost of reprisal. Or the attacker may believe their will be no potential consequences for his actions, for example it is widely believed that Saddam Hussein did not think the United States would intervene when he invaded Kuwait in 1990. He believed there would be no significant cost in terms of international reaction to his invasion of Kuwait and so was undeterred.

Benefits

After calculating cost the attacker must then calculate benefit or the rewards reaped from an attack. This analysis includes the probability of successfully engaging the target or the likelihood that the attack will have any effect on the target. Then the likely effects on the target attacked, what level of effect does the attacker wish to achieve and how likely is the attack able to achieve that level. The calculation also includes the effect of the attack on the relationship between the attacker and the defender, will the attack improve the attacker's position in relation to the defender in the near term or long term, and will it bring an advantage.

Possibility of attacking a target relates directly to the defender's ability to defend his asset. If there is no chance of success or a very limited chance of success this tips the scales of the analysis towards cost. An attacker with little hope of success because of his adversary's defenses is unlikely to launch an attack that will cost him in resources and potential penalties. This is the concern of anti ballistic missile systems in nuclear deterrence. In the Mutually Assured Destruction concept one state is unlikely to attack the other because neither state can defeat the retaliatory strike of the other, because they both lack sufficient defenses. If one side of a nuclear exchange can defend against a retaliatory strike through a robust anti ballistic missile defense then the attacker may believe he can defeat his adversary's response. This in turn increases the

possibility of nuclear exchange. A strong defense deters an attack by convincing an attacker there will be no gains commensurate with the cost of attack.

Probability of successfully engaging relates to the attackers belief that his attack will achieve the effect desired. Although related to successful attack of a target, successful engagement is tied to target resiliency. If attacking a target will not achieve the desired endstate or is unlikely to achieve the desired endstate then there is no benefit to be derived or the known cost and potential costs are greater than potential benefits. If the Japanese had known how resilient both the US Pacific Fleet and the US resolve were prior to December 7, 1941, would they still have bombed Pearl Harbor?

Another element of benefit analysis is the reason for the attack. An adversary attacks to change the relationship with its competitor. The attack may occur to gain a near term competitive advantage. An attack may also be preemptive in nature. An adversary may believe that it must attack before its competitor grows in strength and a future attack may not be possible, that is, an attack to check growing power. The stronger an adversary believes its attack is more likely to achieve its strategic ends, the more likely it is to attack. This is the comparative phase of cost benefit analysis. Ultimately, the questions a belligerent asks itself are: is the cost worth the strategic benefit? And, is it the optimal means of achieving an adversary's endstate?

How is the Cyber Domain different

Cost

Compared to operations in other domains, operations in cyberspace are inexpensive. A computer with internet access has the potential to disrupt a regional power grid[8], degrade a nation's financial institutions[9], or physically destroy some piece of infrastructure[10]. Similar effects in other domains would require expensive missiles,

planes, ships or land forces. “The prerequisites for a cyberattack are few: talented hackers, intelligence on the target, exploits to match the vulnerabilities found though such intelligence, a personal computer or any comparable computing device and any network connection.”[11]

The attacker can also repeat the use of cyber resources with little cost. A missile launched or a bomb detonated or a bullet fired can never be used again. Most of the costs invested in creating the physical means of attack are lost at the time of attack. The cost of the electrons used to send a cyber attack is negligible. “It costs about 4 cents per machine… You could fund an entire cyberwarfare campaign for the cost of replacing a tank tread…”[12] The predominant cost in the cyber attack is the intellectual capital spent in developing the means of attack. The interconnectivity of cyberspace allows an attacker to launch his attack from virtually any part of the world against any other part. This allows the attacker to protect his primary investment, the intellectual capital and even his physical means, relatively safe from counterattack. While not all attacks are equal and some methods may cost more than others, the potential return on investment for a cyber attack makes it a very attractive and affordable means of attack.

