American Cyber Insecurity:

The growing danger of cyber attacks

Chris Brown, Desmond Lee, Colin Scott, Daniel Strunk

"There is no penalty to attacking us now. We have to figure out how to change that."

Retired General James Cartwright, Former Vice-Chairman of the Joint Chiefs of Staff[1]

"Which cyber-exploitation activities (if any) might the United States be willing to give up in exchange for reciprocal constraint from the Chinese and others? And how, exactly, can international cybersecurity norms develop and operate in the largely-anonymous digital world, where attribution of cyber-espionage is slow, uncertain, sometimes impossible, and always very difficult to prove in the public realm? I have not seen any serious public discussion of these questions by U.S. officials."

Jack Goldsmith, Harvard Law School Professor[2]

Introduction and Statement of Problem

The following paper is a response to this problem so astutely captured by Jack Goldsmith. The United States has a vast superiority in the cyber realm. The benefit this accrues the United States, in terms of the military, economic, and intelligence gathering arenas, is enormous. But the United States is anywhere from invulnerable in the cyber landscape. At the heart of America's cyber security vulnerability are two key factors: 1.) a lack of transparency in how states use and view cyberspace and 2.) a lack of established norms to guide state action in cyberspace. A successful U.S. Grand Strategy in the cyber realm thus needs to address these two issues specifically, increasing clarity and understandings between nations and thus decreasing the likelihood of misinterpretation and escalation into conventional conflict.

To clarify, we address the specific area of *cyber attacks* as opposed to *cyber espionage* or *cyber crime*. In scholarly work on cyber-security there remains a tendency to conflate these distinct threats.[3] This tendency is problematic because it obscures

[1] Stevens, T. (2012). A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. Contemporary Security Policy, 33(1), 155.
[2] Jack Goldsmith, "What is the government's strategy for the cyber-exploitation threat," Lawfare Blog, August 10, 2011. www.lawfareblog.com/2011/08/what-is-the-government's-strategy-for-the-cyber-exploitation-threat/
[3] Benjamin Wittes, "Book Review: America the Vulnerable," *Lawfare Blog*, December 28, 2011, http://www.lawfareblog.com/2011/12/america-the-vulnerable-inside-the-new-threat-matrix-of-digital-espionage-crime-and-warfare/#.Up4w2ZrUgVY.twitter

significant differences between these problems that may call for dramatically disparate policy responses. While both cyber espionage and cyber crime are certainly areas of concern for the United States, cyber attacks, since they involve network disruption and danger to critical infrastructure and financial markets, pose the most pressing threat. The United States has more to gain than lose from the current murkiness in norms surrounding cyber espionage. Furthermore, espionage is not something that can feasibly be solved through diplomacy. The situation is reversed for cyber-attacks. Espionage is a fact of life; cyber attacks need not be. As the most connected and network dependent great power in the world, we have the most to lose. There is no reason to believe that this risk will decrease. The status quo will likely worsen—the gamble inherent in the present situation is untenable.

Scholars who consider the cyber issue a red herring, not worth the attention it receives from universities and the military, discount the importance of recent developments in the cyber sphere. States are currently gearing up for future conflicts in the cyber arena. China, India, Russia, the United Kingdom, and South Korea have all joined the United States in establishing formal military cyber command and control policies.[4] The FBI has estimated that 108 countries have dedicated cyber attack capabilities.[5] There are a projected 30,000 "cyber-cops" in China who possess "the training and expertise that would allow them to conduct cyber penetrations," with the UDS joint strike fighter project and the USAF air traffic control systems reported as their potential targets.[6] James Lewis notes evidence that major cyber powers have carried out

---

[4] Hughes, Rex. "A treaty for cyberspace." *International Affairs*. no. 2 (2010): 523-541.
[5] Germain, Jack. "The Art of Cyber Warfare, Part 1: The Digital Battlefield." *TechNewsWorld*, April 29, 2008. http://www.technewsworld.com/rsstory/62779.html?wlc=1263772777 (accessed December 5, 2013).
[6] Hughes, Rex. "A treaty for cyberspace." *International Affairs*. no. 2 (2010): 523-541.

network reconnaissance of potential U.S. critical infrastructure targets in preparation for possible attacks.[7]

But not only are states gearing up for future conflicts, numerous cyber attacks have already taken place. Since the start of the new millennium, these state-sponsored attacks have varied in targets from government websites to critical infrastructure. In 2001 as part of a response to a maritime dispute in the South China Sea, China levied a cyber attack on a California electricity plant bringing it close to shutdown.[8] Attacks on Estonian networks in 2007 and Georgia's state systems in 2008 have demonstrated Russia's capabilities in levying its cyber power in a military capacity.[9] More alarming than any of these incidents, the CIA reported that in 2007 several cyber-attacks on public electricity networks were carried out in regions inside and outside the United States. This led Retired US Admiral Mike McConnell, who previously served as the head of the CIA, the DIA, and the NSA, to warn in late 2009 that he saw adversaries of the United States as capable of disabling major segments of the U.S. power grid.[10] The Obama Administration added to these fears when it warned that a cyber attack could undermine systems that provide water, power, or other critical services to Americans.[11]

As cyber attacks increase in number, scope, and sophistication, the use of cyber networks is anything but decreasing. On the contrary, such networks are becoming exponentially more tied to civilian and military infrastructure, in both the United States and beyond. As this cyber activity continues to boom, the likelihood that a

---

[7] Lewis, James. "Multilateral Agreements to Constrain Cyberconflict." *Arms Control Today*. no. 5 (2010): 14-19.
[8] Geers, Kenneth. "Cyberspace and the changing nature of warfare." *SC Magazine*, August 27, 2008. http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/ (accessed December 5, 2013).
[9] Markoff, John, and Andrew Kramer. "U.S. and Russia Differ on a Treaty for Cyberspace." *The New York Times*, , sec. World, June 27, 2009. http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=1 (accessed December 5, 2013).
[10] Hughes, Rex. "A treaty for cyberspace." *International Affairs*. no. 2 (2010): 523-541.
[11] Nakashima, Ellen, and . "In U.S.-Russia deal, nuclear communication system may be used for cybersecurity." *Washington Post*, April 26, 2012. http://articles.washingtonpost.com/2012-04-26/world/35453448_1_cyberspace-cybersecurity-russia-and-china (accessed December 5, 2013).

misunderstanding between nations grows ever more precarious. A misinterpretation could easily lead to escalation, spilling out into unintended consequences involving conventional forces. General Kevin Chilton of the U.S. Strategic Command, when delivering a speech at the 2009 Cyberspace Symposium, voiced the beliefs of many military experts when he warned that a cyber-attack on an advanced information economy could lead to a substantial conventional or even nuclear response.[12] The peril is doubled when one considers that the initial steps of a cyber attack are nearly identical to the initial steps of cyber espionage, and that most state cyber actions are done in secret.[13]

In Part I we provide a brief overview of the history of the cyber arena. In Part II, we provide policy recommendations and delineate specific actions the United States can undertake to advance norms and TCBMs in the cyber arena.

