AU/ACSC/WIELAND/AY11

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

DEFINING DETERRENC IN CYBERSPACE

WORKING TOWARD A FRAMEWORK TO INTEGRATE CYBER DETERRENCE

by

Maj Steve Wieland

Maxwell Air Force Base, Alabama

April 2011

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Singapore government, the US Department of Defense or the Singapore Ministry of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Table of Contents

Abstract

The goal of deterrence is not to deter the use of a particular weapon. Rather, a nation deters undesirable behavior. Cyber warfare can produce three basic effects—SCADA attacks that cause physical destruction, loss of confidence in one's information, and disruption. These effects and their associated limitations will not produce a strategically decisive result. Cyber warfare must be used in conjunction with other instruments of power to successfully coerce another nation to accede to political demands. However, denying a potential adversary the benefits of cyber coercion or raising the costs of attempting it comprise important components a deterrence strategy. To deny benefits, defensive measures will prevent attacks from being successful. Alternatively, resiliency of critical systems will allow mitigate the value of attacks. The costs of attack consist of words and deeds. Clear, culturally appropriate communication of response measures helps dissuade actions. The actual retaliation after a cyber attack deters future attacks. Looking toward the future, a deterrence posture must include resiliency, organizational changes across the board, use of technology, and appropriate, integrated response measures.

The 2015 Iranian Conflict

The decades-long tension between the United States and the Islamic Republic of Iran turns to war after a series of provocations and missteps. The United States and Iran now wage a pitched battle to control the Straits of Hormuz. Momentum is beginning to turn as air strikes against Iranian military targets begin to take their toll. The American military appears to be gaining the upper hand. Without an operational nuclear weapon, the Iranians do not hold out hope of winning a conventional battle against the world's lone superpower. Despite Iran's rhetoric of "continuing to fight the Devil's crusaders with all of the Islamic Republic's men, women, and children for as long as the will of Allah allows," most power brokers within the Iranian regime believe the regime cannot survive an extended conflict.

The Iranians turn to a strategy of damaging the United States' economy and attempt to use political pressure from other major powers so the Americans will negotiate an end to the conflict. Terror attacks against American interests, including some within the United States, attempt to attack the will of the American people, undermine the economy, and divert resources to antiterrorism measures. Iran also declares the Straits of Hormuz part of sovereign Iranian territory and announces its policy to deny tankers access through the straits—by force if necessary—if the oil is destined for the United States or to a nation that will sell oil to the United States. Iran's ability to enforce such a policy is largely irrelevant, since its announcement results in yet another spike in the price of oil.

Within a few days, the national air traffic control system goes down for almost 40 minutes. No significant incidents result from the outage, but it causes massive disruptions in the airline network already under strain from heightened security measures. Next, the major banks are swamped with calls from angry customers with incorrect balances; many of whom show no

money in their accounts. Just as media accounts are fueling panic and hordes of people are demanding their accounts cashed, generators at three power plants simultaneously seize, cutting power to much of Seattle's metropolitan area. The physical damage to the plants will take them off of the power grid for weeks or months.

Multiple groups claim responsibility for the attacks, deny coordination with the Iranian government, and promise more devastating attacks if the United States does not end the conflict with Iran. The American people are in a panic. The stock markets close both to prevent irrational fear-based trading and in response to reports that question the integrity of electronic trades. Some Americans call for the Administration to up the stakes—with nuclear weapons if necessary; others protest in the streets that the costs of continuing the conflict are too high. However, all demand that the government protect them against future attacks.

Introduction

This hypothetical scenario set in the year 2015 highlights how an adversary might attack civilian cyber targets to advance its political objectives. It also describes a scenario where the United States is unsuccessful in deterring an attack against its homeland. Cyber warfare is different from deterring the use of nuclear weapons, a cornerstone of American strategy since the beginning of the Cold War. As the newest domain of warfare, cyber warfare has not fully been digested by military strategists and politicians. This paper seeks to define a framework to begin resolving the challenges associated with deterring cyber warfare.

The concept of cyberdeterrence is somewhat misleading. From a strategic perspective, nations do not deter the use of a weapon; rather, they deter an adversary's behavior. As will be discussed, a nation's deterrent strategy is generally agnostic to which weapons are or are not used. The exception to this assertion is the use of nuclear weapons, which by virtue of their

massive destructive power have strategic consequences by their very use. Cyber weapons, on the other hand, do not possess the killing power or physical destruction comparable to nuclear weapons. At an operational or a tactical level, individual weapons—including cyber weapons—can be deterred. Deterring cyber weapons have unique challenges. Cyber deterrence requires different approaches to address cyber warfare's distinct capabilities and limitations.

This paper begins with a working definition of cyber warfare. Next, it delves into the relevant characteristics that distinguish cyber warfare from other forms of warfare. These characteristics are followed by the effects cyber warfare can create and its political utility as a coercive tool. Then, the paper examines various models of deterrence and discusses those aspects particularly relevant to cyber deterrence. After reviewing existing United States policy, this paper will propose a framework to move towards cyber deterrence, including that described in the opening scenario.

Distinguishing Characteristics from Other Forms of Warfare

Cyberspace is its own medium with its own rules. Cyberattacks, for instance, are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities. Permanent effects are hard to produce.[1]

- *Martin Libicki*

In a memorandum to the Department of Defense, the Vice Chairman of the Joint Chiefs of Staff, Gen James Cartwright, defines "cyber warfare" as "an armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defense, and cyber enabling actions."[2] The definition nearly mirrors the definition for undersea warfare—only the word "cyber" replaces "submarine". The Vice Chairman of the Joint Chiefs of Staff recognizes the similarities to other domains of warfare. However, cyber warfare has unique

characteristics that distinguish it from the other domains. These differences include the theoretical nature of the field, the anonymity of the Internet, the lack of early warning and detection, the problems associated with attribution, private ownership of cyber infrastructure, the "cyber" geography, and the redistribution of power.

Theoretical Nature of Cyberwar

Cyberwar has not been a tradition of warfare. Much like airpower at the beginning of World War One, militaries have not employed cyber warfare on a large scale. The principles and capabilities of cyber warfare are not derived from past military application but from its potential in future conflicts. Criminals have used cyberspace and may show a glimpse of cyber warfare's consequences. Identity theft using the Internet is commonly reported in the news media, causing disruptions in the victims' lives and causing some businesses to distrust the identities of their customers. In November 2008, criminals benefited from fraudulent transactions from 130 ATMs in 49 cities in just a 30-minute period.[3] Moreover, the CIA claims criminal groups operating outside of the United States have broken into utility companies' systems and have extorted payments to prevent a shutdown.[4] In 2000, a prospective employee who was not hired at an Australian sewage treatment plant used a cyber attack to dump thousands of gallons of raw sewage.

Examples of actual cyber warfare are rare. The Estonians assumed the Russian government initiated attacks on Estonia after the relocation of a controversial statue, but later, the Estonians arrested one of its citizens for perpetrating the attacks.[5] The degree of actual Russian government involvement, if any, is not clear. Instead, Russia's conflict with Georgia may have been the first case study of coordinated major military operations with cyber warfare.[6] Prior to the invasion, Georgia experienced denial of service attacks against government and military

communications systems and Georgian news agencies.[7] During the military invasion, the Russians bombed around the Baku-Ceylon pipeline, a principle strategic target in Georgia but intentionally did not hit it.[8] Simultaneously, cyber attacks demonstrated the ability to shut down the pipeline via cyber means without actually doing so. Although the Russian government never claimed responsibility for the cyber attacks, the pattern of cyber activity was consistent with Russia's military action in the physical environment. Neither event was particularly large scale, strategically significant, or even clearly attributable to a particular actor. The empirical evidence on cyber warfare is limited, and drawing too many conclusions on Russia's use of cyber warfare or how this may apply to other actors is dangerous.

Perhaps the most interesting example of a potential cyber warfare attack involves a worm named Stuxnet and an Iranian nuclear facility. Stuxnet spread throughout the world but only affected Siemens-manufactured industrial control systems running with a very specific configuration, the configuration used at Iranian uranium enrichment facilities.[9] The worm caused the Iranian centrifuges to spin outside of its normal operating parameters despite showing normal readings to technicians.[10] The result, according to a *The New York Times* report, is a multiyear delay in the Iranian nuclear program.[11] The United States and/or Israeli governments are reported suspects, but neither admits any involvement.

Do these examples provide insight on how cyber warfare will be used in the future? At this point, cyber warfare has been used so infrequently that making too many conclusions may prove foolhardy. Cyber deterrence will be almost exclusively based on theory. Then again, much has been also written about nuclear deterrence, which only two bombs used in combat for actual experience.

Early Warning and Detection

Cyber warfare occurs at machine speeds.[12] The first indication of an attack may be when the victim perceives he is under attack.[13] Although viruses may be indiscriminate, as one can see from the Stuxnet example, a targeted attack takes a great deal of intelligence. Thus, today's probe may be tomorrow's attack vector.[14] Analyzing seemingly innocuous probes and information is one approach in determining if an attack is pending and to resolve any vulnerabilities. However, the level of noise on many networks makes this an arduous, if not an impossible, task. At present, the cyber environment lacks reliable early warning of attack.

Anonymity and Attribution

Major General Susan Helms of the United States Strategic Command cites cyber attribution as one the major challenges in cyber warfare.[15] She points out several questions one must ask in regard to cyber attacks:

- Was the effect intentional?
- If so, who is responsible?
- How do you mitigate the possibility of third-party intervention to escalate the crisis?

An example of the difficulty and importance of answering these questions before initiating a response was demonstrated on 14 August 2003 when the power went out across much of the northeastern section of the United States.[16] Federal, military, and civilians leaders had to determine if the event—which would eventually cost $7-10 billion in damages—was cyber related and whether it was intentional.