The low cost of entry into operations in the cyber domain opens the door to a wide array of potential adversaries. Super empowered groups or individuals can use the same ways and means as state actors. For example the Distributed Denial Of Service (DDOS) attacks launched against both Estonia in 2007[13] and Georgia in 2008[14] are believed to have been perpetrated by a cyber criminal networks like the Russian Business Network. “If an individual using a personal computer can execute an attack on major national or international targets, then individuals become the equals of states in

cyberspace".[15] This complicates deterrence efforts on the part of the defender. If an attack can be successfully attributed to a specific individual or organization how can the defender know if the attacker was working at the behest of his government or of his own volition.[16] This complicates the potential responses by the defender. Should the response be against the state the attack originated from, (possibly treating the attack as an act of war), or should the response be against the individual, (possibly treating the attack as a criminal act)? Improper responses could potentially create interstate conflict or weaken future deterrence efforts.[17]

Attribution

Unlike a missile attack or other attack in the physical domains, a cyber attack leaves little to no evidence behind for the defender to determine who actually attacked him. For a state to effectively retaliate against a cyber attack, it must know who executed the attack. As discussed above, retaliation against the wrong state or actor has the potential to be worse than the attack itself. If a state cannot successfully attribute the source of an attack, it cannot safely retaliate. If a state cannot retaliate, than an important element of deterrence, cost of an attack, is missing and the state's ability to deter is impeded. The ability to accurately attribute attacks to the attacker has improved as technology has advanced but attribution is still not certain.[18]

An example of an early misattribution is an intrusion into DOD networks in February of 1998. Officials labeled the attack as one of the most organized and systemic ever launched at that time. The attack occurred during a time of heightened tensions with Iraq and some came to the initial conclusion that Iraq was responsible for the attack based on circumstantial evidence. However an FBI investigation revealed

that the attack had actually come from an Israeli hacker, Ehud Tenebaum and two California teens who had hacked the systems just for fun.[19]

Efforts at attribution have improved but the evidence may not be sufficient to demonstrate culpability of a state or group (for example, the DDOS attacks against one of the most cyber-connected countries in the world, Estonia,[20] in 2007). Estonia knew the attacks originated, in part, from Russia. Despite a mutual legal assistance treaty, Russia refused to assist Estonia with its investigation. This behavior and other circumstantial evidence indicated that the Russian government may have been complicit in or authorized the attacks but no conclusive evidence was ever found.[21] The only person actually charged and convicted of the attack was an Estonian of Russian descent.

Despite the geometric progression of technology, five years after the Estonian DDOS attacks we still have not completely overcome the challenges of attribution in cyberspace. The United States is one of the most technologically advanced countries and it is still working on the problem of attribution. According to Leon Panetta, the US Secretary of Defense, "The department [of Defense] has made significant advances in solving a problem that makes deterring cyber adversaries more complex: the difficulty of identifying the origins of that attack."[22] Of note, the Secretary stated that they have made advances versus solved the problem. This leaves the possibility that an adversary may still carry out his attack in anonymity. Most importantly, for deterrence to be effective the potential attacker must believe the defender has the capability to identify his attacker.

Repetitiveness

One of the unique characteristics of cyber operations is that the attacker must find a vulnerability in the defender's system to successfully launch an attack. A useful analogy in the land domain might be to consider, the defender's system to be like a castle under siege that is invulnerable to catapults or battering rams but has a multitude of doors. To gain entry, the attacker must pick the lock on one of the doors, have a spy inside the castle open a door or sell the lord of the castle a door for which the attacker has a key. Picking the lock represents the hacker, an external threat that uses malicious code or gaps in programming to gain access to a system. Insider threats are represented by the spy or the door. Either way a system cannot be overcome by brute force or an overwhelming assault. An attacker must find the weakness in the system that allows him in before the attack may begin. When the defender identifies the vulnerability, he can take steps to close the gap in his defenses. Thus the attacker's ability to use the same method of attack repetitively is limited.

The hacker finds vulnerabilities in programming codes that allow entry into a system or develops malicious code that deceive unsuspecting users into bringing into the system by using techniques such as spoofing or the use of Trojan horses. Once a defender recognizes that he is being attacked he goes through the process of identifying how the attacker entered the system and determining what door he used. After the defender identifies a programming weakness he can "repair the vulnerability directly or…tell the software vendor and press for a solution."[23] The defender can shut down portions of his system that are vulnerable or take the whole system offline to prevent further damage until repairs can be completed. Also the defender can alert users to the methods of attack to prevent future penetrations as well. "As a general

rule, tricks exhaust themselves to the extent (1) that their existence and thus the need to protect against their recurrence is obvious and (2) that counters to their recurrence are straightforward to implement."[24] In other words, the defender sees enemies in the castle he can find the open door, close it and change the lock or even nail it shut.