[12] Hodge, Nathan. WIRED, "General: We Just Might Nuke Those Cyber Attackers." Last modified May 13, 2009. Accessed December 6, 2013. http://www.wired.com/dangerroom/2009/05/general-we-just-might-nuke-those-cyber-attackers/.
[13] Lewis, James. "Multilateral Agreements to Constrain Cyberconflict." *Arms Control Today*. no. 5 (2010): 14-19.

Figure 1.1

Clarifying our Terminology:

There is no universally accepted definition of many of the terms utilized by scholars and policymakers to describe certain activities in the cyber sphere. For this reason, we will clarify the terminology that we use in this paper and the reasoning behind its use.

Cyber War:
The definition of the term *cyber war* is highly controversial. Cyber scholar Thomas Rid insists that any act of *cyber war* must be violent, instrumental, and political, and that no cyber event in history has had all three of those traits. Jason Healey maintains that *cyber war* consists of any operations that cross a threshold into armed attack. Many prominent figures in the United States defense community insist that we are already engaged in *cyber war*. Given the highly contested definition of the term *cyber war*, we have elected to forego its use in our policy recommendation.

Cyber Attack:
We define *cyber attacks* as the malicious use of offensive cyber capabilities to undermine, manipulate, or destroy critical civilian and military networks and infrastructure.*

Cyber Espionage:
We define cyber espionage as an attempt to penetrate the networks of an adversary in order to extract sensitive or protected information.

Cyber Crime:
We define cyber crime as an offensive cyber operation that is conducted for material and criminal, rather than political, gains.

For the purpose of this paper, we focus on *cyber attacks*. In our view, *cyber attacks* form the first-rate threat to U.S. interests emanating from the cyber sphere. For this reason our policy recommendation does not focus on lower tier threats in the cyber field. These second-rate threats include cyber espionage and cyber crime. Cyber espionage, which involves the attempt to penetrate adversarial networks in order to extract sensitive information, is certainly an important issue in its own right. In our judgment, however, focusing on the threat posed by cyber attacks is the most realistic and viable way forward.

*This definition of cyber attack is similar to what Thomas Rid calls *cyber sabotage*.

Part I—The History of Cyber Conflict: Cases, Trends, and Lessons

Contrary to popular belief, the cyber sphere has a rich history spanning several decades[14]. From its earliest beginnings, nations and non-state actors have disrupted the cyber sphere, using cyber capabilities to attack, defend, or spy on each other. Mining the key lessons from this unappreciated history of cyber conflict is essential to crafting an effective and forward-looking American cyber strategy. As a result, this section addresses the history of cyber conflict. First, we flag a handful of key events in the history of cyber conflict, explain the U.S. response to these events, and trace the impact of these events on U.S. cyber strategy. Second, we will examine the evolution of the cyber threat environment, paying special attention to the last decade. Third, we address the alternative interpretation of the lessons of cyber history put forth by cyber skeptics. Last, we present our assessment of the meaning of events, trends, and strategic responses over the course of cyber history and enumerate key lessons for today's policymakers.

While our policy recommendation is specifically designed to address the threat posed by *cyber attacks* (as defined in Fig. 1.1), we have elected to examine cyber history through a broader lens. Our decision to take this approach was largely influenced by the work of Jason Healey of the Cyber Statecraft Initiative. In his comprehensive history of cyber conflict, Healey identifies a handful of key events that served as wake-up calls to U.S. cyber strategists. These wake-up calls included instances of both *cyber attacks* and *cyber espionage*. In our assessment, taking a holistic approach that addresses wake-up calls of both varieties ensures a more insightful evaluation of the lessons to be drawn from cyber history. To diminish the importance of key wake-up calls caused by *cyber*

[14] Jason Healey, "The Lessons of Cyber Conflict History, So Far…" last modified May 30, 2013. http://www.intgovforum.org/cms/wks2013/workshop_background_paper/199_1367614021.pdf

espionage would render our analysis of cyber history incomplete. The primary advantage of this more inclusive approach is that it clearly highlights a troubling historical trend in U.S. cyber strategy that is extremely pertinent to today's policymakers. The historical record reveals a consistent failure of U.S. policymakers to produce proactive cyber strategies. Instead, the jarring events referred to by Healey have prompted reactive policy shifts in the cyber sphere. Of these events, Healey writes, "Each shocked and surprised the defenders and decision makers that suffered through them, but their lessons were soon forgotten, until a new wave of cyber leaders were again 'awakened' to a similar shock."[15] As a result, the process of crafting and refining U.S. cyber strategy in the last two decades has been largely cyclical and backward looking. U.S. cyber strategy has historically sought to prevent a repeat of the most recent cyber event. Time and again, U.S. policymakers have been lulled into a false sense of security after addressing yesterday's cyber threats. They then spring into action again only after being hit with a new wake-up call, typically of a greater magnitude. The case studies outlined in the following section highlight this pattern.

Cyber History: Key Events and U.S. Strategic Response

This section will highlight a handful of key events in the history of cyber conflict and the responses to them by American cyber strategists. Throughout the 1970s and 1980s, U.S. strategists began to voice concern over the national security implications of the United States' increasing reliance on interconnected computer networks. By 1993, cyber alarmists like John Arquilla and David Ronfeldt of the RAND Corporation were

[15] Jason Healey, "The Lessons of Cyber Conflict History, So Far…" last modified May 30, 2013. http://www.intgovforum.org/cms/wks2013/workshop_background_paper/199_1367614021.pdf

declaring, "Cyber War is Coming!"[16] Despite the warnings of cyber alarmists, cyber security was largely regarded as a marginal issue until a series of wake-up calls forced U.S. policymakers into action.

1. *Morris Worm*

In 1988, college student Robert Tappan Morris created a worm designed to do two things: infect as many computers as possible and prove difficult to stop.[17] Though conceived as a simple prank, the Morris Worm caused nearly 10% of the Internet to crash and provided the first major wake-up call in cyber history. The Morris Worm highlighted the total lack of U.S. defensive capabilities and prompted the first policy reaction to the cyber threat, the establishment of a Cyber Emergency Response Team (CERT) at Carnegie Mellon University.