The anonymity of the Internet naturally leads to difficulties in attribution.[17] Hackers are known to exploit seams in US intelligence and law enforcement jurisdictions by launching attacks through intermediary points.[18] For example, an attacker in Iran may compromise a

computer of a private citizen in the United States that subsequently compromises a computer in North Korea that then attacks the intended target in the United States. Since the United States does not maintain law enforcement contacts with North Korea, the information from the North Korean government would have to be obtained through clandestine or covert means (which would most likely negate the possibility of criminal prosecution). When the trail leads from North Korea back to a US citizen, a court order would probably have to be obtained to investigate further. Only then would the investigators trace back to actual perpetrators in Iran.[19]

Whereas criminals and spies have a vested interest in keeping their identities hidden from law enforcement, some actors may be easier to attribute. Larger cyber attacks will likely be in conjunction will physical attacks or in concert with other instruments of power.[20] The attacker is likely not as concerned about keeping his identity hidden as he is with exerting pressure on the victim to gain concessions. In the opening scenario, for example, the Iranians wanted to raise the stakes for the United States to continue the conflict, and probably wanted the Americans to know that it was the perpetrator behind the attacks, even if it did not explicitly take credit for the attacks. However, if a state wishes to engage in covert operations or espionage, it will hide its cyber involvement as it would its physical involvement. The use of Stuxnet against the Iranian nuclear program is a good example. Assuming state involvement, the perpetrator chose not to disclose its involvement. One could also reasonably assume if the means of sabotage would have involved kinetic means (e.g. bombing of key equipment at the facility), the perpetrator would have similarly hidden his role.

The anonymity and difficulty of attribution in cyber warfare increases the possibility of false-flag operations.[21] Third-parties may use cyberspace to escalate a conflict or to otherwise facilitate its objectives. Consider the current conflict in Libya. Suppose the insurgents hacked into the computers of Libyan forces and subsequently attacked key targets in NATO countries

with the hope of antagonizing a harsh response by NATO forces on the Libyan government. Even if the Libyans denied their involvement, they would likely not cooperate to find the true attacker. Furthermore, the Libyan government is vulnerable to a rebel sympathizer with access to a government computer launching the attack. Attribution of covert actors will always be an inexact science, and all source of intelligence must be considered to find the true attacker.

Private Control of Cyber Infrastructures and Cyber Systems

The government does not control many systems or information needed to begin the attribution process in a cyber attack. The private sector owns and operates most of the nation's cyber infrastructure.[22] In fact, the Internet is not a "global commons"; it is a collection of interconnected, mostly private, networks.[23]

The technologies and lines of responsibility between government and private systems are blurry. From a technological perspective, commercial-off-the-shelf products, open-source software, and TCP/IP products comprise an overwhelming presence in virtually every segment of information technology—both in the public sector and the private sector.[24] Large internet service providers use the same equipment as smaller organizations.[25] The vulnerabilities in domain name service (DNS) software are present in large and small servers.[26] While common technologies yield efficiencies, they also yield common vulnerabilities. Western militaries and governments are critically dependent upon expertise and support from the private sector, unlike in any other national security problem.[27] Conceivably, this dependence blurs lines of responsibility. While the private sector is responsible for securing its systems, the government cannot abdicate its responsibility to protect life and property.[28] Yet, unlike in the physical domain, the differences between private security measures (e.g. locks on doors), law

enforcement measures (e.g. neighborhood patrols), and military actions (e.g. repelling invasion) are not well defined in cyberspace.

Cyber Geography and Sovereignty

Cyberspace is not bound by traditional geography; rather, cyberspace has its own geography. A positive aspect of geography in cyberspace is backup data stored off site in case of disaster. Many of Wall Street's computers for electronic trading were physically located in the World Trade Center. Fortunately, the 9/11 attacks did not impact the trades since another server mirroring the data was located across the street.[29] However, this server could have just as easily been in another state or another country. Information resident across international borders entails different jurisdictions and varying degrees of cooperation with the United States government. Furthermore, interconnected computer systems allow some attacks to be launched from anywhere on the planet.

At the physical level, cyber infrastructures have chokepoints, including undersea cables, satellites, and "cyber hotels"—locations where large numbers of fiber-optic cables converge.[30] Dr. Kamal Jabbour of the Air Force Research Labs claims physical control of cyberspace infrastructure allows for the control of information passing through it.[31] Many of the most critical systems require physical access to exploit them, since their operators take measures to mitigate inadvertent or intentional disruptions from external connections.[32] Cyber geography has a physical component, but it also has a non-physical component.

Logically, data can reside anywhere and move dynamically. For example, Facebook randomly assigns data to a data center.[33] Facebook users do not know and probably do not care where their data is stored. Their data may move and the route it takes may change with a flip of the switch or a change in the code. The logical nature of cyberspace differs from other forms of

warfare. Mountains and oceans cannot move; whereas, logical cyber geography can change rapidly.

The application of logical cyber geography comes from computer code. The code that runs software and hardware is also an important component of cyber geography. A system is only vulnerable when a developer writes the code with errors, and the program does something that was not intended.[34] If there are vulnerabilities in the code, they only last as long as the time a developer can fix them and deploy the patch. This concept generates a race between the developer and the attacker. A great attack tool today may be obsolete tomorrow.

Redistribution of Power

Cyber warfare is relatively cheap. A research lab can find vulnerabilities in routing software and other common network components for $3-20 thousand.[35] The exercise "Dark Angel" proved that with $500 million and 3 years time, an adversary could launch devastating attacks against United States infrastructure.[36] States that cannot afford blue-water navies or offensive land and air forces can afford a cyberspace capability.[37] More troubling, terrorists and other non-state actors can afford many of the same capabilities. Cyber power gives these states and non-state actors to have unprecedented operational reach and a capability to strike targets within the American homeland. For those entities willing to use terrorism, the addition of a cyber warfare capability allows them to conduct coordinated operations across multiple domains without the burden of maintaining expensive expeditionary platforms. As opposed to traditional warfare where the defender has the advantage in terms of required active and passive resources, deploying defensive cyber measures costs far more than the corresponding offensive cyber weapons, further shifting power to those with the capability to attack.[38] Given the lower barriers

to entry, reduced operating costs, and operational reach, groups such as al Qaeda, Hamas, and Hezbollah could be capable of launching major or minor attacks against the United States.[39]

Cyber Warfare's Contributions to National Power

Cyber warfare's principles differ somewhat from more traditional forms of warfare; however, its capabilities can produce military and coercive effects. Cyber warfare gives political leaders another tool to influence others to accede to political demands. As with other forms of warfare, cyber warfare has limits, which political and military leaders must consider when implementing strategy.

Nature of Cyber warfare Effects

Based on the DoD's definition of cyber warfare, it can produce three primary effects. First, cyber attacks can cause damage or destroy physical assets. Many critical infrastructure devices rely on Supervisory Control and Data Acquisition (SCADA) and distributed control systems to automate and control tasks, including physical tasks. The Government Accountability Office warns of the catastrophic damage attacks on SCADA systems could impose (e.g. flooding from opening dams or loss of electrical power from overloading electric generators) and also warns that foreign governments or terrorists groups are capable of exploiting the vulnerabilities.[40] The Idaho National Labs demonstrated such a vulnerability in an experiment where a cyber attack caused a power plant generator to self-destruct, damage that would take months to fix.[41] If directed against a dam, massive flooding would result; if directed against a nuclear power plant, an attacker could release widespread radiation.[42]

Cyber warfare can also to cause effects such that an adversary loses confidence in its information. Cyber attacks have the capacity to produce what Clausewitz described as the fog of

war.[43] The Allies went to great lengths to deceive the Germans of the actual location of the landing in France, which ultimately put the German military in a more disadvantageous position. Cyber gives another medium to deceive the adversary and frustrate command and control from a loss in the confidence in the data he is receiving.[44] Nations more dependent on cyber technologies are hurt more from a loss in confidence in these technologies.

Cyber warfare also has the potential to cause the civilian populace to lose confidence in basic institutions. In the opening scenario, the Iranians altered banking information. Next to major physical damage to critical infrastructure, Scott Borg of the US Cyber Consequences Unit ranks the loss of confidence in banking and other financial institutions as the greatest cyber security threat facing the United States.[45] Cyber's ability to induce other security problems, such as restoring confidence in financial institutions, creates the capacity to cause Clausewitzian friction as well as fog.[46]

Cyber warfare has the ability to cause disruption. Denial of service attacks against key nodes is much like an electronic warfare platform jamming a radio channel.[47] Other forms of disruption include the deletion of files. These disruptive activities are not persistent. Network defenders can mitigate denial of service attacks, and files can be restored from backup tapes. But in many cases, attacks do not have to persist. For example, the jamming (electronic or cyber) of a key radar site may last long enough for a strike package of aircraft to move towards their target. The disruption of the air traffic control in the opening scenario lasted only 40 minutes, but key leaders probably spent a great deal more time analyzing the outage and determining a course of action even after recovering from it. Disruption enables the effectiveness of other actions.

Cyber power goes well beyond direct application of cyber warfare. The use of cyberpower enhances other military forces in a myriad of ways. A study of over 12,000 F-15 training sorties found those with Link 16 capability (a tactical data link between aircraft and

other tactical platforms) had an air-to-air kill ratio 2.6 times higher than those without Link 16.[48] Cyber capabilities enable planners to share critical operational and intelligence information to facilitate effects-based targeting, credited with the success of the campaign against Iraq in 1991.[49] Cyber capabilities also enabled PSYOPS by providing the ability to send messages directly to Iraqi commanders.[50] Militaries, particularly the US military, rely on cyber power. Likewise, civilian society also relies upon cyber capabilities for everything from power production to banking to shopping to using social networks to connect with friends, which are potential targets which must be defended.

Cyber warfare & Political Coercion

Cyber warfare's effects are coercive. Cyber warfare is simply incapable of destroying a society or forcefully taking over another nation. As a purely coercive instrument, cyber warfare shares many of the same capabilities and limitations as other coercive tools.