Insider attacks come in two varieties that are also difficult to repeat. One is the individual who assists an adversary by attacking the system from the inside. The other is a part of the system that has been compromised by the attacker before it has been introduced. Again once the defender realizes that he has been attacked forensics allow him to identify the source of the attack or the open door. Either form of insider attack is difficult to establish, costly, and unlikely to be successfully repeated.

An exception in the attacker's need to penetrate the defender's system is the DDOS attack. In this type of attack the attacker overwhelms the defender's system with illegitimate traffic to prevent the legitimate flow of information and bog down the defender's system. To use the castle metaphor, the enemy sends mobs of people to the castle doors to prevent anyone from coming in or out of the castle and expend the defender's time determining what to do with the hordes attempting to gain entry. Even this attack is limited in its ability to persist and repeat. Defender's can filter the illegitimate traffic, reroute systems or increase capacity. For example, in the Estonian DDOS attack some systems were brought back online after a couple of days. Subsequent DDOS attacks weeks and months later had little to no effect on the Estonian systems. Overall attacks in the cyber domain lose their effectiveness as they are repeated as shown in the figure below.

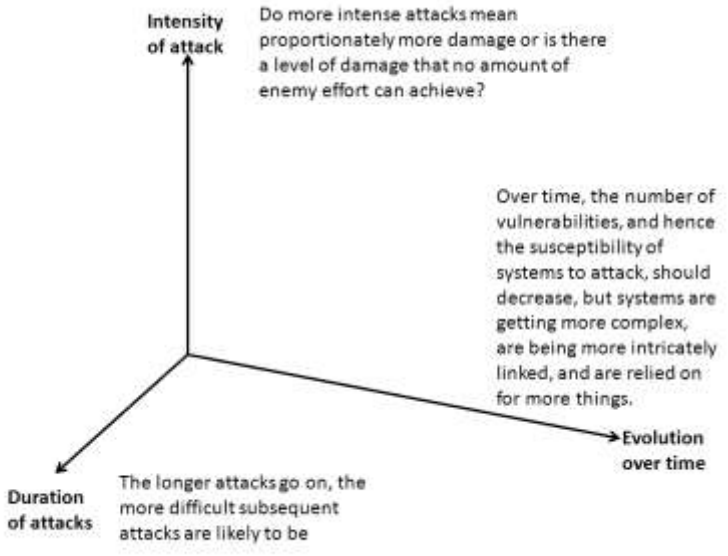


Figure 1

Nascence

Unlike the other domains, cyberspace has only been around for a relatively short period of time. The novelty of cyberspace has created a domain that is replete with ill-defined terms, concepts and doctrine. Land and sea domains have been in existence for centuries. Even the air domain, which man has only really mastered in the last century, is well defined and understood. While the space domain is also relatively new, the ideas of the other domains, land, sea and air, have more easily transferred to it.

Part of the problem of definitions for cyberspace relative to the other domains is that cyberspace is a man-made domain that does not lie completely in the physical world. Cyberspace consists of three elements. The physical element contains the computers, servers, and other physical parts that the programming resides on and allows systems to communicate with each other. The programming element is the algorithms and computer code that allows devices to interact with users and other

machines. The data element is the actual information stored on the machines that is accessed by users or used by the machines to make calculations or decisions based on the programming element.[26] Most of the actions in cyberspace take place within the latter two elements, with little effect on the physical world other than the movement of electrons invisible to the human eye across cables and radio waves that connect the hardware.

This disconnection from the physical world means that concepts from the other physical domains are not readily transferable to cyberspace. For example, the concept of an attack in cyberspace is not as well defined. In the physical domains an attack is easily conceived of as "the act of attacking [to set upon *sic*] with physical force"[27]. If one state sets upon another with physical force it is generally accepted that it constitutes an attack that the other state has the right to defend itself against. Since most of what actually occurs in cyberspace does not happen in the physical element this definition does not fit well.