2. *ELIGIBLE RECEIVER and SOLAR SUNRISE*

Nearly a decade passed before the 1997 ELIGIBLE RECEIVER (ER97) exercise and the 1998 SOLAR SUNRISE incident again shook U.S. confidence in its cyber security and sparked a reaction by policymakers. In the ER97 exercise, an NSA "red-team" brought in by the DoD easily infiltrated highly sensitive networks, including the computer network at the U.S. Pacific Command center, while avoiding detection for three days. The exercise highlighted the lack of a centralized body in charge of recognition, assessment, attribution, and reaction (RAAR) to cyber intrusions. The 1998 SOLAR SUNRISE attacks, launched by a group of California teenagers, compromised unclassified DoD systems and "demonstrated real world problems predicted in ER 97."[18] While the amateurish SOLAR SUNRISE hackers inflicted little damage, their attack

[16] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Studies* 12.2 (1993): 23
[17] Jason Healey, *A Fierce Domain: Conflict in Cyberspace 1986 to 2012* (Washington: Cyber Conflict Studies Association) Kindle Locations 693-702
[18] Ibid., Kindle Location 1011.

exposed a major cyber vulnerability. In response to the ER97 exercise and the SOLAR SUNRISE incident, the DoD established the Joint Task Force- Computer Network Defense (JTF-CND) in March 1998. The strategic rationale behind the establishment of the JTF-CND was that it would place responsibility for RAAR of cyber intrusions under one roof and thus streamline future U.S. responses to cyber intrusions.

3. *MOONLIGHT MAZE*

The MOONLIGHT MAZE incident provided the next major shock to American cyber strategists. In 2000, U.S. officials discovered, by accident, that a group of technically advanced hackers had infiltrated computer networks and compromised tens of thousands of files of classified information at the Pentagon, NASA, and the Department of Energy over a two year period. It took more than three years for the JTF-CND to eliminate the last of the backdoors installed into confidential networks. The attacks were ultimately traced to a number of Internet cafés in Russia, prompting speculation that the operation was a state-sponsored espionage effort. The MOONLIGHT MAZE incident again provided clear evidence that U.S. cyber defense was inadequate in the face of a growing threat and prompted another round of organizational realignment with the objective of bolstering defensive capabilities.

5. BUCKSHOT YANKEE

In 2008, a USB stick infected with a technically advanced worm was inserted into a laptop on a U.S. military base in the Middle East. The worm jumped the "air gap" between classified and unclassified networks of the Department of Defense, establishing a virtual beachhead and compromising troves of confidential information. Former Deputy Secretary of Defense William Lynn called this incident "the most significant breach of

US military computers ever."[19] While U.S. officials did not publicly attribute the attack to a particular country, a 2011 Reuters report claimed, "Experts inside and outside of the US government strongly suspect that the original attack was crafted by Russian intelligence."[20] The US response to the attack, codenamed BUCKSHOT YANKEE, spent over a year cleaning the worm from military networks. As the most damaging wake-up call to date, this incident prompted a major policy shift. In its immediate aftermath, policymakers began to consider merging NSA and military cyber defense operations and creating a US Cyber Command to shore up American cyber defense. In June 2009, the Secretary of Defense directed the US Strategic Command to establish a sub-unified Cyber Command in order to shore up defensive capabilities and protect against another similar incident.

Cyber History: The Evolution of the Cyber Threat Environment

As the cyber threat environment has evolved in recent years, certain elements have remained relatively constant. Of these elements, three stand out in particular. First, precise attribution of cyber attacks has proven to be extremely challenging throughout the course of cyber history. Despite major technological advances in the last two decades, attribution difficulties have persisted. In our assessment, this constant feature of the cyber sphere has shaped the threat environment; it emboldens attackers, who are unlikely to face retribution. Second, the fundamentally asymmetric nature of cyber conflict has remained essentially static. Technically sophisticated actors in the cyber sphere can conduct damaging attacks at a relatively low cost. Speaking to this asymmetry, former Deputy Secretary of Defense William J. Lynn writes, "A dozen determined programmers

[19] Jason Healey, *A Fierce Domain: Conflict in Cyberspace 1986 to 2012* (Washington: Cyber Conflict Studies Association) Kindle Location 4851.
[20] Ibid., Kindle Location 4867.

can, if they find a vulnerability to exploit, threaten the United States global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target."[21] The final constant feature of the threat environment is the imbalance between cyber offense and cyber defense. The history of cyber conflict has clearly demonstrated that cyber attackers have possessed, and will continue to possess, a distinct advantage over defenders. In the cyber sphere, defenders are tasked with protecting every corner of vast networks, while attackers must simply find a minute vulnerability to exploit. The offense-defense imbalance in the cyber sphere has grown increasingly important given the evolution of the cyber threat environment in recent years.

In the early years of cyber history, relatively few actors with relatively modest capabilities were engaged in cyber conflict. The last two decades, however, have seen dramatic increases in the number of nations and non-state actors engaged in cyber conflict, the sophistication of cyber attacks, and the frequency of cyber incidents. This trend has accelerated in recent years. Even cyber skeptics like Thomas Rid of King's College London concede this point. Rid writes, "The empirical trend is obvious: over the past dozen years, cyber attacks have been steadily on the rise. The frequency of major security breaches against government and corporate targets has been going up. The volume of attacks is increasing. So is the participation in attacks…the range of aggressive behavior online is widening."[22]

In our assessment, these developments have changed the cyber threat environment in meaningful ways. The last decade has seen a diffusion of potentially dangerous cyber capabilities to a host of new actors with unknown intentions. Furthermore, the

[21] William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89.5 (2010): 2.
[22] Thomas Rid, "Cyber War Will Note Take Place," *Journal of Strategic Studies* 35.1 (2012): 15.

sophistication of cyber capabilities, especially those possessed by major strategic actors, has increased dramatically as national militaries and intelligence agencies have become more involved in the cyber sphere. The most significant example of this trend is emergence of the STUXNET worm, the most sophisticated piece of malicious software ever created, in 2010. While many attribute the origin of Stuxnet to the United States, and it thus potentially serves as a demonstration of American superiority in launching cyber attacks, the fact remains that it has since been reverse engineered by numerous countries. Thus, the United States could now feasibly fall victim to this devastating technology. Finally, the sheer quantity of cyber attacks and intrusions has increased exponentially in the last decade.

In assessing the evolution of the cyber threat environment, it is crucial to note that changes in offensive capabilities do not occur in a vacuum. The past decade has also brought advancements to defensive cyber capabilities in the United States. In particular, the establishment of the United States Cyber Command in 2009 integrated disparate defensive capabilities under one organization and dramatically enhanced U.S. cyber defense. The fact remains, however, that despite the increase in defensive capabilities, cyber attackers have retained a distinct advantage over cyber defenders to this day.