Robert Pape in *Bombing to Win* critiques the ability of military forces to use coercion, particularly through the use of airpower in strategic bombing campaigns.[51] He adds the "risk" and "decapitation" strategies of coercion to the more traditional strategies of punishment and denial.[52] Moreover, Pape defines a risk strategy as one that "slowly raises the possibility of civilian damage"[53] and a decapitation strategy as one that "seeks to achieve both punishment and denial effects by destroying a small collection of crucial leadership targets."[54]

Pape concludes a punishment strategy that uses airpower as its coercive instrument generally fails, since airpower cannot deliver the mass of conventional munitions required to cause sufficient pain for the civilian population to force its government to accede to the enemy's demands.[55] Rather, an aerial punishment strategy is more likely to induce resolve than fear. He sees a risk strategy as a weaker form of punishment. If the use of airpower in a punishment

strategy is unlikely to succeed, then the threat of future gradual punishment is also unlikely to succeed. Pape argues decapitation strategies require a great deal of intelligence to be successful, which may not be feasible. Airpower might be able to isolate leaders and disrupt command and control for a short time but not in the long term. Aerial denial strategies can work, but they are not necessarily the best tool. Airpower alone cannot usually provide enough mass to be successful.

Other domains of warfare suffer limitations in coercive strategy as well. A blockade is sea power's primary tool of coercion.[56] Blockades are effective only against nations particularly vulnerable to overseas trade and without alternative land routes. Land power can engage in a denial strategy by defeating an adversary's army, but it can rarely pursue a punishment strategy until after decisive victory.[57] However, the United States Army (and certainly the Marine Corps) no longer engages in land-only operations, and if it did, it is difficult to image a scenario where it would be successful.

Likewise, cyber coercive strategies suffer from limitations. Whereas the opening scenario describes an Iranian attempt to use a cyber-based punishment strategy presumably to coerce the United States to end the conflict on favorable terms, would such a strategy be effective? If airpower using non-nuclear weapons has been historically incapable of successful coercion due largely to lack of massed destruction, it follows that cyber warfare would have to impose catastrophic punishment. Libicki argues that casualties are the biggest factor in causing war-weariness and points out that no one has yet to die as a result of cyber war.[58] Much like a naval blockade, a more cyber-dependent society would be more sensitive to cyber-imposed punishment. However, as Libicki points out, cyber attacks depend on vulnerabilities in cyber systems, and once exploited, the attacked party can usually mitigate the exploited vulnerability by patching the vulnerability.[59] Thus, repeatability and persistence become major limitations for

cyber warfare. The lack of repeatability makes a cyber risk strategy even weaker than an aerial risk strategy. Likewise, the inability to persist negates a cyber-based decapitation strategy, since command and control can only be disrupted for a short time. A cyber denial strategy is also extraordinarily difficult. Although cyber attacks can incapacitate or even destroy some critical infrastructure, it cannot destroy or incapacitate an adversary's ability to act.

The limitations of each of the domains of warfare may suggest coercion is impossible. However, history has several examples of successful coercion. In 1999, NATO successfully coerced the Serbian government to abandon ethnic cleansing in Kosovo.[60] The air aspect of the campaign was the most visible and played an important role in the coercive strategy. However, the threat of NATO introducing ground troops played a vital role in ending the conflict.[61] The non-military instruments of power contributed to ending the conflict as well. The Russian decision not to support its Serbian allies played an important part of Milosevic's decision to end the conflict.[62]

The synergistic effects of the military domains and the instruments of national power leverage each other's effects and mitigate their limitations. Although cyber warfare's effects cannot normally win a conflict in isolation, it may play an important, perhaps vital part, in a larger strategy. Whether cyber warfare is the centerpiece of the effort, much like airpower was during the 1999 Kosovo conflict or in DESERT STORM, or whether it plays a supporting role to other military domains, such as the role space played during DESERT STORM, it has the potential to play a significant role in future conflicts. As a technologically dependent nation, the United States is particularly vulnerable to a coercive strategy with a major cyber component.[63]

Forms of Deterrence

What exactly are the deterrence objectives? Is the objective to deter "use" of space and cyber weapons, to deter "attacks" in the space and cyber domains, or to deter notable disruptions of our space and cyber networks? Or, is it really all about deterring any type of attack, kinetic or non-kinetic, on the US and her allies? [64]

-Major General Susan Helms

Strategic Deterrence

Deterrence is the inverse of coercion.[65] Since cyber warfare's limitations make it unlikely to succeed in coercion without the use of the military domains or the other instruments of national power, a focus on deterring cyber warfare at the strategic level is like focusing on the symptoms of disease rather than the cause. A 2011 RAND study that analyzes how the People's Republic of China (PRC) would pursue militarily reunification with Taiwan provides a good example.[66] The study concludes the PRC would use cyber attacks to disrupt, delay, and confuse the US response. Yet, the heart of the deterrence problem is not the cyber attacks; rather, the US needs to deter the PRC from invading a US ally.

At the strategic level, deterrence includes all of the instruments of power and involves a relational approach.[67] Deterrence relationships are not static; rather, they change based on the situation.[68] Deterrence may be immediate or general.[69] Immediate deterrence addresses a particular audience during a specific crisis; whereas, general deterrence is steady state and implies numerous audiences. Regardless, deterrence attempts to guide the enemy to come to the conclusion that the costs of action outweigh the costs of inaction. Stephen Blank argues that deterrence must meet three conditions to be successful.[70] First, both sides have to have access to similarly understood data about each side's capabilities, intentions, and resolve. Second, they must have enough time to make the right decision. Third, the party to be deterred must appreciate it has something of significant value to lose.

Most importantly, deterrence is in the mind of the adversary. The deterrent message must—through actions and words—be perceived through the lens of the adversary's view of the geo-political world.[71] The adversary's history and culture will play a major role in his perceptions. For example, if an entity attempted to deter American action with the threat of guerilla warfare, the "Vietnam Syndrome" may cause the President to hesitate due to the US's negative experiences in the Vietnam War much more so than a US president in office prior to the Vietnam War.[72] The enemy's perceptions, not a particular weapon or set of weapons, lead to cost-benefit calculations that ultimately determine whether he will behave aggressively or not.

Nuclear Deterrence

The possible exception to the rule that deterrence is agnostic to a particular set of weapons is when nuclear weapons are involved. As Lawrence Freedman points out in *Deterrence*, "Actual nuclear use would be a catastrophe offending strategic logic as well as ethical principles. But the faint possibility of use, precisely because it would be a catastrophe, left a formable imprint."[73] Even the potential of nuclear conflict drove policies to ensure a non-nuclear conflict did not escalate to a nuclear one.[74] Nuclear deterrence is about preventing destruction on a mass scale.

Cyber warfare does not pose the grave consequences as do nuclear weapons. In fact, cyber warfare shares few similarities. Cyber weapons cannot produce the widespread societal destruction of nuclear weapons, and once used, cyber weapons suffer from limited persistence and repeatability. Nuclear weapons can be used until their stocks are exhausted. Nuclear weapons are expensive and require scarce materials that can reasonably be monitored and controlled; cyber weapons are inexpensive and impossible to track.[75] Nuclear weapons are attributable, have a clear threshold for use, are at the top of the escalation ladder, and are capable

of targeting and destroying enemy military targets; cyber weapons do not have any of these characteristics.[76] Stability in a nuclear deterrence environment relied upon neither side having an effective defense; cyber systems can only be attacked if there is a vulnerability in the code and defense fails. Furthermore, cyber warfare involves potential third-parties and shared responsibilities with the private sector. Although much has been written on nuclear deterrence, the strategic problem set is completely different. Comparing cyber deterrence to nuclear deterrence will lead to seriously flawed conclusions.

Conventional Deterrence

Freedman sees a fundamental difference between nuclear and conventional deterrence, "Conventional deterrence requires a *demonstration* of capability, while nuclear deterrence is mere matter of will."[77] The necessity for the demonstration of capability leads conventional deterrence to fail. The strategist Collin S. Gray goes so far as to say, "Deterrence is inherently unreliable."[78] In fact, history is plush with examples of failed deterrence—the attack on Pearl Harbor, Israel's belief that their military demonstrations would hold the Arabs at bay in 1973, and Saddam Hussein's decision to remain in Kuwait in 1990.[79]

Cyber warfare, as a subset of non-nuclear warfare, suffers from the same dilemmas. Stephen Blank contends that in conventional deterrence both sides must be prepared to go to war.[80] Limited war sometimes happens, which builds credibility for future conventional deterrence. He follows that in the cyber domain nations can expect near constant low-level cyber conflict as adversaries probe capabilities and thresholds. While this proposition may seem daunting, former Secretary of Defense William Perry offers a counterview by stating that cyber warfare's stealth, global and real-time reconnaissance, precision strike, and small logistics requirements will provide a credible deterrent for theater-level conventional war.[81] On one hand,

conventional deterrence theory drives a need from time to time to demonstrate cyber capabilities and engage in near constant cyber conflict. On the other hand, the capabilities may be a stabilizing factor to prevent regional conflicts.

Deterring Non-State Actors

Non nation-state deterrence models, such as terror and criminal deterrence models are more complicated but may include aspects applicable to cyber. Both models focus primarily on deterrence through denying the actor a benefit rather than focusing on imposing costs. Gray cites the lack of a "return address" as a major difficulty when trying to deter terror groups.[82] By their nature, terror groups take measures to avoid detection and do not have populations or overt military forces against which to retaliate. However, groups such as al Qaeda, though probably not deterrable by killing its soldiers, can be deterred with credible threats against the leadership, by exploiting seams in its organizational structure, or by convincing potential recruits through antiterrorism efforts that jihad is futile.[83] Many of these same approaches, particularly the denial of potential benefits, apply to cyberspace.

In criminal deterrence, the likelihood of getting caught is more important than the severity of the punishment.[84] The application of anti-crime measures (e.g. security guards, locks on doors and windows, etc.) plays an important role as well.[85] A third factor is the concept of a societal norm that regards criminality as an improper lifestyle. This norm tends to prevent people from becoming criminals in the first place.[86] Studies have shown people with increased ties to family and positive role models are less likely to commit crime. From a cyber perspective, the combination of attribution, preventative measures, and an international norm making cyber warfare a taboo act are possible similar applications of criminal deterrence.