The United States Department of Defense defines an attack in cyberspace or Computer Network Attack (CNA) as **"**actions taken through the use of computer networks to disrupt, deny, degrade, manipulate or destroy information resident in target information system or computer networks, or the systems / networks themselves."[28] By this definition a DDOS would be characterized as a CNA as it attempts to disrupt communications flow for a system. However the Estonians did not classify the DDOS against it in 2007 as an attack and invoke Article 5 of the NATO charter, in part because "…among Allies there existed ambiguity over what exactly constituted a weapon under the Alliance's charter. This was a war in an absolutely different dimension; it was a

virtual war that encompassed computers from all over the world."[29] At the other end of the spectrum, Chinese efforts at compromising US computer systems are not classified in the DoD definition as attacks, however, a simple search on the internet will reveal that the popular consensus is that those efforts are considered attacks, at least in the media.

Within cyberspace there is a wide spectrum of operations. Operations may vary from Computer Network Exploitation (CNE), in which an adversary explores an opponent's computer network looking for vulnerabilities that may be exploited later to a CNA that results in effects in the physical world such as shutting down a power grid. Between these two ends of the spectrum lie a variety of operations, many of which have already occurred, that a defender could define as an attack from cyberspace. Because cyberspace is new to conflict, international law and customs have not been established to clearly define within the global community where the lines are drawn in terms of acceptable versus unacceptable behavior.

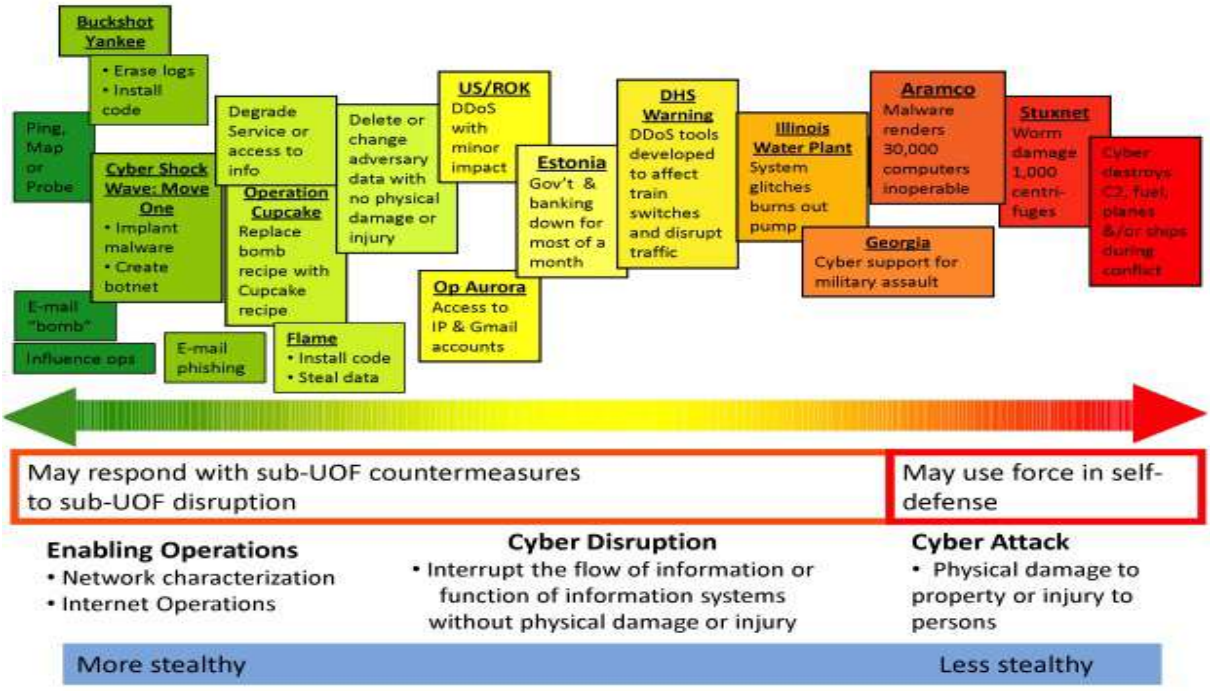
The ends of the spectrum are relatively easy to define. CNE readily equates to spying in the physical domains. Is a hacker that probes an adversary computer network to find weaknesses any different than a satellite in space that flies over an adversary's land to view the posture of his defense forces? Or is a hacker that breaks into his opponent's system to steal secrets about his advance technology different than a spy who pays a scientist to give him those same secrets? The difference is that spying in cyberspace may be relatively easier and cheaper than in the physical domains. The acts themselves are the same. It is in the methods that they differ. Activities of this kind happen in the physical domains and cyber domain daily and do not cause states to

"counter attack" one another. Instead, states build strong defenses to keep their secrets safe.