Cyber Skepticism: An Alternative Interpretation of Cyber History's Lessons

Some cyber scholars have analyzed developments in the cyber sphere in the last three decades and concluded that the cyber threat is largely overhyped. Among the most prominent of these cyber skeptics is Thomas Rid, the author of *Cyber War Will Not Take Place*. In Rid's assessment, cyber war has not taken place at any point in history and is

unlikely to take place in the future. Rid borrows from Carl von Clausewitz and establishes three criterion that would have to be satisfied for a cyber event to be considered an act of war. In order to constitute an act of cyber war, an event would have to 1) be lethal or potentially lethal, 2) serve as a means to end, and 3) be driven by a political objective. According to Rid, no event in the history of cyber conflict has fulfilled all three of the criteria to constitute an act of war.

Instead, Rid argues that offensive cyber operations break down into three categories that have long been fixtures in the sphere of international politics: subversion, espionage, and sabotage. According to Rid, sabotage is an attempt to weaken or destroy an economic or military system, espionage is an attempt to penetrate an adversarial system in order to extract sensitive information, and subversion is the attempt to undermine the authority or integrity of an established authority or order.[23]

Examining the history of cyber conflict through this framework, Rid concludes that the cyber threat is overinflated. He notes that there has never been a deadly use of a cyber weapon and that, despite decades of warnings by cyber alarmists, there has never been a truly catastrophic cyber attack. Furthermore, in Rid's view, developments in the cyber threat environment in recent years have actually decreased the likelihood of a devastating cyber attack against the United States. He asserts that the sophistication needed to conduct a major cyber attack is increasing and that only a handful of strategic actors would be capable of launching such a strike against the United States.[24] In Rid's view, offensive cyber activity originating from actors outside of this top-tier group is essentially just noise.

[23] Thomas Rid, "Cyber War Will Note Take Place," *Journal of Strategic Studies* 35.1 (2012): 22.
[24] Ibid., 28.

In our view, Rid's assessment of cyber history and diagnosis of the threat today is misguided. First, Rid's assertion that a catastrophic cyber attack will not happen because it has not happened is a logical fallacy. Neither Rid nor any other cyber skeptic can make this claim with total confidence. Second, Rid's application of Clausewitz's principles to the cyber sphere misses the point. We concede that no event in cyber history fulfills Rid's three criteria, that cyber attacks have yet to claim a human life, and that a cyber Pearl Harbor resulting in significant violence and casualties is very unlikely. But to declare the cyber threat overinflated for its failure to adhere to this narrow definition of warfare is imprudent. The cyber threat is about more than mass casualties or physical damage: a major cyber attack could do unacceptable damage to U.S. national interests without causing a single casualty. On this point, Rid concedes, "In highly networked societies, non-violent cyber attacks could cause economic consequences without violent effects that could exceed the harm of an otherwise smaller physical attack."[25] In this case, Rid is categorically correct. Given the development of the cyber threat environment in recent years, the primary concern of policymakers should not be preventing an instance of *cyber war* as defined by Rid. Instead, it should focus on preventing attacks that strike a blow to the foundation of American power; its financial markets, its energy infrastructure, its communications systems, and its military infrastructure. Attacks of this nature would not only directly cause damage, but would also increase the likelihood of escalation into a full-scale exchange of cyber attacks between nations. By dismissing the threat to these critical elements of American power as overhyped, Rid misreads the history of cyber conflict and the development the cyber threat environment in the last decade.

[25] Thomas Rid, "Cyber War Will Note Take Place," *Journal of Strategic Studies* 35.1 (2012): 9.

The Lessons of Cyber History

Based on our assessment of the history of cyber conflict, we have identified three key lessons that must be considered in the formulation of an American cyber strategy for the future.

1) Cyber attacks have been, and will remain, difficult to predict. Given the difficulty of predicting cyber attacks, it is critical to reduce the incentives of launching cyber attacks, especially for the most capable strategic actors in the cyber sphere. Thus an effective cyber strategy would impose additional costs to launching a cyber attack.

2) Over the course of cyber history, the magnitude of damage caused by wake-up calls has consistently increased. Weighing the relatively modest damage caused by the 1998 Solar Sunrise incident against the massive harm inflicted in the BUCKSHOT YANKEE incident a decade later clearly demonstrates this point. For this reason, it is crucial to consider the potential magnitude of damage that could be caused by the next wake-up call. This highlights the necessity of preemptively addressing cyber threats.

3) The most powerful actors in the cyber sphere have not launched full-scale, unrestrained cyber attacks on one another to this date. This lesson, the most promising to be drawn from cyber history, must be considered in the formulation of American cyber strategy. This is, however, not a reason to rest on our laurels; maintaining this delicate balance and insuring the explicit codification of this set of tacit practices will require proactive action.

The strategy proposed in the Part III of this paper pays due attention to the lessons of cyber history outlined above. In doing so, it proposes an alternative to the cyclical pattern of reactive policy shifts in the cyber sphere that has played out over in the last two decades. Instead of putting forth another ad hoc solution to a perceived change in today's threat environment, it charts a new way forward for the United States in the cyber realm.

Part II—Charting the Course of Policy

The cyber domain poses areas of immense opportunity and challenge for the United States. Yet, despite the immense level of vulnerability present in the cyber realm there is scant international consensus on what constitutes a cyber-attack or how states should operate within cyber space.[26] This lack of foundational understanding undermines security and invites instability. Differing conceptions of acceptable state action have resulted in vastly different levels of support for cyber intrusions across the globe. Coupled with the lack of a common language when discussing cyber issues, is an absence of state explanation for expected responses to cyber-attacks.

This ambiguity is dangerous and could lead to unexpected escalation. Despite skeptics claims to the contrary, there has been a marked increase in attacks directed at American networks[27]. War in the foreseeable future will certainly not be relegated solely to the interaction between computers but the action that occurs in cyberspace can have a profound impact on physical space. As one of the largest players in the wired world it is in the United States' interests to begin the discussion on acceptable state behavior in cyber space in order to protect itself and reduce the ambiguity that could lead to conflict.

[26] Scott W. Beidleman. 2009. Defining and Deterring Cyber War, *Military Technology* 35(11): 9.
[27] Hughes, Rex. "A treaty for cyberspace." *International Affairs*. no. 2 (2010): 523-541.

This section of our report, after examining current policy, offers a potential course of action to alleviate some of the most pressing concerns facing American interests in cyberspace.