However, strategists must not mirror criminal deterrence too closely. Freedman contends that the major difference between domestic law enforcement and international deterrence is the generally held belief of the supreme authority of the state's monopoly on the use of force to enforce the law.[87] Few criminals retaliate against law enforcement or judicial institutions after being punished. Also, criminals usually will move to a softer target if the costs are too great. For the most part, they do not care who they victimize; they care more about what they receive from their criminal behavior. Contrary to criminals, in the international arena, targets are politically important, and there is no recognition of a superior authority that would prevent retaliation to punitive measures.

Deterring Particular Weapons

While the use of a particular weapon or domain is irrelevant at the strategic level (except for nuclear weapons), militaries may wish to deter particular weapons at the operational or tactical level, especially if the weapon's use will have strategic consequences. As an example from the opening scenario, Iran had few means available to attack the United States' homeland. In this scenario, deterring the use of cyber weapons would have had strategic consequences, since cyber warfare was a major enabler of Iran's operational reach.

Deterring particular weapons is nothing new. Since World War One, the United States has actively deterred the use of chemical weapons. It equips its military with protective devices, such as masks, and trains to operate in contaminated environments.[88] It has signed a treaty that clearly sets an international norm against their use.[89]Furthermore, the United States has stated if chemical weapons are used, its response will be "overwhelming and devastating."[90]

Aspects of Deterring Cyber Warfare

With a legitimate need to incorporate cyber deterrence, a deterrent relationship must include clearly communicated, credible, contingent promises to respond to aggression.[91] Furthermore, the ability for the enemy to impose harm and the control of escalation are important governing factors in deterring cyber warfare.

The Enemy's Ability to Impose Harm

If the enemy cannot reasonably expect benefits from imposing harm, he will have no need to attack. Following this logic, the lesser the potential impact, the lesser the likelihood the enemy will attack. Unfortunately, at the present time there is little doubt that a conventional power could launch a successful, coordinated cyber attack on US infrastructure.[92] Some of the US's vulnerabilities have already been discussed earlier; however, vulnerabilities exist across diverse areas of American society. Denying the enemy's expected benefits of a cyber attack by protecting systems is one approach.

Resilience, or the ability to survive despite attack, offers another alternative. Deterrence is enhanced as the probability of an attack failing to achieve its full potential decreases.[93] Communicating and demonstrating resiliency may be as important as actually being resilient. The US economy proved to be less fragile than thought after the 9/11 attacks.[94] The Germans and Japanese did not buckle under the pressure of Allied bombing of cities in World War Two. Demonstrating similar resilience in the face of cyber attack enhances deterrence.

Credibility

Both actions and words build credibility for deterrence. Libicki claims a good defense adds to credibility, since attacks are less likely to be successful.[95] Past actions against one adversary plays a major role in deterring future adversaries.[96] A weak (or no) response may lead

a future adversary to believe he can expect a weak response; conversely, a strong response implies a strong response in the future. In terms of cyber deterrence, an attack that is not detected weakens deterrence; however, a false positive detection is worse, since a new enemy may be created and legitimacy suffers.[97] Credible actions must be matched with a plan to implement them.

The lack of clear cyber doctrine also hurts deterrence.[98] Doctrine should clarify roles and responsibilities. The lack of doctrine may lead an adversary to believe a response is not a credible threat, as the opponent has not developed a methodology to respond. Several factors contribute to the lack of doctrine development. The difficulty of attributing the source of the attack frustrates the ability to determine if the event is a law enforcement, military, or an intelligence matter and delays assignment of roles and responsibilities.[99] The lack of a history of attacks is also a contributing factor. Regardless of the reasons, Brig Gen Huba Wass de Czege claims a doctrine of drastic counterattacks to cyber warfare is required to be a credible deterrent.[100] Although de Czege does not address the proportionality of the response and its relationship to credibility, he complements Freedman by asserting that to be credible the adversary must believe threats will be enforced.[101]

Threat of Response

The threat of response in cyberspace represents the costs to the attacker. A retaliatory strike against the attacking machine does little more than to damage a computer worth a few hundred dollars, which from the attack's perspective may be worth the cost.[102] Of course, this assumes that the supposed source was truly the original attacker and not an intermediary. Since attackers may use a series of computers to cover their tracks, before responding the victim must ensure it knows the true identity of the attacker. Given that false-flag operations will increase

with the risk of retaliation, speedy attribution is vital to any response.[103] Had Estonia or another friendly country blindly responded to immediate source of attacks, it would have damaged innocent systems in the United States, China, and Europe.[104]

A tit-for-tat cyberwar goes against the side that is most reliant on cyber and has the most to lose. Assuming correct attribution, retaliation cannot simply neutralize the attacking system; it must strike back (via cyber or other means) at something of value such that an adversary will receive a strategic setback as a result of the response.[105] All of the instruments of power must be on the table, and the adversary must recognize this to be true for the threat to have meaning.

Controlling Escalation

A consideration of any response is to respond with an appropriately strong response without needlessly escalating the conflict. For example, a defaced website may warrant a diplomatic response; an attack on a power plant may warrant a cyber or a physical attack on part of the adversary's infrastructure. Establishing thresholds is difficult but necessary. States must walk a fine line between setting the line too high or too low.[106] If the response is too violent, the adversary may perceive injustice and follow up with increasing more violent attacks.[107] Since deterrence is not perfect and it sometimes fails, states need to balance the need to response with pain and the need to control the conflict. Since the majority of cyber attacks are unlikely to cause death or major destruction, state may choose to tolerate of a cyber attack in order to prevent escalation of a larger conflict.

Communication

As Gray points out, deterrence "is in the minds of the enemy leaders. [I]t is their worldview, not ours, that must determine whether or not deterrence works."[108] The deterrent message must be culturally packaged to make sense from the adversary's point of view. The

adversary must clearly comprehend the boundaries and the risks associated with crossing them;[109] otherwise, the enemy's misinterpretation of the message may result in aggression despite the deterrent message.

While diplomats have familiarity with communicating messages in a culturally sensitive manner, communicating messages to deter cyber warfare can be problematic, who have different interests and worldviews. First, the message to deter cyber aggression must go to multiple audiences simultaneously.[110] States must ensure the potential audiences perceive the deterrent messages reasonably similarly. Second, in the cyber environment, methods are not available to signal cyber intentions to the enemy.[111] During the Cold War, if a Soviet submarine got too close to United States, the United States could signal its disapproval by increasing the alert level of its bomber force. Not only did this action avoid having to make a politically uncomfortable statement, it backed the words of deterrence with deeds. The cyber environment has no equivalent.

Existing US Policy

The United States' policy on cyber deterrence is somewhat vague. International law provides guidelines on some cyber activity and warfare in general. Disparate US Government documents also provide insight on the Government's position, but a single policy document does not exist specifically for cyber deterrence. Finally, informal standards also drive cyber norms and perceivably substitute as policy.

International Law

International law governs aspects of cyber activity and the use of force. Article 2, paragraph 4 of the United Nations charter determines which actions constitute the use of force

and when the use of force is appropriate.[112] Specifically, the charter prohibits "the threat or use of force against the territorial integrity or political independence of any state, or in a manner inconsistent with the purpose of the United Nations."[113] Legal experts widely interpret the charter allows anything short of violent force, since non-violent means are methods of solving conflict without war. Following this logic, cyber operations are only prohibited if they intentionally cause death or physical destruction. Furthermore, international agreements immunize countries against aggression or intervention solely because a message transited its territory.[114] Suppose Country A launches a cyber attack on Country B, and the attack transits County C's infrastructure and occurs without Country C's knowledge. Perceivably, this doctrine would prevent Country B from retaliating against Country C. Yet, these examples of international law were developed prior to the development of modern information systems, and their relevance and interpretation in cyber warfare is still yet to be determined.

Formal US Policy

The relative youth of cyber technology entices debate over the role of the military and the government in general. The *National Security Strategy* recognizes the importance of cyber technologies to the United States and focuses on two broad categories to secure cyberspace—investment in people and technologies and strengthened partnerships.[115] The focus on investment centers on preventing attack and on resiliency, particularly with government systems. The focus on strengthening partnerships is more robust:

> We will also strengthen our international partnerships on a range of issues, including the development of ***norms for acceptable conduct in cyberspace***; laws concerning ***cybercrime***; data preservation, protection, and ***privacy***; and approaches for network ***defense and response to cyber attacks***. We will work with all the key players—including all levels of government and the private sector, nationally and internationally—to ***investigate cyber intrusion*** and to ensure an ***organized and unified response to future cyber incidents.*** Just as we do for natural disasters, we have to have ***plans and resources in place*** beforehand.[116]

The document explicitly links the aforementioned actions to a means of deterring cyberwafware. The *National Security Strategy* acknowledges many of the challenges associated with cyber deterrence. However, it leaves the acceptable boundaries vague (in fact, one could infer that the document sets a goal to define these bounds with the "development of norms" clause) and does not communicate the severity of a response or if a response will be limited to a cyber retaliation or may be expanded to include other instruments of powers.

The 2003 *National Strategy to Secure Cyberspace* addresses response somewhat more explicitly by stating, "When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner."[117] The strategy provides a starting point, but it does not provide much direction on what will be done during and after a cyber attack.