At the opposite end of the spectrum from CNE is an actual CNA. The best example of a real CNA is the Stuxnet virus attacks against Iran in 2010.

> The Stuxnet event was as clearly a cyber attack as any publicly announced event to date. Intentionally designed malware directed against a nation-state resulted in the physical destruction of state-owned equipment. The centrifuges were destroyed as effectively as if someone had taken a hammer to them, and these were not just random bits of equipment. The destroyed centrifuges were a critical component of Iran's nuclear ambitions.[30]

While Iran did not admit that the Stuxnet virus was an attack, the results of the virus were little different than if the facility had been bombed. This type of attack has the potential to kill bystanders as any other explosive attack. Clearly this type of attack is equivalent to any attack in the physical domain.



[31]

Figure 2

It is between the ends of the spectrum that what constitutes an attack becomes harder to define. The figure above illustrates the types of attacks along the spectrum that have already occurred and where those attacks may begin to reach the definition of attack within the realm of international law.

The figure illustrates the spectrum of cyber operations. Some of these operations that fit the US DoD definition of a CNA, do not necessarily fit the definition of an attack currently and commonly held within the international community. The best example of this is the DDOS attacks against Estonia in 2007. This attack was an attempt to disrupt the Estonian government computer systems which falls within the joint definition "actions taken through the use of computer networks to disrupt… information resident in …computer networks"[32] Despite the attack fitting in the definition the United States did not invoke the NATO Charter and come to Estonia's mutual defense. Where the line is drawn is important for deterrence. A potential enemy must understand that his actions will be construed as an attack or there will be no expectation of reprisal within his calculations of whether or not to attack.

Deterrence in Cyberspace

The concept of deterrence in cyberspace is no different than the concept of deterrence in any of the physical domains. The defender makes the attacker's decision to attack unpalatable enough to prevent him from carrying out his attack. There are aspects of the cyber domain that uniquely differentiate it from the physical domains. These differences do not change the fundamental concept but they do add some unique challenges.

Differences of Cyber Deterrence

The predominant difference of deterrence in cyberspace is the calculation of cost of operations in cyber. The low cost of operations affects both the ability to attack and defend in the cyber domain. Additionally, attribution and the ambiguity of what constitutes an attack affect the balance of the cost benefit analysis. The interconnectedness of cyber creates vulnerabilities for defenders and opportunities for attackers that do not exist in the physical domain. These attributes adjust the values when determining a cost benefit analysis.

As discussed previously, the cost, in terms of resources consumed and resources risked in cyberspace, is very low. To increase the potential cost, a defender in theory must then increase the potential risk of retaliation. Without the ability to impose cost upon an attacker the defender cannot deter attacks. He can only build his defenses in the hopes that repetitive attacks do not eventually lead to success.

Another factor in the computation of cost is attribution. If a defender cannot know where an attack came from then he cannot retaliate. If there is no possibility of retaliation, then there is no potential cost for making the attack. In the same vein the ambiguity of what an attack consists of can effect the attacker's valuation of cost of an attack. If the attacker believes his actions do not constitute an attack or do not constitute an attack large enough to cause reprisal then again there is no cost to factor in. Low resource value and the potential for no retaliation make an attack in the cyber domain potentially quite lucrative for an adversary.

The low cost of resources required for operations in the cyber domain also benefit the defender in deterrence. Unlike the physical domain where it may be difficult or expensive to build resiliency in a system, in the cyber domain the programming and

data elements can be inexpensively replicated and potentially replaced in the event of a catastrophic loss. Unless a cyber attack includes an element of physical destruction, systems can be brought back on line at low cost to the defender. For example, in a DDOS the network that is overwhelmed is not physically damaged. After the attack has been circumvented the system can resume normal functionality. A resilient system lowers an attacker's cost benefit analysis.