Current Policy

The Obama administration has released a number of documents that detail current American policy in cyberspace. Cyber security has increasingly come to the forefront of domestic and international news with the revelations of Stuxnet and the Edward Snowden leaks. Official policy has recently focused on increasing the strength of domestic infrastructure against potential intrusions. International efforts to govern cyberspace have not moved far past the 2001 Budapest Convention on Cybercrime despite growing calls for more substantive intervention.

The 2009 Cyberspace Review by the Obama administration indicated that "the status quo is no longer acceptable" and that "the United States must signal to the world that it is serious about addressing this challenge with strong leadership and vision."[28] The 2009 Review recommended a top down approach directed from the White House aimed at clarifying "roles, and responsibilities for cyber security-related activities across the Federal government." [29] Additionally the Cyberspace Review recognized the importance of developing international norms in governing cyberspace and advised the United States to "develop a strategy designed to shape the international environment and bring like-minded nations together on a host of issues."[30] In tandem with developing international

[28] White House, *Cyberspace Policy Review*. 2009. iii.
[29] Ibid 10
[30] Ibid 30

norms, the Review recognized the importance of fostering partnerships with private enterprise in order to decrease American vulnerability[31].

As directed by the Cyberspace Policy Review, the White House ordered a 60 day review to evaluate U.S policies and structures for cybersecurity. This review culminated in a number of recommendations and measures aimed at addressing American vulnerabilities in cyberspace. Chief among these goals was the appointment of a "cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities."[32] Along with this recommendation, the 2009 review developed a near term action plan that addressed nearly every facet of the developing cyber problem. Included in this plan was a measure to promote cyber security awareness nationally and develop an incident response plan through which private entities could report malicious cyber activity. These were promising short term goals that were rearticulated in the 2011 White House International Strategy for Cyberspace.

An international focus reemerged in the 2011 International Strategy for Cyberspace, which stated that the America would "establish an environment of expectations, or norms of behavior, that ground foreign and defense policies and guide international partnerships" in cyberspace[33]. Despite these declaratory statements there has been precious little progress in the realm of international politics surrounding the legality of cyber-attacks. Much has been said about the necessity of fostering international norms of behavior in-between states, however little has been accomplished.

This can partly be explained by the lack of substantive events occurring in the cyber domain. It has been hard to develop rules of the road when relatively few large

[31] Ibid 29
[32] Ibid vi.
[33] White House, *International Strategy For Cyberspace*. 2011. 9.

scale cyber-attacks have occurred in the platform's history. There have also been issues of difference between the United States and other international actors that have forestalled the development of rules guiding state action in cyberspace. Russia and China conceive of cyber security issues in a different manner than the United States, which was highlighted in the Shanghai Cooperation Organization's 2008 declaration decrying the "dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural sphere of other states."[34]

These emerging powers decry the intrusion of American ideas, through social media platforms such as Facebook and Twitter, into their cyberspace. This has made the pursuit of international agreements difficult as there is seemingly little common ground from which to negotiate. Recent trends ,however, suggest that there may be a space opening for discussion of cyber-attacks as witnessed by the recent agreements between the United States and Russia to share information regarding cyber-threats over the Cold War Era Threat Assessment Hotline[35, 36, 37]. If such an agreement can be secured with Russia, a chronic cyber security instigator, than it may be possible to reach a larger scale agreement with other partners.

Current think tank analysis, notably the Council on Foreign Relations Report, and academic literature on the subject argue for the necessity of developing international norms regarding cyber power. Yet the 2001 Budapest Convention on Cyber Crime marks the last international agreement, with widespread support, that deals with this new domain. The Budapest Convention, however, was not tasked with determining what

[34] Jason Healey. 2011. The spectrum of national responsibility for cyberattacks. *The Brown Journal of World Affairs* 18 (1): 57.
[35] Ellen Nakashima, "In U.S-Russia Deal, nuclear communication system may be used for cybersecurity
[36] http://fcw.com/Articles/2013/06/19/russia-cybersecurity-cooperation.aspx?Page=2
[37] Stevens, T. (2012). A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. Contemporary Security Policy, 33(1), 163.

constitutes acceptable state behavior in cyberspace. Rather it delineated a common set of cyber crimes, unrelated to cyber attacks, for countries to adjudicate.

The most recent administrative effort to secure the net was the attempted passage of the Cybersecurity Act of 2012, which failed to garner the 60 votes necessary to advance the bill past cloture[38]. The bill attempted to augment the security standards of crucial infrastructure sites across the United States, following a massive cyber-attack simulation directed by the White House in June of 2012[39]. There is no further cyber security legislation on the horizon for this Congress.

Current policy poses numerous problems for American interests despite official efforts to foster international engagement; norms surrounding the use of cyber-power can and must be developed further.

Problems with the status quo

The current strategic situation in cyberspace poses numerous problems for the United States.

1) First, a lack of agreement over acceptable behavior in cyberspace allows third party actors, often with the tacit consent of their governments, to attack American servers and companies with little fear of retaliation. Current strategists focus on the precise attribution of cyber-attacks but are frequently unable to pinpoint their origin. Such a focus often paralyzes investigative efforts, as unfriendly countries are able to blame these incidents on third party actors.[40] This has created an environment in which nations are able to claim deniability about the offensive events directed at the United States that are clearly occurring within their

[38] http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/
[39] Barack Obama, "Taking the Cyberattack Threat Seriously," *Wall Street Journal*, 20 July, 2012
[40] *Untangling Attribution: Moving Accountability in Cyberspace*, United States House, 111th Cong. 15(2010) (statement of Robert K. Knake International Affairs Fellow in Residence The Council on Foreign Relations)

borders.[41] These attacks pose an apparent security risk for the United States but currently fall below the threshold that would initiate a state response. There is already ample evidence that China's People Army has "focused hostile efforts against non-secure U.S. transmissions."[42] Yet there is no clear guidelines for how the United States should engage these situations except through increased defense spending. The lack of norms perpetuates such an environment as there exists no countervailing check on state aggression. This is not to say that a norms based regime would solve all the problems posed by third party cyber-attacks on the United States but it would make it harder for states to knowingly harbor such actors.[43] As the technology behind cyber attribution improves, which it is expected to do quickly, the ability to plausibly deny the knowledge of such agents will become increasingly difficult.