The 2010 *National Cyber Incident Response Plan* places primary responsibility for responding to cyber incidents with DHS.[118] DHS is responsible for coordinating with law enforcement agencies, specifically the Federal Bureau of Investigation and the United States Secret Service as well as with other Federal agencies to include the intelligence community. DHS also is tasked with facilitating cooperation between the federal government and the private sector. The Department of Defense performs a supporting role, but the plan explicitly stipulates the President can authorize military action to counter attacks on critical infrastructures.[119]

Under existing law the President has broad emergency powers over anything transmitting over the electromagnetic spectrum.[120] The proposed Protecting Cyberspace as a National Asset Act of 2010 explicitly would give the President the authority to declare a national cyber emergency that would subsequently allow the government to direct private entities to comply

with emergency measures in response to a cyber-based national security threat.[121] The introduction of this bill suggests, at a minimum, a degree of legal ambiguity concerning the government's authority to direct the private sector to undertake certain measures even in the face of a national crisis. Since nobody can direct any measures, obtaining unity of effort will require collaboration and cooperation.

Doctrine

The Vice Chairman of the Joint Chiefs of Staff's attempt to develop common cyber-related definitions[122] may eventually lead to a joint cyberspace operations doctrine. Joint doctrine specifically on cyberspace operations has yet to be published.[123] The study, *Securing Cyberspace for the 44th Presidency*, criticizes the military's lack of doctrine and claims it weakens deterrence in part by failing to clarify roles and missions within the government and in part by failing to communicate credibility to the enemy.[124] In particular, it cites the overclassification of cyber capabilities as a problem. In the Cold War, the weapons' general capabilities were known, while the specific design information was closely guarded. Cyber capabilities, on the other hand, are a closely guarded secret. Much like the doomsday machine in the movie *Dr. Stangelove*, cyber weapons that could be used to deter cyber attacks on the US are worthless if nobody knows they exist.[125] The *National Military Strategy for Cyberspace Operations* (*NMS-CO*) acknowledges limitations in joint doctrine in the cyber domain and sets a goal to correct the deficiency.[126]

The Air Force's doctrine is somewhat more mature than the joint doctrine. In July 2010, the Air Force published AFDD 3-12, *Cyberspace Operations*, the first doctrine specifically dedicated to cyberspace operations.[127] AFDD 3-12 fails to clarify what—if any—role the Air Force has in defending against cyber attacks on critical infrastructure. AFDD 3-12 specifically

states that the Air Force is heavily dependent upon the SCADA and distributed control systems in civilian critical infrastructure, but it offers no solution on how these systems will be defended.[128] AFDD 3-12 focuses on defending Air Force-unique system and providing an offensive capability. It is a start, but US military doctrine as whole is lacking.

Informal Norms/Policies

As has been discussed, most of the United States' critical infrastructure is owned and operated by the private sector. Thus, non-governmental policy has an impact on the nation's cyber deterrence posture. Libicki argues that in one sense a lack of a government deterrence policy actually enhances private-sector security.[129] He claims the only incentive for utilities and other critical infrastructure companies to provide security is the threat of being sued. If the United States characterized cyber attacks on critical infrastructure as acts of war, the companies would be immunized against liability, negating their primary incentive to protect their systems. Even if this argument is true, critical infrastructure companies have little incentive to improve security, since the theoretical threat of a lawsuit is in many cases less than the tangible costs of upgrading security.[130]

The processes to share information are informal but critical to defending critical cyber assets. Information Sharing and Analysis Centers (ISACs) provide a forum to exchange information among the private-sector members and the applicable government entities.[131] The membership in an ISAC or the information shared with the ISAC is voluntary. Private companies are reluctant to disclose information on cyber events due to financial or liability concerns. The lack of reporting not only hurts deterrence, it prevents the government from being able to learn lessons from the attacks.[132]

A Potential Framework for Deterrence

Strategic Deterrence

Since deterrence at the strategic level involves deterring behavior rather than deterring a specific means of aggression, policymakers must include cyber capabilities—offensive and defensive—into a larger concept of deterrence.[133] In some cases, the addition of cyber into the deterrence calculus means little. In other cases, cyber may be one of the few tools a weaker nation has to coerce the United States. Regardless, the United States needs to define "red lines" in the cyber environment that are not to be crossed.[134] Freedman, a proponent of norms-based deterrence, argues the establishment of international norms provides a better model of deterrence, in part because pressure to conform comes not from a single country but from the international community as a whole.[135] In the context of general deterrence, the international norms provide defined "red lines".

Although general deterrence has its role, deterrence is not static and requires inclusion into a broader set of deterrence relationships.[136] Kugler argues that even in a strategic paradigm, cyber deterrence cannot conform to a one-size-fits-all approach.[137] Deterrence must also consider the adversary, its capabilities, and the appropriate response. Cyber deterrence will have a piece to play in these immediate deterrence situations along with capabilities from the other warfighting domains and the other instruments of power. Culturally appropriate communication is important. The implementation of cyber deterrence must include resiliency, organizational changes, technological tools, and retaliatory measures.

Resiliency

Successful deterrence requires either denying expected benefits to the enemy or raising his expected costs. Resilience denies benefits to the enemy and may be the best form of

deterrence against cyber warfare, particularly against non-state actors where offensive action is often difficult. In cyber warfare, the offensive holds an advantage over the defense.[138] The attacker can choose the time and place of the attack. He can attack at the speed of light. In order for the defender to achieve true defense-in-depth, he must rely on internationally coordinated plans and responses. The defender also must have situational awareness on vulnerabilities across all types of national critical infrastructure. Enhancing information sharing and speedy attribution help limit the impact of an attack. Interestingly, another advantage of a strong defense is that is largely attribution agnostic. These factors suggest that showing legitimacy and mitigating the pain associated with a cyber attack is more effective than preventing one.[139]

Logical and physical redundancy of critical infrastructure systems is ideal, but complete redundancy would probably cost more than what is palatable. At a minimum, the United States should pursue redundancy and resilience at critical chokepoints (e.g. undersea cables, satellites, ground stations, and cyber hotels).[140] A more conservative approach would model the North American electrical grid. The electric grid has fault-tolerant, regional connections designed to limit the extent of a major outage.[141] Critical infrastructure owners should design systems to fail in a similar manner. Limiting the extent of an attack, limits the damages. For those acting covertly, they may calculate that the risk of being caught may not be worth it for limited damage.

Another aspect of resilience is being able to operate despite the loss of a cyber system. Much like training to operate in a chemically contaminated environment, aircrews train to operate in an environment where global positioning system is unavailable or degraded.[142] The military and critical infrastructure operators should plan to function in cyber-degraded environments. Periodically, they should exercise their ability to execute their plans. If the adversary knows potential targets have plans, training, and exercises to continue operations

despite cyber attacks, the expected value of the attack decreases. Cyber warfare is likely to happen, and military and civilian entities must be prepared to move past its disruptive effects.

Organizational Changes

Changes in the legal and regulatory framework are vital to reducing vulnerabilities. The *Securing Cyberspace for the 44th Presidency* concluded voluntary action is not working and that the government must regulate critical infrastructure operators.[143] Regulators must apply regulations intelligently. Regulations should not stifle an operator's ability to react to a fast moving situation while providing incentives to secure systems critical to the nation. Regulations should also mandate operators of critical cyber systems communicate incidents and share data on intrusion techniques. The US views cyberspace as a global commons, but its laws do not reflect this viewpoint.[144] Furthermore, the legal system does not clearly and consistently categorize cyber attacks.[145] At times, cyber attacks are considered criminal matters; other times, they are treated as military activity or covert operations. The legal ambiguity undoubtedly causes confusion and hesitation and limits flexibility. Major General Lord commented, "It's easier for us to get approval to do a kinetic strike with a 2,000-pound bomb than it is to do a non-kinetic cyber activity."[146]

Cooperation among government entities and between the public and private sectors also builds credibility and enhances deterrence.[147] Greater transparency in cyber operations is a first step. Gen James Cartwright, the Vice Chairman of the Joint Chiefs of Staff, complained that cyber integration is hurt by overclassification.[148] The reconnaissance team, the defenders, and the attackers do not share information with each other. Given the difficulties of sharing information within the Department of Defense, the information sharing difficulties are magnified across other government organizations and especially with the private sector. Exercising cyber

attacks on critical infrastructure may be one of the best ways to kick-start cooperation. In March 2008, DHS sponsored CYBER STORM II, a simulated cyber attack on critical infrastructure systems in the information technology, communications, chemical, and transportation (rail and pipeline) sectors. The findings of the exercise concluded standard operating procedures, rapid information sharing, and the need for stakeholders to know and clarify responsibilities were important areas needing improvement.[149] Information flow was largely unidirectional and did not provide feedback whether the information was useful or provide robust information to all participants.[150]

As cooperation and trust between organizations improves, a public-private partnership may gain the ability for ISPs to disconnect from harmful or attacking networks. ISPs have "peer connection", interconnections between ISPs.[151] In one case, security researchers determined a particular network was responsible for 75% of the world's spam and hosted 40 child pornography sites. By convincing peered ISPs to disconnect, the amount of spam instantly dropped around the world. This concept may be a valuable tool in the future for the United States, but its success requires a great deal of cooperation both domestically and internationally. In extreme cases, the government may need the authority to direct disconnections. Legal authorities must be clarified before this government-directed tactic is needed.

The military must make doctrine more robust. This includes both offensive and defensive capabilities and relating these capabilities to deterrence. The military should have plans, organizations, and relationships to integrate cyber capabilities with other military capabilities and other instruments of power. While the doctrine will never state policy, it should provide potential adversaries a glimpse of what may happen if they cross a red line. Military leaders must also acknowledge doctrine on cyber warfare will change more often than other doctrine. Frequent changes should not dissuade military leaders from publishing doctrine.