Another aspect of the cyber domain that affects the deterrence calculation is the interconnectedness of cyber. In the physical world an attack against an ally or a distant part of a state's physical territory will not directly affect the state. In the cyber domain attackers may go through an ally's system connected to the defender or go through a less important part of the system to gain entry into the defender's key cyber terrain. A defender cannot build strongpoints of defense or use physical space to assist him in defending himself. He must defend all places all the time to ensure his cyberspace is defended. This increases the cost of defense for the defender and opens windows of opportunity for the attacker.

Similarities of Cyber deterrence

Fundamentally, there is no difference between deterrence in the cyber domain than in any other domain. For deterrence to be effective, the attacker must believe that the benefits of his successful attack will be worth the cost of his attack. Some may argue that the anonymity of cyber may lead to misattribution of attacks, or that the unequal development of cyber technology makes reprisal more difficult as some states are more dependent on cyber than others, or that attacks in cyber will likely escalate because of the imbalance of cyber technology. While all of these hazards do exist with

conflict in the cyber domain, they are not exclusive to it and these are issues that states have been managing before cyber.

Misattribution differs from an inability to attribute an attack as discussed previously. In misattribution the defender believes he knows where an attack came from and who the responsible party is but the defender is wrong. For example, someone from the Russian Business Network, conducting CNE inadvertently infects a US computer system and the US government believes the Russian government is responsible for an attack on its systems. In this hypothetical, the US retaliates against Russia and creates a conflict where none existed because they cannot know exactly who attacked them or why. But a similar scenario could also exist in the physical domains. In the movie "By Dawn's Early Light" a rogue Russian general launches a nuclear missile against the US which the US misattributes to the Soviet government and launches a retaliatory strike[33]. A real example of misattribution is the Mayaguez incident in1975 in which a Cambodian captain seized a US merchant vessel. The US government did not know if the vessel had been officially seized by the Cambodian government or if this was an act of piracy by a renegade member of the Khmer Rouge.[34] While attribution challenges may increase the risk of misattribution in the cyber domain, these challenges are not unique to the cyber domain. If a state knows generally where an attack came from it can hold that state responsible for the attack or for handing over the perpetrators. For example, the United States held Afghanistan responsible for handing over Osama bin Laden after the attacks of September 11, 2001. The Afghan Government's decision not to turn over bin Laden was the main justification for the US attack against Afghanistan.

Another argument that some make for the difference of cyber deterrence is that some states are more dependent on cyber than others. A state without any cyber dependency would not have to include risk of penalty into their analysis because any attack against their cyber infrastructure would have no effect. But this concept assumes that retaliation must come in the same form as the attack rather than from action in a different domain. This is a bad assumption. Reprisals and the threat of reprisal occur across domains. States have responded to terrorists bombings (land domain) with air strikes (air domain). During the Cold War, the threat of nuclear attack (air/space domain) helped to deter the Soviet Union from invading Western Europe (land domain). Current US policy is clear that possible retaliation for a cyber attack may come in any form.

> …the United States will respond to hostile acts in cyberspace as we would to any other threat to our country… We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.[35]

Cross domain retaliation is a reality. The cyber domain is not excluded because it is a new domain or does not exist solely in the physical world.

The potential for misattribution and cross domain retaliation increase the potential for escalation of a conflict. But again, escalation of conflict is not limited to the cyber domain nor is it limited to deterrence. Whether the conflict takes place in one of the physical domains or in the cyber domain the key to de-escalation or limiting the escalation of a conflict is communication. Threats and counterstrikes must be communicated to an adversary, regardless of the domain.

US Policy and Cyber Deterrence

The United States looks at cyber security along three lines of effort: domestic security efforts, international consensus on cyber security, and deterrence through detection and response capabilities.[36]All three of these efforts are a part of deterrence. It is in the last line of effort where the US government has made the most progress. While US policy supports the concept of international consensus on cyber security, there has been little consensus specific to cyber achieved thus far.[37] The first effort has fallen short as a matter of national policy, regulation or law. Overall the United States needs to place greater emphasis on domestic security efforts to enhance its overall deterrence efforts.