2) Second, the ambiguity over state definitions of cyber-attacks increases the probability that unwarranted escalation could occur in the event of a misunderstanding. The lack of information surrounding these thresholds also makes it harder to maintain a credible series of deterrents. If states are unaware of how the United States would react to a cyber-attack it leaves open the possibility for miscalculation. This is a problem that is explicitly addressed in the 2010 National Security Strategy[44]. This ambiguity must be addressed on an international level or a cyber-intrusion could be the catalyst for a major conflict

[41] *Ibid*
[42] Benjamin S Lambeth. 2011. Airpower, spacepower, and cyberpower. *Joint Force Quarterly : JFQ*(60): 46.
[43] Nye, Jr, Joseph S, and HARVARD UNIV CAMBRIDGE MA BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS. 2010. *Cyber power*.
[44] White House, *International Strategy For Cyberspace*. 2011. 9.

that could have been avoided.[45, 46] Uncertainty also exists over American defensive capabilities and this makes it harder to form a credible deterrent.

3) A lack of leadership is encouraging other countries, whose interests are diametrically opposed with America's, to fill the gap in global governance. China and Russia have been advocating for their own conception of internet security that would harm the openness that American companies thrive on. An official agreement settled on by the Shanghai Cooperation Organization defined cyber-attacks as the dissemination of harmful information[47]. This stands in stark contrast to American and Western thinking on the subject. The SCO is comprised of China, Russia, and several other small central Asian countries whose authoritarian tendencies pose a threat to the freedom the global internet is predicated on. If American leadership does not shape the course of the future "other states will step in."[48]

4) There is also an American image problem in cyberspace that is negatively impacting national security. Worldwide there is a perception of American exploitation of cyberspace engendered by a fear of our technical prowess and the revelations of Edward Snowden. This complicates efforts at internet governance as there is widespread belief that America's offensive capabilities are a core problem for the stability of the internet[49]. Clarifying American intentions and priorities in cyberspace could help assuage these fears and clear the way for international agreements that would benefit American interests.

---

[45] Lewis, James. "Multilateral Agreements to Constrain Cyberconflict." *Arms Control Today*. no. 5 (2010): 14-19.
[46] Nye, Jr, Joseph S, and HARVARD UNIV CAMBRIDGE MA BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS. 2010. *Cyber power*.
[47] Jason Healey. 2011. The spectrum of national responsibility for cyberattacks. *The Brown Journal of World Affairs* 18 (1): 57.
[48] Knake, Robert. "Internet Governance in an Age of Cyber Insecurity." Aug 2010. Council on Foreign Relations. Nov 2013.
[49] Jack goldsmith, "cybersecurity treaties: a skeptical View (february 2011)," in Future Challenges in National Security and Law, edited by Peter Berko witz, http://www.futurechallengesessays.com

The current state of affairs regarding cyber governance is untenable and will only worsen. Time is not on our side. As the access barriers to higher end computing continue to decrease the threat will become larger. While American defensive capabilities have increased over the years the recent trends point to an increased frequency and intensity in the attacks launched against American networks.[50] While American offensive cyber capabilities are substantial, we are by far the most vulnerable to cyber-attacks.[51] Any policy option meant to address the growing threat posed by cyberspace must weigh the benefits of curtailing our own capabilities against the potential costs of inaction. The asymmetry posed by our dependence on cyber-controlled systems for everything from our electricity to financial networks, makes the tradeoff more than worthwhile. The longer it takes to begin international engagement over cyber norms and clarify America's position, the longer the interests of the United States and the stability of international security will be needlessly jeopardized.

Policy Options

1) Maintain Status Quo. The United States could remain a signatory to the Budapest Convention on Cybercrime and hope that norms favorable to American interests develop organically. This entails significant risks because as detailed earlier foreign countries are actively seeking to partition the net into separate "national internet segments."[52] This would undermine its economic utility without addressing the underlying security problems.

[50] Thomas Rid (2012): Cyber War Will Not Take Place, Journal of Strategic Studies, 35:1, 15.
[51] Clarke, Richard A., and Robert K. Knake. 2010. *Cyber war : The next threat to national security and what to do about it: The next threat to national security and what to do about it*. New York: Eccoo. 226.
[52] http://www.cnas.org/theinternetyalta

2) A Multi-Faceted Cyber Engagement Campaign. The United States spearheads a multilateral international effort aimed at developing a legal framework for evaluating cyber-attacks. Part of this effort would be the pursuit of an Arms Limitation treaty for cyberspace that would prohibit first use on civilian facilities, tampering with financial markets, and the placement of logic bombs (code designed to carry out malicious functions when triggered) in foreign infrastructure.[53] This effort, even if it was unsuccessful in delivering a binding set of principles, could be foundational in developing a set of norms for national responsibility. This would move policy makers away from the attribution framework that paralyzes action today. This option would have the advantage of visibly reasserting American prominence in internet governance while simultaneously positioning us as guardians of internet freedom. Furthermore it would allow us to have a direct role in shaping the norms that will guide future use of the internet. A similar endeavor should also be pursued with our NATO allies that would build on its 2011 Cyber Defense Policy commitment to engage international actors.[54] This would allow American interests and definitions of cyber-attacks to be clarified in a global setting. Part of this campaign would also be the pursuit of bi-lateral understandings with rising powers whose conceptions of the internet differ from our own. As indicated earlier, promising work has already been done with Russia on this manner.[55]

[53] Clarke, Richard A., and Robert K. Knake. 2010. *Cyber war : The next threat to national security and what to do about it: The next threat to national security and what to do about it*. New York: Eccoo. 269
[54] NATO, *Defending the Networks The NATO Policy on Cyber Defense.* 3.
[55] See Note 13

3) Lone Wolf. The United States issues its own set of unilateral proclamations asserting that future attacks known to be emanating from within a specific nation state will be attributed to that state. This has the advantage of removing the ambiguity surrounding American attribution to cyber-attacks but does little to foster an international consensus on the appropriate response. While a small step in solving the problem, this policy is ineffective on its own. It should rather be viewed as one tool in a larger toolbox of policy strategies.

Recommendation

Cyberspace is a "network of networks that includes thousands of internet service providers across the globe" in which "no single state or organization can maintain effective cyber defenses on its own."[56] A problem transnational in scope requires a transnational response. It is thus our recommendation that the United States pursue multiple courses of action that increase transparency and establish settled cyber norms. In this section, we flesh out 1.) the norms the United States should seek to establish, and 2.) the areas in which Transparency and Confidence Building Measures (TCBMs) are needed. In the next section (Policy Options), we delve in to the multiple courses of action the United States could take to effectuate these norms and TCBMs on the international stage.

What norms should the United States establish?

In the White House Cyberspace Strategy, the United States signaled its interest to work with other states to develop partnerships and increased understanding.[57] By establishing a normative framework for cyberconflict, effective norms will stigmatize the

[56] Hathaway, Oona A. and Crootof, Rebecca, "The Law of Cyber-Attack" (2012). *Faculty Scholarship Series.* Paper 3852. http://digitalcommons.law.yale.edu/fss_papers/3852

[57] White House, *International Strategy For Cyberspace*. 2011. 9.

use of cyberspace in a way that might otherwise lead to escalated conflict.[58] The more explicitly stated the norms, the less chance for misunderstanding. We recommend the United States seek to establish the following explicit norms, which provide greater clarity to the following three unsettled questions between states:

What actions will be considered a cyber-attack, equivalent to a conventional act of war?

- Any use of a cyber network to undermine the function of civilian infrastructure, including:
    - Financial markets
    - Water systems
    - Air travel systems
    - Ports
    - Energy systems, including oil, gas, and electric
    - Hospital systems
- Any use of a cyber network to undermine the function of military infrastructure, including:
    - Significant disruptions or destruction of military networks
    - GPS systems
    - Radar systems
    - Nuclear facilities
    - Other space assets, including satellites

Who will be considered as acting on the state's behalf, should they engage in one of the above attacks?

- Military personnel
- Government personnel
- Intelligence personnel
- Third party actors, where evidence sufficiently shows that they were acting on behalf of any of the above

How does the location of origination of an attack affect whether a state is considered culpable?

- Who is acting in launching a cyber-attack will supersede where the action takes place in determining culpability. In other words, if agents of Country X utilize

[58] Lewis, James. "Multilateral Agreements to Constrain Cyberconflict." *Arms Control Today*. no. 5 (2010): 14-19.

networks in Country Y to launch a cyber attack, Country X will still be considered culpable for having launched a cyber attack.

Strategy behind the norms

These norms are formulated to provide greater lucidity in the cyber landscape, but they are also formulated strategically to serve the interests of the United States and increase the likelihood the norms succeed on the international stage.

First, we have purposefully abstained from recommending that the United States attempt to establish an internationally agreed-upon definition of a cyber attack. To do so risks engaging the United States in an abstract and futile quest and constrains the ability of the United States to conduct certain types of attacks. Rather, the more pragmatic approach that we have taken, and the one with the highest likelihood of international success, is to delineate specific actions that fall under the broad definition, rather than tackle the broad definition itself. Just as "terrorism" does not have an internationally agreed upon definition yet states have established specific actions they view as terrorist attacks, so have we, with these norms, provided more clarity to the actions that will be considered a cyber attack, without falling down the rabbit hole of defining cyber attack writ large.

Second, by including the phrase, "undermine the function" in our delineation of specific cyber attacks, we have excluded acts of cyber espionage from the realm of cyber attacks. This is significant in that the United States arguably does not want to establish norms that would curtail its ability to engage in cyber espionage, an arena in which it has a tremendous advantage.

Third, such norms do not limit the capabilities of the United States during wartime. These norms establish what cyber actions will be considered the equivalent of a conventional attack—they establish what will *lead* to war. But they do not establish, if a war is already taking place, the norms that govern wartime combat. Thus, the United States, by clearly delineating what cyber attacks will be considered equivalent to conventional attacks, decreases the likelihood of escalation to war while simultaneously leaving options on the table should a war unfortunately arise. This plays to the advantage of the United States; due to the asymmetric nature of cyber attacks, we have a great deal to lose from *being attacked*, but we also have massive superiority in this realm should we ever *need to attack*.

Fourth, there may exist concern that states will be unable to determine accurate attribution of cyber attacks. This is dangerous in that it could lead to the wrong state being accused of having launched a cyber attack. That being said, the ability for states to effectively attribute is rapidly increasing. A new technology called "deep packet inspection" allows cyber traffic to be screened at significantly increased levels.[59] This technological development is significant in two ways. First, it makes it easier for states to overcome the attribution problem, therefore giving the above-delineated norms more teeth. Second, as states become ever better at monitoring their networks, it increases the likelihood that misunderstandings and escalation could arise—increasing the necessity for established norms and TCBMs.

Finally, these norms come at a low cost to the United States. Even if it remains difficult to trace the origination of cyber attacks or link a third party to state culpability, norms such as these provide a baseline precedent that will guide state activity and, if a

[59] Lewis, James. "Multilateral Agreements to Constrain Cyberconflict." *Arms Control Today*. no. 5 (2010): 14-19.

state is successful in tracing an attack, give it grounds for action. Currently no internationally agreed upon baseline exists that would give any state grounds for action should it fall victim to a cyber attack of the kind we have delineated. These norms are a first step in rectifying this situation.

What areas need transparency and confidence building measures?

Transparency and confidence building measures are valuable in that they correct for information gaps, make intentions clear, and establish thresholds and thus deterrent effects. In the Tools of Engagement section we dictate specific TCBMs in which the U.S. can engage, but here we focus primarily on the area in greatest need of increased transparency: how the United States will respond to cyber attacks. By clearly establishing the actions the United States would take if provoked, deterrence effects will begin to take effect, limiting the likelihood that a state will choose to launch a cyber attack.

The norms established above determine the "what," "who," and "where" governing certain actions that are considered cyber attacks. But they left unresolved the manner in which the United States would respond should these norms be breached. As with norms, deterrence policy should be clearly stated to have maximum effect. We thus recommend the following deterrence policy be undertaken:

- In assessing whether to use defensive armed forces in response to a cyber attack, the United States will use the effects-based approach to determine if the effects of the attack are equivalent to a conventional armed attack.[60]
- The United States will seek to develop a credible deterrent by announcing its ability to "carpet bomb in cyberspace" using robot networks (botnets) that "direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries."[61]

[60] Hathaway, Oona A. and Crootof, Rebecca, "The Law of Cyber-Attack" (2012). *Faculty Scholarship Series.* Paper 3852. http://digitalcommons.law.yale.edu/fss_papers/3852

[61] Williamson, Charles. Armed Forces Journal, "Carpet bombing in cyberspace." Last modified 2010. Accessed December 6, 2013.

- If engaging in cyber attacks the United States will, in keeping with Jus in Bello, follow the Law of Armed Conflict, including principles of necessity and proportionality.[62]

Tools of Engagement

Unilateral Proclamations

Unilateral proclamations present the first tool in the United States' toolkit. Such proclamations are arguably the quickest and easiest policy strategy to utilize, as they do not rely upon other country's agreement to take effect upon being issued. Such unilateral proclamations could state United States policies and intentions, increasing deterrence effects and elucidating previously unclear U.S. stances.

There are three primary areas in which the United States would benefit in issuing unilateral proclamations: 1.) how the United States will use cyberspace, 2.) what the United States will consider a cyber-attack, and 3.) how the United States will respond to cyber attacks.

In this regard, the norms we previously delineated are informative, as they clearly establish policy with regard to the first and second of these question areas. The United States should clearly state its intention to follow these norms. Additionally, it should state its intention not just to follow such norms, but also to interpret the use of cyberspace by other states in reference to these norms. In this sense, unilateral proclamations can and should be used as a starting point, or a starting draft, from which to establish norms that grow into a larger multilateral agreement.

The deterrence policies previously delineated are equally informative for the third question area—how the United States will respond to cyber attacks. The United States

[62] Hathaway, Oona A. and Crootof, Rebecca, "The Law of Cyber-Attack" (2012). *Faculty Scholarship Series.* Paper 3852. http://digitalcommons.law.yale.edu/fss_papers/3852

should unilaterally proclaim its intention to follow these deterrence strategies, signaling to other countries the manner in which their actions might draw a U.S. response, helping to remove ambiguity.

Bilateral Agreements

Bilateral agreements present one of the most promising areas for developing norms and TCBMs. The White House Cyberspace Strategy indicated that, "The United States is currently prepared to build bilateral partnerships."[63]

Russia

The most promising area for progress in this area is with Russia. The Obama Administration has been engaged in discussions with Russia over the last year to establish a bilateral agreement, stating in an official White House document that, "[The U.S. and Russia] are now leading the way in extending traditional transparency and confidence-building measures to reduce the mutual danger we face from cyber threats."[64] In this vein, both countries have placed an increased emphasis on senior-level dialogue, with a bilateral working group that will focus on identifying information and communication technology threats and coming up with potential solutions.[65]

The discussions between the United States and Russia have primarily been focused on building off of The Nuclear Risk Reduction Center (NRRC) previously established by Ronald Reagan in 1988 to lower Cold War tensions. Originally built so that the United States and the USSR could notify each other of missile tests and space launches that might be mistaken as aggressive acts, the NRRC could be used for equivalent purposes in cyber. In the case that activity is detected by either Russia or the

[63] White House, *International Strategy For Cyberspace*. 2011. 9.
[64] Amber, Corrin. FCW: The Business of Federal Technology, "U.S. teams with unexpected new cyber ally." Last modified June 19, 2013. Accessed December 6, 2013. http://fcw.com/Articles/2013/06/19/russia-cybersecurity-cooperation.aspx?Page=1.
[65] Ibid.

United States, communication could be activated to allow for the easing of tension. Even more significantly, Russia has already agreed, as does the United States, that the Law of Armed Conflict applies to cyberspace. Codifying the application of the LOAC, establishing the new use of the NRRC, and creating a "phone-based hotline" between the U.S. and Russia, similar to the nuclear hotline currently in existence, could form a three-pronged bilateral agreement. Such an agreement would drastically decrease the likelihood of potential misunderstandings between two of the world's most prominent cyber powers.[66]

China

The United States's current success with Russia is to a large extent rooted in its shared perception of threats. Both face large amounts of cyber theft at the hands of China and both deal with third-party hacktivists. Additionally, a shared history of norm and TCBM development exists between the two nations. The same cannot be said for China, but there is reason to be hopeful that similar bilateral measures between the United States and China might have promise.

First, any success with a bilateral agreement between Russia and the United States would put pressure on China to state its intentions in the cyber realm. The United States, Russia, and China currently stand as the three most powerful players in cyber. China would not want to create a situation in which it has isolated itself from the other two major powers.

[66] Nakashima, Ellen. "In U.S.-Russia deal, nuclear communication system may be used for cybersecurity." *Washington Post*, April 26, 2012. http://articles.washingtonpost.com/2012-04-26/world/35453448_1_cyberspace-cybersecurity-russia-and-china (accessed December 6, 2013).

Second, both the United States and China benefit from greater clarity and understanding with regard to each other's intentions. Both desire to avoid escalation to conventional warfare or crippling attacks on infrastructure.

Third, and most significant, both the United States and China are harmed by the asymmetric nature of cyber attacks. Both are great powers that, due to the nature of cyber attacks, find themselves uniquely vulnerable to small states or third-party actors. In that cyber attacks could be used as a leveling device to even the playing field between actors, both China and the United States benefit by increased cooperation to establish norms and TCBMs.

Multilateral Institutions and Agreements

Working through Multilateral Institutions such as the UN and the NATO alliance would present the United States with a global forum to shape cyber issues. In this regard, the norms previously delineated would serve as an excellent launching pad for an international code of conduct. The 2011 International Strategy for Cyberspace already cites increased involvement by the Obama administration with regional organizations such as the Association of Southeast Asian Nations and the G-8 in addressing cyber issues.[67] Utilizing these frameworks to promote and clarify the norms of state behavior in cyber-space would provide a powerful set of institutional factors promoting stability. The United States could use these venues to pursue an arms limitation treaty for cyberspace. Such a treaty as indicated earlier would seek to establish a no first-use policy on civilian infrastructure and also seek to prohibit the placement of logic bombs during peacetime[68]. These practices are inherently destabilizing and a prohibition on their implementation

[67] White House, *International Strategy For Cyberspace*. 2011. 11.
[68] Clarke, Richard A., and Robert K. Knake. 2010. *Cyber war : The next threat to national security and what to do about it: The next threat to national security and what to do about it*. New York: Eccoo. 269.

would appeal to many nations. It would also give credence to the retaliatory policies set out by the United States if more nations adopted similar practices.

Conclusion

This paper has sought to address America's growing vulnerability to cyber attacks. As this nations dependence on networks for every facet of American life increases, remedial steps must be taken to secure the source of this vulnerability. Norms of non-use and restraint have begun to develop in the international community, but this is no guarantee of increased improvement or security. Proactive measures are needed to solidify these practices and insure future progress. The means to achieve these ends have been elucidated within this paper. They include the pursuit of multilateral agreements aimed at addressing the asymmetric nature of the United States' exposed position in cyberspace. The development of norms regarding what constitutes a cyber attack is a foundational step in establishing a regime necessary to protect American interests.

Grand Strategy must consider all aspects of national power. Interconnected networks have come to occupy a crucial space in this calculus. As the United States looks ahead to a potentially turbulent future, our ability to secure the cyber sphere will protect critical elements of our national power. This is an inflection point not only in the history of cyber strategy but more broadly considering the uncertainty of the United States' future role in the world. Should the United States not advance a cyber strategy on its own terms we cede ground to our adversaries, forfeiting leadership in this crucial arena at a time when the United States' future dominance is already questioned. This is not an opportunity the United States can afford to miss.