Technological Tools

In testimony to Congress, General Kevin Chilton recognized two major hurdles to address detection, and ultimately attribution, of cyber attacks.[152] First, the military needs to focus on high-tech intelligence, including attribution technologies. Seemingly minor event may serve as precursors to bigger attacks. The government must get better at attribution. Cyber operators need timely and accurate attribution of attackers. Identity management is a possible solution. After the implementation of the Common Access Card, intrusions in the DoD decreased 50%.[153] Authenticating other critical data is crucial to maintaining confidence in the data. Checksum and hash values are good, but more sophisticated and possibly redundant tools are needed for key data. Second, cyber defenders need to anticipate threats before they arrive.[154] Detailed, all-source intelligence can provide some warning. Systems designed to learn and adapt during an attack provide another method of accomplishing this vision.[155]

Some countries employ the concept of a country-level firewall capable of monitoring all traffic and capable of nearly cutting off from the outside world.[156] The concept of inspecting items at the border of a country is not new. However, the concept of inspecting every bit of information transiting across the American border is probably not feasible. Monitoring key nodes is feasible, though. In July 2010, the *Wall Street Journal* alleged that the NSA was developing a program called Perfect Citizen, a network of sensors to protect critical infrastructure sites, including nuclear power plants.[157] The NSA quickly denied any such monitoring and insisted Perfect Citizen was "purely a vulnerability and capabilities development contract." The NSA would neither confirm nor deny additional details regarding Perfect Citizen.[158] Yet, a Perfect Citizen-like system is needed to help provide defense in depth.

Honey pots could be added to a system like that originally described by the *Wall Street Journal*. Honey pots are decoy computers or networks intended to deceive an attacker into

thinking a honey pot is an operational computer or an operational network. Honey pots are used to disrupt and delay attackers.[159] They are also intelligence gathering platforms causing attackers to disclose their tactics and procedures, thereby providing valuable information for future defense and deterrence activities. No technological solution is a silver bullet. Multiple layers and multiple tools are needed to achieve defense in depth.

Retaliatory Measures

If deterrence did not include the risk of punishment, the only thing that would deter an adversary would be the expense of actually mounting the attack. Security enhancements and resiliency are important measures, but these measures are much more effective when backed by a credible threat of retaliation that is clearly communicated in a culturally appropriate context.[160] If an adversary rendered military or key financial systems inoperable, the United States should justifiably respond.[161] In this situation, a state could expect the response would involve a countervalue target, which may not be limited to a cyber attack. Gen Chilton's Congressional testimony made clear that responses to cyber attacks could involve traditional military actions and the application of other instruments of power.[162] As discussed earlier, a cyber attack against the attacking machine yields little value. A sense of symmetry comes not from symmetric tactics or similar targets; rather, symmetry derives from the imposition of a similar degree of pain in counterstrike.[163]

Military doctrine and policy statements should address several issues on retaliation. First, speedy attribution is vital. Covert operations, 3rd parties, certain non-state actors, and actions taken to prepare the cyber battlefield have vested interests to hide their identities. In a shooting war, attribution may not be a major concern, and the threshold to respond is much less.

Conclusions

The time has arrived to demystify cyber warfare. In the modern world, no domain of warfare is likely to singularly coerce a nation to accede to the political demands of another party. Cyberwafare provides a tool that when packaged with other tools can generate effects to achieve political goals. Thus, the ultimate strategic goal is not to deter the use of a particular tool of coercion; the goal is to deter the very use of coercion.

Deterring against individual tools is inappropriate at the strategic level. However, deterring individual weapons—including cyber weapons—can be vital parts of operational and tactical plans, particularly when the use of cyber weapons has strategic consequences. In these situations deterring the use of cyber weapons is entirely appropriate. Yet, cyber deterrence does not neatly fit into any deterrence model but has differences and similarities to several models. Unlike nuclear deterrence, a breakdown of cyber deterrence does not result in society changing consequences. As with conventional warfare, cyber warfare may require a demonstration of capability, perhaps in hostile conflicts, to deter future adversaries. Cyber deterrence also follows some aspects of the criminal deterrence model in that the likelihood of getting caught likely plays a major role. Attribution, a difficult prospect in cyberspace, is necessary to deter terrorists and 3rd party agitators looking to escalate conflicts for their group's gain. Furthermore, setting an international norm against "bad" cyber behavior is an option. Of course, this also binds the United States to complying to the norm.

A strong defense deters those who otherwise cannot be identified; however, in cyberspace, attackers have the advantage over defenders. Resilience—both operational and technological—becomes more important than defense. Both military and civilian operators must

credibly prove they can operate despite attacks. Until intelligence can conclusively identify the attackers, deterrence relies on denying benefits to the enemy.

However, once the attacker is identified, in order to deter future attacks, the United States must retaliate appropriately. Cyber weapons could be used if they are best to produce the desire effects and objectives, but the United States is not limited to them. The response may involve any aspect of the military or any other instrument of power. Credibility, capability, and effective communication to potential adversaries are as important to retaliation as the selection of the response tools.

Cyber deterrence may never be perfect, but some of its weaknesses can be mitigated. In many cases, it will always be a race between the attacker and the developers and administrators trust into unwitting defense roles. The United States must credibly communicate resolve in deterring cyber attacks. Exercises and demonstrations need to back up official statements. Policy changes need to facilitate the government's ability to adequately protect its citizens and to effectively cooperate with foreign and domestic partners and between the public and private sectors. The policy must include spelling out which government agencies are responsible for defending civilian cyber systems, just as the government defends the borders, the coasts, and the airspace. Upgrades in technology should allow greater control and attribution, which will have ripple effects across the spectrum of deterrence.

Cyber deterrence is challenging. It lacks a historical basis, and the "known" facts may lead a rational person to believe that cyber deterrence is destined to fail. Yet, similarities to other problems also lead a rational person to see commonality between cyber warfare and other forms of warfare. Cyber warfare may not be deterrable all the time, just like other forms of warfare are not universally deterrable. Integrating cyber weapons into a broader strategic context provides the best chance to address the challenges associated with cyber deterrence.

[1] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), iii.
[2] Gen James A. Cartwright to Chiefs of the Military Services, Commanders of the Combatant Commands, and Directors of the Joint Staff Directorates, memorandum, n.d.
[3] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: The White House, n.d.), 2.
[4] Clay Wilson, "Cyber Crime," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 433.
[5] BBC News, "Estonia Fines Man for 'Cyber War," 25 January 2008, http://news.bbc.co.uk/2/hi/technology/7208511.stm.
[6] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, 6 January 2011, 2, http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf..
[7] Ibid, 6.
[8] Ibid 4-5.
[9] William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, 15 January 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&ref=general&src=me&pagewanted=all.
[10] Nicholas Falliere, Liam O. Murchu, and Eric Chien. "W32.Stuxnet Dossier," version 1.4 (February 2011). Symantec Corporation. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Sources differ on the exact nature of the effects on the centrifuges. Broad et al. claim that Stuxnet caused the centrifuges to spin "wildly out of control." Falliere et al., "W32.Stuxnet Dossier," pg 43, describes the virus causing programmable logic controllers to change speeds at programmed intervals. What is clear is that Stuxnet caused the centrifuge to operate outside of its recommended operating parameters and that the operators received readings falsely indicating normal operation.
[11] Broad et al., "Israeli Test on Worm Called Crucial in Iran Nuclear Delay."
[12] John W. Gloystein, "Cyberdeterrence in 2035: Redefining the Framework for Success," Air War College Research Paper, 10 February 2010, 8.
[13] Libicki, *Cyberdeterrence and Cyberwar*, 62.
[14] Kevin R. Beeker, "Strategic Deterrence in Cyberspace: Practical Application," Air Force Institute of Technology research paper, June 2009, 62.
[15] Susan J. Helms, "Schriever Wargame 2010: Thoughts on Deterrence in the Non-Kinetic Domain," *High Frontier* 7, no. 1 (November 2010): 14.
[16] Michael Dumiak, "Casus Belli," *Defense Technology International* 4, no. 8 (1 September 2010): 31.
[17] Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, 15 July 2010, 10.
[18] Bonnie N. Adkins, "The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?" Air Command and Staff College research paper, April 2001, 17.
[19] This example only considers the legal status of the computers and not of the transmission path. The process becomes much more difficult if LE/intelligence agencies need to investigate ISPs, undersea cable telecommunications providers, satellite providers, etc. The number of ISP and telecommunication providers dictate a large number of records to collect.
[20] Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 317-318.
[21] Libicki, *Cyberdeterrence and Cyberwar*, 44
[22] Levon R. Anderson, "Countering State-Sponsored Cyber Attacks: Who Should Lead?" US Army War College research paper, 30 March 2007, 6.
[23] "Cyberwar," *Economist* 396, no. 8689 (3 July 2010): 12.

[24] William D. O'Neil, "Cyberspace and Infrastructure," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 128.
[25] Edward Skoudis, "Information Security Issues in Cyberspace," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 183.
[26] John A. McCarthy et al."Cyberpower and Critical Infrastructure: A Critical Assessment of Federal Efforts," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 549.
[27] Gregory J. Rattray, "An Environmental Approach to Cyberpower," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 270.
[28] McCarthy et al, "Cyberpower and Critical Infrastructure," 551.
[29] Patrick Allen, *Information Operations Planning* (Norwood, MA: Artech Housem, 2007), 32.
[30] Rattray, "An Environmental Approach to Cyberpower," 259, and Stuart H. Starr, "Toward a Preliminary Theory of Cyberspace," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 58.
[31] Gloystein, "Cyberdeterrence in 2035," 7.
[32] Libicki, *Cyberdeterrence and Cyberwar*, 18-19.
[33] Jeff Rothschild, "High Performance at Massive Scale – Lessons Learned at Facebook." Address. University of California, San Diego, 8 October 2009.
[34] Libicki, *Cyberdeterrence and Cyberwar*, xiv.
[35] Skoudis, "Information Security Issues in Cyberspace," 183.
[36] Beeker, "Strategic Deterrence in Cyberspace," 11.
[37] Kugler, "Deterrence of Cyber Attacks," 316.
[38] Huba Wass de Czege, "Warfare by Internet: The Logic of Strategic Deterrence, Defense, and Attack," *Military Review*, July-August 2010, 92.
[39] Kugler, "Deterrence of Cyber Attacks," 338.
[40] Government Accountability Office, *Critical Infrastructure Protection: Challenges and Efforts to Control Systems*, GAO-04-354, March 2004, 11.
[41] Jeanne Meserve, "Mouse Click Could Plunge a City into Darkness, Experts Say," *CNN.com*, 27 September 2007. http://articles.cnn.com/2007-09-27/us/power.at.risk_1_generator-experiment-cnn?_s=PM:US.
[42] McCarty et al, "Cyberpower and Critical Infrastructure," 549-550.
[43] James A. Lewis, "Thresholds for Cyberwar," Center for Strategic Studies Report (Washington, DC: Center for Strategic Studies, September 2010), 4-5.
[44] Detecting incidents where data is changed is much more difficult. While a user normally knows if a system crashes, he may not know if data is subtlety changed.
[45] Lindsay Trimble, "Senior Leader Perspective: Scott Borg," National Security Cyberspace Initiative newsletter, Smithfield, VA, June 2010, 2. http://nsci-va.org/SeniorLeaderPerspectives/2010-06-17-CyberPro_interview_Scott_Borg.pdf.
[46] For a discussion on the concept of friction in war see Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton university Press, 1976), 119.
[47] Skoudis, "Information Security Issues," 171.
[48] Martin C. Libicki, "Military Cyberpower," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 282-283.
[49] Richard G. Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq* (Washington, DC: Air Force History and Museums Program, 2002),
[50] Allen, *Information Operations Planning*, 10.
[51] See Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996). Pape examines the strategic bombing campaigns against both Germany and Japan during World War Two and the bombing campaigns during the Korean War, the Vietnam War, and Operation Desert Storm.
[52] Ibid, 12-54.

[53] Ibid, 18.
[54] Ibid, 54.
[55] Ibid, 316.
[56] Ibid, 42-43.
[57] Ibid, 41.
[58] Libicki, *Cyberdeterrence and Cyberwar*, 122.
[59] Ibid, 56.
[60] See Benjamin S. Lambeth, *NATO's AirWar for Kosovo: A Strategic and Operational Assessment* (Santa Monica, CA: RAND Corporation, 2001). Overall, the conflict in Kosovo prevented the Serbian Government from perpetuating a large-scale eviction and/or extermination of the Kosovar Albanians. Lambeth discusses (pg 24-25) Milosevic's atrocities after the NATO campaign began. Yet, despite the killings, NATO was ultimately able to compel the Serbia to accede to its demands and to stop further genocide in Kosovo.
[61] Ibid, 72-77.
[62] Ibid, 81.
[63] Libicki, *Cyberdeterrence and Cyberwar*, 28.
[64] Helms, "Schriever Wargame 2010," 13.
[65] Lawrence Freedman, *Deterrence* (Cambridge, UK: Polity Press, 2004), 65.
[66] Cliff et al., *Shaking the Heavens and Splitting the Earth: Chinese Air Force Employment Concepts in the 21st Century* (Santa Monica, CA: RAND Corporation, 2011), 189.
[67] Freedman, *Deterrence*, 4.
[68] Helms, "Schriever Wargame 2010," 12-13.
[69] Freedman, *Deterrence*, 40-42.
[70] Stephen Blank, "Can Information Warfare be Deterred?" *Defense Analysis* 17, no. 2 (August 2001), 131.
[71] Helms, "Schriever Wargame 2010," 12-13.
[72] Mindaugus Rekasius, "Unconventional Deterrence Strategy," Naval Postgraduate School thesis, June 2005, 21.
[73] Freedman, *Deterrence*, 12.
[74] Kugler, "Deterrence of Cyber Attacks," 323.
[75] Beeker, "Strategic Deterrence in Cyberspace," 11.
[76] Libicki, *Cyberdeterrence and Cyberwar*, xvi.
[77] Freedman, *Deterrence*, 39. (Emphasis added).
[78] Collin S. Gray, *Maintaining Effective Deterrence* (Carlisle Barracks, PA: Army War College Strategic Studies Institute, August 2003), 17.
[79] Blank, "Can Information Warfare be Deterred?" 130-131.
[80] Ibid, 128.
[81] Ibid, 123. Although Secretary Perry states that cyber warfare may deter conventional war, he does not make the same assertion for guerilla war. As discussed in this paper, cyber warfare can be used in punishment strategies, but guerillas often have little for a major power to punish.
[82] Gray, *Maintaining Effective Deterrence*, 7.
[83] Ibid, 28.
[84] Freedman, *Deterrence*, 64.
[85] Ibid, 60.
[86] Ibid, 15.
[87] Ibid, 9.
[88] Beeker, "Strategic Deterrence in Cyberspace," 41.
[89] United States Chemical Weapons Convention. "About the CWC," United States Department of State, Bureau of International Security and Nonproliferation and United States Department of Commerce, Bureau of Industry and Security, http://www.cwc.gov/cwc_about.html (accessed 5 April 2011).

[90] Conley, "Not with Impunity: Assessing US Policy for Retaliating to a Chemical or Biological Attack," *Air and Space Power Journal*, Spring 2003. The US policy implies retaliation with nuclear weapons; however, it is vague enough to allow for a wide range of options.
[91] George M. Robinson, "Deterrence and the National Security Strategy of 2002: A Round Peg for a Round Hole," Naval Postgraduate School thesis, December 2003, 82.
[92] O'Neil, "Cyberspace and Infrastructure," 127.
[93] Gloystein, "Cyberdeterrence in 2035," 20.
[94] Allen, *Information Operations Planning*, 32.
[95] Libicki, *Cyberdeterrence and Cyberwar*, 73.
[96] Gray, *Maintaining Effective Deterrence*, 29.
[97] Libicki, *Cyberdeterrence and Cyberwar*, 28-29.
[98] Langevin et al, *Securing Cyberspace for the 44th Presidency*, Report of the CSIS Commission on Cybersecurity for the 44th Presidency (Washington, DC: Center for Strategic and International Studies, December 2008), 24.
[99] Libicki, *Cyberdeterrence and Cyberwar*, 110.
[100] de Czege, "Warfare by Internet," 90.
[101] Freedman, *Deterrence*, 36.
[102] Libicki, *Cyberdeterrence and Cyberwar*, 61.
[103] Ibid, 44.
[104] Langevin et al., *Securing Cyberspace for the 44th Presidency*, 25-26.
[105] Kugler, "Deterrence of Cyber Attacks," 327.
[106] Ibid, 65-67.
[107] Gary LaFree, Laura Dugan, and Raven Korte. "The Impact of British Counter Terrorist Strategies on Political Violence in Northern Ireland: Comparing Deterrence and Backlash Models," *Criminology* 47, no 1 (February 2009): 11.
[108] Gray, *Maintaining Effective Deterrence*, 9.
[109] Freedman, *Deterrence*, 117.
[110] Ibid, 47.
[111] Langevin et al., *Securing Cyberspace for the 44th Presidency*, 25.
[112] Starr, "Toward a Preliminary Theory of Cyberspace," 67.
[113] Thomas C. Wingfield, "International Law and Information Operations", in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 526.
[114] Allen, *Information Operations Planning*, 250.
[115] The White House, *National Security Strategy*, May 2010, 27-28.
[116] Ibid, 28. (Emphasis added).
[117] The White House, *The National Strategy to Secure Cyberspace*, February 2003, 50.
[118] Department of Homeland Security, *National Cyber Incident Response Plan*, interim version (Washington, DC: Department of Homeland Security, September 2010), M-1.
[119] Ibid, 10.
[120] Alan Paller, "President has had 'Kill Switch' for Communications since 1934," *Government Computer News*, 28 June 2010.
[121] *Protecting Cyberspace as a National Asset Act of* 2010, S 3480, 111th Cong., 2010.
[122] Gen James E. Cartwright to Chiefs of the Military Services, Commanders of the Combatant Commands, and Directors of the Joint Staff Directorates, memorandum, n.d.
[123] AFDD 3-12, *Cyberspace Operations*, 15 July 2010, 45
[124] Langevin et al., *Securing Cyberspace for the 44th Presidency*, 24-26.
[125] Ibid, 26.
[126] Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (U) (Washington, DC: Chairman of the Joint Chiefs of Staff, December 2006) (Secret) Information extracted in unclassified, F-1.

[127] AFDD 3-12, *Cyberspace Operations*, 15 July 2010, 45
[128] Ibid, 4.
[129] Libicki, *Cyberdeterrence and Cyberwar*, 64-65.
[130] Anjelka Kelic, Drake E. Warren, and Lawrence R. Phillips, "Cyber and Physical Interdependencies," Sandia Report SAND2008-6192 (Albuquerque, NM: Sandia National Laboratories, September, 2008), 10.
[131] Presidential Decision Document/NSC-63. Critical Infrastructure Protection, 22 May 1998. (For Official Use Only)
[132] Langevin et al, *Securing Cyberspace for the 44th Presidency*, 31
[133] Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 15.
[134] Beeker, "Strategic Deterrence in Cyberspace," 83-84.
[135] Freedman, *Deterrence*, 4-5.
[136] Ibid, 4.
[137] Kugler, "Deterrence of Cyber Attacks," 310.
[138] de Czege, "Warfare by Internet," 93-94.
[139] Langevin et al., *Securing Cyberspace for the 44th Presidency*, 26.
[140] Rattray, "An Environmental Approach," 269.
[141] O'Neil, "Cyberspace and Infrastructure," 145.
[142] Beeker, "Strategic Deterrence in Cyberspace," 53.
[143] Langevin et al., *Security Cyberspace for the 44th Presidency*, 2.
[144] Gloystein, "Cyberdeterrence in 2035," 21.
[145] Wingfield, "International Law and Information Operations," 525.
[146] Beeker, "Strategic Deterrence in Cyberspace," 82.
[147] Kugler, "Deterrence of Cyber Attacks," 335.
[148] Kramer, "Cyberpower and National Security," 14.
[149] Department of Homeland Security, *Cyber Storm II Final Report* (Washington, DC: Office of Cybersecurity Communications, National Cyber Security Division, July 2009), 1-3.
[150] Ibid, 15-17.
[151] Beeker, "Strategic Deterrence in Cyberspace," 69-70.
[152] Ibid, 43.
[153] Ibid, 66-67.
[154] Ibid, 45.
[155] de Czege, "Warfare by Internet," 93.
[156] Skoudis, "Information Security Issues in Cyberspace," 189.
[157] Siobhan Gorman, "US Plans Cybershield for Utilities, Companies," *Wall Street Journal*, 8 July 2010. http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html
[158] Lance Whitney, "NSA Offers Explanation of Perfect Citizen," *CNET News*, 9 July 2010. http://news.cnet.com/8301-1009_3-20010155-83.html
[159] Allen, *Information Operations Planning*, 45.
[160] Kugler, "Deterrence of Cyber Attacks," 339-340.
[161] Kramer, "Cyberpower and National Security," 16.
[162] Beeker, "Strategic Deterrence in Cyberspace," 48.
[163] Admittedly the concept of a symmetrical response is much easier with a nation-state. The concept of retaliating against a cyber attack from a terrorist group is no less difficult than retaliating against a physical terrorist attack.

Glossary

AFDD – Air Force Doctrine Document
ATM – Automatic Teller Machine
CIA – Central Intelligence Agency
DOD – Department of Defense
DHS – Department of Homeland Security
DNS – Domain Name Service
IP – Internet Protocol
ISAC - Information Sharing and Analysis Center
ISP – Internet Service Provider
NATO – North Atlantic Treaty Organization
NSA – National Security Agency
PRC – People's Republic of China
PSYOPS – Psychological Operations
SCADA - Supervisory Control and Data Acquisition
TCP – Transmission Control Protocol
US – United States

Bibliography

Adkins, Bonnie N. "The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?" Air Command and Staff College research paper, April 2001.

Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, 15 July 2010.

Allen, Patrick. *Information Operations Planning*. Norwood, MA: Artech Housem 2007.

Anderson, Levon R. "Countering State-Sponsored Cyber Attacks: Who Should Lead?" US Army War College Research Paper, 30 March 2007.

BBC News. "Estonia Fines Man for 'Cyber War,'" 25 January 2008, http://news.bbc.co.uk/2/hi/technology/7208511.stm (accessed 4 April 2011).

Beeker, Kevin R. "Strategic Deterrence in Cyberspace: Practical Application." Air Force Institute of Technology Research Paper, June 2009.

Blank, Stephen. "Can Information Warfare be Deterred?" *Defense Analysis* 17, no. 2 (August 2001), 121-138.

Broad, William J., John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *The New York Times*, 15 January 2011. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&ref=general&src=me&pagewanted=all (accessed 27 March 2011).

Cartwright, Gen James E. Vice Chairman, Joint Chiefs of Staff. To Chiefs of the Military Services, Commanders of the Combatant Commands, and Directors of the Joint Staff Directorates. Memorandum, n.d.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1989.

Clagnaz, John J. "US Cyber Command Cyberspace Superiority in the 21st Century." Air Force Institute of Technology Research Paper, Air University, March 2010.

Cliff, Roger, John Fei, Jeff Hagan, Elizabeth Hague, Eric Heginbotham, and John Stillion. *Shaking the Heavens and Splitting the Earth: Chinese Air Force Employment Concepts in the 21st Century*. Santa Monica, CA: RAND Corporation, 2011.

Conley, Harry W. "Not with Impunity: Assessing US Policy for Retaliating to a Chemical or Biological Attack." *Air and Space Power Journal*, Spring 2003.

"Cyberwar." *Economist* 396, no. 8689 (3 July 2010), 11-12.

Davis, Richard G. *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*. Washington, DC: Air Force History and Museums Program, 2002.

de Czege, Huba Wass. "Warfare by Internet: The Logic of Strategic Deterrence, Defense and Attack." *Military Review*, July-August 2010.

(accessed 2 December 2010).

Department of Homeland Security. *Cyber Storm II Final Report*. Washington, DC: Office of Cybersecurity and Communications, National Cyber Security Division, July 2009.

Department of Homeland Security. *National Cyber Incident Response Plan*. Interim version. Washington DC: Department of Homeland Security, September, 2010.

Dumiak, Michael. "Casus Belli." *Defense Technology International* 4, no. 8 (1 September 2010).

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32.Stuxnet Dossier," version 1.4 (February 2011). Symantec Corporation. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (accessed 4 April 2011).

Freedman, Lawrence. *Deterrence*. Cambridge, UK: Polity Press, 2004.

Gloystein, John W. "Cyberdeterrence in 2035: Redefining the Framework for Success." Air War College research paper, 10 February 2010.

Gorman, Siobhan. "US Plans Cybershield for Utilities, Companies." *Wall Street Journal*, 8 July 2010. http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html (accessed 12 December 2010).

Government Accountability Office. *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*. GAO-04-354, March 2004.

Gray, Colin S. *Maintaining Effective Deterrence*. Carlisle Barracks, PA: Army War College Strategic Studies Institute, August 2003.

Helms, Susan J. "Schriever Wargame 2010: Thoughts on Deterrence in the Non-Kinetic Domain." *High Frontier* 7, no. l (November 2010): 12-15.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, 6 January 2011. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (accessed 25 Mar 2011).

Joint Chiefs of Staff. *National Military Strategy for Cyberspace Operations* (U), Washington, DC: Chairman of the Joint Chiefs of Staff, December 2006. (Secret) Information extracted in unclassified.

Kelic, Anjelka, Drake E. Warren, and Lawrence R. Phillips. "Cyber and Physical Interdependencies." Sandia Report SAND2008-6192. Albuquerque, NM: Sandia National Laboratories, September 2008.

Kramer, Franklin D. "Cyberpower and National Security: Policy Recommendations for a Strategic Framework." in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 3-23. Dulles, VA: Potomac Books, 2009.

Kugler, Richard L. "Deterrence of Cyber Attacks" in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 309-340. Dulles, VA: Potomac Books, 2009.

LaFree, Gary, Laura Dugan, and Raven Korte. "The Impact of British Counter Terrorist Strategies on Political Violence in Northern Ireland: Comparing Deterrence and Backlash Models." *Criminology* 47, no. 1 (February 2009), 17-45.

Lambeth, Benjamin S. *NATO's AirWar for Kosovo: A Strategic and Operational Assessment*. Santa Monica, CA: RAND Corporation, 2001.

Langevin, James R., Michael T. McCaul, Scott Charney, and Harry Raduege. *Securing Cyberspace for the 44th Presidency.* A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington, DC: Center for Strategic and International Studies, December 2008.

Lewis, James A. "Thresholds for Cyberwar." Center for Strategic and International Studies report. Washington D.C., September 2010. http://csis.org/files/publication/101001_ieee_insert.pdf (accessed 21 March 2011).

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.

Libicki, Martin, C. "Military Cyberpower." in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 275-284. Dulles, VA: Potomac Books, 2009.

McCarthy, John A., Chris Barrow, Moeve Dion, and Olivia Pacheco. "Cyberpower and Critical Infrastructure: A Critical Assessment of Federal Efforts." in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 543-556. Dulles, VA: Potomac Books, 2009.

Meserve, Jeanne. "Mouse Click Could Plunge a City into Darkness, Experts Say." *CNN.com*, 27 September 2007. http://articles.cnn.com/2007-09-27/us/power.at.risk_1_generator-experiment-cnn?_s=PM:US (accessed 21 March 2011).

O'Neil, William D. "Cyberspace and Infrastructure." in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 113-146. Dulles, VA: Potomac Books, 2009.

Paller, Alan. "President has had 'Kill Switch' for Communications since 1934." *Government Computer News*, 28 June 2010.

Pape, Robert A. *Bombing to Win: Air Power and Coercion in War*. Ithaca, NY: Cornell University Press, 1996.

Peterson, Phillip A. and Clark, John R. "Soviet Air and Antiair Operations."*Air University Review*, March-April 1985.

Presidential Decision Document/NSC-63. Critical Infrastructure Protection, 22 May 1998. (For Official Use Only)

Rattray, Gregory J. "An Environmental Approach to Cyberpower." in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 253-274. Dulles, VA: Potomac Books, 2009.

Rekasius, Mindaugus. "Unconventional Deterrence Strategy." Naval Postgraduate School thesis, June 2005.

Robinson, George M. "Deterrence and the National Security Strategy of 2002: A Round Peg for a Round Hole." Naval Postgraduate School thesis, December 2003.

Rothschild, Jeff. “High Performance at Massive Scale – Lessons Learned at Facebook.” Address. University of California, San Diego, 8 October 2009.

Skoudis, Edward. “Information Security Issues in Cyberspace.” in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 171-205. Dulles, VA: Potomac Books, 2009.

Starr, Stuart H. “Toward a Preliminary Theory of Cyberpower.” in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 43-85. Dulles, VA: Potomac Books, 2009.

The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, n.d.

The White House, *National Security Strategy*, May 2010.

The White House. *The National Strategy to Secure Cyberspace*. February 2003.

Trimble, Lindsay. “Senior Leader Perspective: Scott Borg.” National Security Cyberspace Initiative newsletter. Smithfield, VA, June 2010. http://nsci-va.org/SeniorLeaderPerspectives/2010-06-17-CyberPro_interview_Scott_Borg.pdf (accessed 22 March 2011).

United States Chemical Weapons Convention. “About the CWC,” United States Department of State, Bureau of International Security and Nonproliferation and United States Department of Commerce, Bureau of Industry and Security, http://www.cwc.gov/cwc_about.html (accessed 5 April 2011).

US Senate. *Protecting Cyberspace as a National Asset Act of* 2010, 111th Cong., S 3480, 2010.

Whitney, Lance. “NSA Offers Explanation of Perfect Citizen.” *CNET News*, 9 July 2010. http://news.cnet.com/8301-1009_3-20010155-83.html (accessed 12 December 2010).

Wilson, Clay. “Cyber Crime” in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 415-436. Dulles, VA: Potomac Books, 2009.

Wingfield, Thomas C. “International Law and Information Operations.” in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 525-542. Dulles, VA: Potomac Books, 2009.