United States Department of Defense is striving to improve deterrence by improving its capabilities, creating organizations and policies to improve response, and working with industry and international partners.[38] DoD recognizes

> that deterring malicious actors from conducting cyber attacks is complicated by the difficulty of verifying the location from which an attack was launched and by the need to identify the attacker among a wide variety and high number of potential actors. ..the Department actively seeks to limit the ability of such potential actors to exploit or attack the United States.[39]

According to the former Secretary of Defense "Over the last two years, DoD has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment."[40] DoD is also investing in personnel to improve its talent pool and create capabilities to detect attacks and respond in kind if necessary. DoD has created US Cyber Command to lead the effort in international cyber operations and their efforts in domestic cyber defense. By working with the executive branch, other government agencies, and private industry it has improved cyber defenses and is

working on improving the policies which govern actions in cyberspace. Overall DoD has demonstrated improvement of its cyber capabilities over the last few years.

The United States is also working to better define the rules of cyberspace. The US International Strategy on Cyberspace states

> Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them. We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace…[41]

Clearly, the United States government recognizes that applying current norms of behavior is a good but insufficient start to defining norms in cyber space. While multiple international agencies and private entities play a role in cyber security, currently there is no international organization recognized as the lead for developing these norms.

> For over a decade, however, the U.S. government—while complaining about cyberattacks, espionage, and exploitation by other states and non-state actors—has avoided international arrangements that go significantly beyond obligating a group of predominantly European states to criminalize and cooperate in prosecuting specified forms of conduct.[42]

US policy is changing.The United States should place greater emphasis on creating international norms for acceptable behavior in cyberspace. As a world leader the United States should be leading the charge in garnering consensus among nations.

The first line of effort, domestic security, is where the least progress has been made. Legislative efforts to create standards for cyber security for critical infrastructure have failed. On 12 February 2013, the President signed an executive order to enhance domestic cyber security.[43] There are still significant issues that need to be resolved including cost to industry, application of standards, and liability for private industry among others. The executive order establishes the National Institute of Standards and

Technology as the executive agent for developing the cybersecurity standards but those standards are voluntary for industry.[44] Protection from potential litigation will encourage private corporations to follow the standards but there are no requirements for compliance.[45] Additionally, there are no liability protections for industry as they share information regarding attacks.[46] This may inhibit the open sharing of information between industry and the government out of fear of litigation for negligence. The US government must continue efforts to increase domestic cyber security.

Conclusion

Deterring in cyber is no different than in any other domain: develop a strong defense, let your enemy know implicitly or explicitly where your limits for reprisal are, and have the ability to counter attack. To be able to deter in the cyber domain, like in the physical domains, the US government must further develop the capability to attribute an attack and international norms for behavior and definition of attack in cyber. If the defender can identify where a cyber attack comes from and the attacker believes the defender will identify him, the cost calculation is significantly altered from an attacker who believes he can attack with impudence. The attacker must understand what the defender believes is an attack that may generate a reprisal. A defender cannot deter an attack that his adversary does not believe is an attack. The United States still must improve its deterrent stance but, given time to resolve these issues, deterrence in the cyber domain will be no different from the other domains.

Endnotes

[1]Carl Von Clausewitz, *On War* (Princeton, New Jersey: Princeton University Press, 1976), 593.

[2]Office of the Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America*, Washington, DC (February 2011): 8.

[3]Thomas Schelling as quoted by Alex S. Wilner in "Deterring the Undeterrable: Coercion, Denial and Deligitimization in Counterterrorism," *Journal of Strategic Studies* 34, no. 1 (February 2011): 6.

[4]Jeffery W Knopf, "Three Items in One," in *Complex Deterrence Strategy in the Global Age*, ed. T.V. Paul, Patrick M. Morgan, and James J Wirtz (Chicago and London: University of Chicago Press, 2009), 38.

[5]Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (Fall 2010):106 http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf (accessed January 2013).

[6]John Roth, Douglass Greenburg, Serena Wille, *Monograph on Terrorist Financing*, (National Commission on Terrorist Attacks Upon the United States): 6.

[7]Goodman "Cyber Deterrence," 106.

[8]*Cyber Attacks on US Are Becoming More Lethal*, Homeland Security News Wire,19 September 2011, http://www.homelandsecuritynewswire.com/cyber-attacks-us-are-becoming-more-lethal (accessed January 2013).

[9]Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired Online*, August 21, 2007 http://www.wired.com/politics/security/magazine/15-9/ff_estonia?currentPage=all (accessed November 2012).

[10]Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," *Joint Forces Quarterly* no 63, (October 2011), http://www.ndu.edu/press/why-iran-didnt-admit-stuxnet.html (accessed November 2012) 71.

[11]Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, California: Rand Corporation, 2009), 59.

[12]John Markoff, "Before the Gunfire, Cyberattacks" *New York Times*, August 12, 2008 http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1& (accessed November 2012).

[13]Libicki, *Cyberdeterrence*, 2.

[14]Markoff, "Before the Gunfire".

[15]Goodman, "Cyber Deterrence," 112.

[16]Libicki, *Cyberdeterrence,* 46.

[17]Ibid, 41.

[18]Leon Panetta, "Secretary Leon Panetta's Speech About Cybersecurity," Council on Foreign Relations online, October 12, 2012 http://www.cfr.org/cybersecurity/secretary-leon-panettas-speech-cybersecurity/p29262# (accessed November 2012).

[19]Goodman, "Cyber Deterrence," 120.

[20]Joshua Davis, "Hackers Take Down the Most Wired Country in Europe."

[21]Goodman, "Cyber Deterrence," 111.

[22]Leon Panetta, "Secretary Leon Panetta's Speech About Cybersecurity."

[23]Libick, *Cyberdeterrence*,56.

[24]Ibid, 57.

[25]Ibid, 60.

[26]Ibid, 12.

[27]*Merriam Webster Online,* http://www.merriam-webster.com/dictionary/attack (accessed December 2012).

[28] Memorandum for Chiefs of Military Services, Combatant Commanders, Directors of Joint Staff Directories, *Joint Terminology for Cyberspace Operations*,3 http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf (accessed December 2012).

[29]Haly Laasme, "Estonia, Cyber Window into the Future of NATO," *Joint Forces Quarterly* no. 63 (October 2011): 60,http://www.ndu.edu/press/estonia.html (accessed November 2012).

[30]Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," 71.

[31]Gary D. Brown and Owen W. Trullos, "On the Spectrum of Cyberspace Operations," Small Wars Journal Online (11 December 2012) http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations (accessed December 2012).

[32]Ibid.

[33]Bruce Gilbert, *By Dawn's Early Light*, DVD, Directed by Jack Sholder (Hollywood, CA: HBO Productions, 1990).

[34]Clayton Chun author of *The Last Boarding Party – The USMC and the SS Mayaguez 1975*, interviewed by author, Carlisle, PA, March 8, 2013.

[35]Barack Obama, *International Strategy for Cyberspace* (Washington, DC: The White House, May 2011), 14.

[36]Leon Panetta, "Secretary Leon Panetta's Speech About Cybersecurity,"

[37]Abraham D Sofaer, David Clark, Whitfield Diffie, "Cyber Security and International Agreements," in *Proceeding of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy* (Washington DC: National Academy Press, 2010)

[38]Leon Panetta, "Secretary Leon Panetta's Speech About Cybersecurity."

[39]US Department of Defense, *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* (Washington, DC: Department of Defense, November 2011), 6 http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%2934%20Report_For%20webpage.pdf (accessed October 2011).

[40]Leon Panetta, "Secretary Leon Panetta's Speech About Cybersecurity."

[41]Barack Obama, *International Strategy for Cyberspace*, 9.

[42]Abraham D Sofaer, David Clark, Whitfield Diffie, "Cyber Security and International Agreements," 180.

[43]White House, Office of the Press Secretary, "Executive Order on Improving Critical Infrastructure Cybersecurity," February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0 (accessed 23 February 2013).

[44]Ibid.

[45]Alexei, Alexis, "President Obama Signs Executive Order on Cybersecurity, Seeks Voluntary Standards," *Bloomberg BNA*, February 18, 2013, http://www.bna.com/president-obama-signs-n17179872423/ (accessed 23 February 2013).

[46]Ibid.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu