# Cybersecurity and Rising China: Analysis of Policy Proposals

Matthew Steyl

University of North Carolina at Chapel Hill

Curriculum in Global Studies

April 8, 2014

## Chapter 1: Background and Introduction

### Introduction

In the US today, discussions of foreign policy by politicians and policymakers across the country have been dominated by a single subject: a rising China. As two wars wind down, the US has turned its attention East-- dominated in particular by President Obama's "Pivot to Asia." Candidates for office have embraced "tough on China" as a qualifier as necessary for ensuring success at the polls where "tough on crime" was not long before. One particular area of US-China friction gaining prominence is that of cybersecurity: the protection of US intelligence and digital infrastructure, as well as private intellectual property, from electronic attacks and intrusions (DHS "Cybersecurity Overview").

Chinese hackers have struck United States government agencies and businesses, including banks and news organizations, a direct provocation that has since been traced back to the Shanghai headquarters of the People's Liberation Army (Mandiant). Even more recently, documents have emerged alleging US cyber incursions against Chinese targets. This conflict has become a direct and pressing source of enmity between the US and China, and has begun to elicit aggressive proposals from US policymakers.

The escalating "cyberwar" with China is one facet of the countries' long-standing and increasingly conflicted relationship, and is extremely integral to the future of that relationship. Protecting US strength and intelligence in this arena is vital to the maintaining of US global political and economic hegemony and its ability to take a leading role in Asia.

Power, especially in the international sphere, is relative, and so as China rises relative to the US, its power, in Asia as well as globally, has grown dramatically, threatening US hegemony and the current geopolitical order. How the US handles this rise and relations with China, especially in areas of economic conflict and competition, will have a large effect on the future of the US-China relationship, US international hegemony, and China's future power.

**Background and Historical Context**

China's rise, coupled with US's domestic financial issues, has threatened US status as the world's sole superpower. China is already a regional power, wielding significant influence in Asia and dominating Asian politics; as it continues to grow and expand its reach it will soon be a world power, possibly a superpower. How the US handles its economic competition with China now will have far reaching consequences for both countries, and the world.

If the United States is to maintain its global influence, it must adequately address such emerging threats as direct cyber attacks on its businesses and government entities. US national defense, economic security, and its mandate of spreading democracy and rule of law abroad all depend on the maintenance of that influence, and its ability to direct the discussion and impose its will abroad. Only through a rational and nuanced policy response to these threats can the US guarantee continuing dominance and influence on the global stage.

Knowledge of Chinese hackers first came to public light in a report published by the private security contractor Mandiant, entitled "Exposing One of China's Cyber Espionage Units." Mandiant identified China's People's Liberation Army (PLA) Unit 61398 as the origin of many cyber attacks, perpetrating "a long-running and extensive cyber espionage campaign" with the help of direct funding from the Chinese government, based in a neighborhood in Shanghai near a PLA base. Unit 61398's work is considered a "state secret," and it allegedly employs hundreds of hackers. "Mandiant has observed APT1 (Unit 61398) compromise 141 companies," 115 of which are in the US, with this observation representing only a fraction of the group's activities (Mandiant).

Victims include firms in information technology, aerospace, public administration, telecommunications, as well as companies representing several other industries. These security breaches have led to the thefts of intellectual property from its victims over periods ranging up to five years. Unit 61398's persistent, state-funded cyber attacks against US represent a dangerous and direct foray against US interests. US Congressman Mike Rogers has called it a "massive trade war" against the US and its European allies.

A range of responses have already been proposed to deal with this threat, including both possible means of retaliation and defensive measures. These attacks are direct attempts at stealing US intelligence data, and cyber espionage is damaging to the US's national defense and security efforts in the region. Chinese overtures are also a direct threat to the competitiveness of US firms, and the private information of their clients, as this information and the intellectual property which ensures competitiveness are made available to competing, often government-controlled Chinese firms.

To effectively protect American intellectual property from theft by Chinese firms, as well as government and military secrets, the US government must enact an effective policy response to these attacks. China relies on these thefts to empower its own state-owned enterprises and to improve its own security and intelligence apparatus, and will not give up lightly this method of ensuring its firms competitiveness.

Even more recently, allegations of US cyber attacks against Chinese targets have surfaced. When whistleblower Edward Snowden revealed the existence of the National Security

Agency (NSA) program PRISM, which allegedly conducts online surveillance and widespread data collection of US citizens as well as those of other countries, including China, Chinese officials were quick to point out the hypocrisy of the US condemning China's own cyber overtures.

The NSA also allegedly employs its own "team of hackers and spies" to target US rivals, including and especially China (Aid). This team, called the Office of Tailored Access Operations (TAO) has "successfully penetrated Chinese computer and telecommunications systems for almost 15 years." TAO's cyber espionage is a mystery even to most NSA agents, and only those with the highest levels of security clearance are permitted to access its workspaces.  TAO's goals are similar to those of the PLA's Unit 61398; to collect intelligence on foreign targets by hacking into computer systems and stealing data from the compromised computers' hard drives. TAO is also charged with developing the means to use a cyberattack to destroy foreign telecommunications and computer systems.

Both countries can be seen as equally guilty and it will be difficult to develop a response to the Chinese attacks without at least addressing the US's part in the cyber conflict. The US's ability to condemn or in any way respond to Chinese cyber attacks is mitigated by any involvement in cyber attacks and attempts at intelligence gathering in China. At the same time, the US cannot afford to stop these efforts without at least determining a means to prevent the Chinese attacks as well.

**US Policy Responses**

In the US, considerable attention and energy is currently devoted to responding to this new development, with many diverse policies recommended by a variety of policy experts and politicians. Constituents are directly affected by a rising China, including those whose jobs are outsourced, and those who similarly face unemployment when Chinese organizations outperform their American competitors.

In the government's most prominent response to China's rise, President Obama has announced a "Pivot to Asia" which would rebalance and refocus US foreign policy to the Far East, and shift US efforts to respond to the new foreign policy challenges posed by China and by Asia as a whole. The Obama administration is carrying out this pivot with the understanding that the rise of China and other nations in East Asia will affect global policy in the coming years.

The Pivot anticipates the US taking a direct role in resolving its economic disputes with China, including cybersecurity and intellectual property theft, as well as in other area conflicts including those in the South China Sea and other territorial disputes. Former Secretary of State Hillary Clinton promised the Pivot would result in engagement with China over human rights issues as well (Campbell).

During the 2012 election cycle, an oft-repeated policy touted by Presidential candidate Mitt Romney was to label China as a currency manipulator. Romney prioritized this response so highly that he often claimed he would take this action on the first day of his Presidency (Wingfield and Katz). Currency manipulation, according to Romney and others, has allowed Chinese firms to outcompete American ones, and has increased demand for Chinese goods.

Addressing cybersecurity is a more recent development, but calls for leaders to take decisive action are increasing in volume and number. Directly accusing and confronting China over these cyber attacks itself reflects a more aggressive response to rising China, and may provoke further conflict and competition as a result, so more accommodating responses should also be considered.

Responding to these concerns, legislators reintroduced CISPA for the second time in two years in February 2013. CISPA, or Cyber Intelligence Sharing and Protection Act, has bipartisan co-sponsors in Congress, but is widely reviled by many groups in the US. Its goal is to protect US businesses from cyber attack by improving their ability to share information with each other and the government (HR 624). However, Internet companies and privacy advocates alike denounce the bill, claiming it violates certain rights and civil liberties in the name of security. Proponents of the bill argue that it is necessary for the protection of US cyber infrastructure, businesses and intellectual property against cyber threats, in particular those originating in China.

Other attempts to improve US cybersecurity against Chinese incursions have been made, including by the President, who also in February 2013 issued an executive order with new cybersecurity guidelines for companies; this order was received much more favorably by domestic groups than CISPA, although its effectiveness is as yet unproven (Executive Order -- Improving Critical Infrastructure Cybersecurity).

These policies reflect the attention and importance given to this issue by leaders in the United States, and represent the first response to the discovery of a Chinese cyber threat. The President, members of Congress, and other political candidates, have all prominently advocated for and taken policy actions to deal with China’s cyber attacks on US businesses and intelligence agencies.

“Tough on China” is thus an important trait for political candidates touting their foreign policy bona fides, many of whom go to great lengths or espouse radical policies in an effort to earn this description. As unemployment remains steadily high and the US economy stagnates, many American leaders and policy experts point to China, whose undervaluation of the Renminbi, skirting of trade rules and regulations, and, now, cyber attacks on US firms, demonstrate economic transgressions which require swift response from the US.

A confrontational response has many backers, both in the political arena and among academics and experts, who tout potential economic forays against China as the means by which the US can maintain its primacy as a global power. There is also a call among many think tanks and policy groups, represented in a wide spectrum of views, for a more moderate, balanced approach to China, wherein cooperation is valued much more highly than competition.

The US response and actions in the cybersecurity realm, therefore, is not only vital to determine the relationship of these two nations and the future of US hegemony in the East, it is also an important demonstration of how foreign policy goals and practices are determined and implemented by different leaders in the US.

## Research Question

The thesis will analyze the proposals of policy experts, from a variety of political ideologues with a multitude foreign policy ideals and goals. The main goal of this thesis is an analysis of policy responses to the issue of cybersecurity, with an eye towards which proposals are preferable to and more politically viable than others and what aspects of policies make them preferable or not, and viable or not.

Due to the position of public opinion, politicians have historically favored more protectionist policies than might otherwise be the case (O'Halloran). This cybersecurity issue will serve as a demonstration of how tending towards “tough on China” in order to curry public favor might not offer the ideal foreign policy to protect and advance US interests.

This thesis will examine policy prescriptions from think tanks representing a variety of political ideologies and backgrounds in order to help to elucidate a more rational and nuanced policy which both advances US interests and helps maintain its economic strength and security interests on the world stage, and then analyze, based on dominant political pressures and the current ideological climate, the viability of these proposals to determine which if any of these proposals are likely to happen, and how the cybersecurity issue is likely to continue to unfold.

# Works Cited

Aid, Matthew M. "Inside the NSA's Ultra Secret China Hacking Group." *Foreign Policy*. Foreign Policy, 10 June 2013. Web.

Campbell, Kurt. "The Obama Administration's Pivot to Asia." The Obama Administration's Pivot to Asia. The Foreign Policy Initiative, Washington, DC. *The Foreign Policy Initiative*. Web.

"Cybersecurity Overview." *Homeland Security*. United States Department of Homeland Security, n.d. Web.

"Executive Order -- Improving Critical Infrastructure Cybersecurity." *Whitehouse.gov*. The White House, 12 Feb. 2013. Web.

Mandiant. *APT1: Exposing One of China's Cyber Espionage Units*. Rep. Mandiant, Feb. 2013. Web.

O'Halloran, Sharyn. *Politics, Process, and American Trade Policy*. Ann Arbor: University of Michigan, 1994. Print.

United States. Cong. House. Intelligence. 113th Cong., 1st sess. HR 624. U.S. House of Representatives Permanent Select Committee on Intelligence, 18 Apr. 2013. Web.

Wingfield, Brian, and Ian Katz. "Romney's Pledge on China Currency Won't Be Met in a Day." *Bloomberg.com*. Bloomberg, 24 Oct. 2012. Web.

## Chapter 2: Literature Review and Key Terms

### Comparing Policies

In order to determine what would be the best responses and solution to the cyber attacks originating in China, it is important first to explain what makes some policy responses preferable to others. In the simplest terms, the better a policy's outcome for the United States, the better that policy is relative to others.

The realm from which this paper draws is first that of think tanks based in Washington DC, those which have a closer proximity to policymakers and are therefore both more informed about policy issues and more influential on policy actions. These think tanks frequently publish literature on a variety of public policy issues, and increasingly their attention has turned to China, and to cybersecurity.

Within this more specific category of think tanks' cybersecurity analyses, only those which actually provide recommendations are used. Many experts simply make note of the changing dynamic of cyber issues; those which also build upon that dynamic to provide insight as to how the US might proceed form the dimensions for this study.

The literature is examined from a US perspective, and so the "best policy" is that which is best for the United States, not necessarily the preferred policy China would have the US take. Because they are developed by US political thinkers, these policies are written to appeal to and advance US interests. A policy which is preferable for the US would only be preferable for China as well in such cases where the US can hope to advance its own interests by ameliorating Chinese concerns or issues.

The intended outcome of any such policy is the advancement of US national interests. Given that the advent of Chinese cyber attacks is both detrimental to US national interests and a direct threat to national security, it is assumed that the more a policy is able to ameliorate these issues, by improving cybersecurity and the protection of American cyber infrastructure and intellectual property or by discouraging the continuation of these attacks, the better that policy is from the viewpoint of the US However, both the “national interest” and “national security” have a broader definition in established literature, and one which is important to the comparison and evaluation of policy proposals and potential solutions to this issue.

### The National Interest

All proposed solutions for the cybersecurity issue seek first to protect US intelligence, intellectual property, or both, but through different methods and so with varied final results and additional effects. Analyzing the value of a particular proposal requires attention not only to the amount by which the problems are alleviated, but also how this alleviation and overall anticipated effects of the proposal affect the US “national interest.”

This national interest is defined variously by scholars. The neoliberal view of globalism states that a nation’s interests have a basis in security, but extend to economic growth and the accumulation of wealth (Lechner and Boli). That is to say, a nation seeks first to maintain its own preservation and national security, but as long as these goals are met, and even while they are being met, “national interest” focuses on economic prosperity.

Alternate views of globalism and of national interest, including increasingly popular justice globalism; focus on the rights of citizens, on cultural and societal values and protections, and on fostering improved socioeconomic equality and growth (Lechner and Boli). These goals can also be evaluated in policy, although they are less easily measurable and less directly tied, in a political and economic sense, to the global standing of the nation.

The national interest of economic wellbeing is an aggregate, and so policies which seek to promote that interest should be judged by the promotion of aggregate wellbeing, not just the prosperity of a single industry or group. Moreover, the national interest that is based on national security is also fluid and changing, as noted by Jordan et. al.. This idea of security is based on maintaining US policy hegemony, the ability of the United States to have total freedom in dictating its own policy choices (Romm, Defining National Security).

National interest is in this way a metric by which policies can be evaluated. Those which are more useful to the promotion of this national interest, in the area of cybersecurity, are themselves better policies than those which are not. Thus of these policies, those which are strongest are those which could contribute the most towards this national interest.

## Literature on China Policy

China’s rise to prominence has generated considerable debate and conjecture regarding the US’ potential responses to this rise. This debate, however, is mired in issues, often narrow, and frequently treats the unfolding relationship between the US and China with a particularly Washingtonian brand of elitism. Treatment of China by DC experts tends in many cases, and with few exceptions, to employ this elitism, as well as exoticism and a general lack of nuance that limit the quality of the discussion.

The elitism that pervades the discussion of China frequently portrays the US, and the West in general, as defenders and protectors against Chinese aggression. In general, the debate lends itself to giving the US the benefit of rational, nuanced, and developed understanding, while denying this type of analysis to China. The problem with this view of the issue is that it takes away from any true understanding of Chinese agency, and prevents actions and policies from considering China's own interests beyond perceived aggression. That is not to say that China's actions are neither expansionist nor aggressive, but that the debate over rising China would benefit from a more complex perspective.

Another feature of this growing debate is its exoticism. In the West China has maintained an exotic, mysterious, and opaque image since the colonial era. Exoticism is present in all aspects of the policy debate surrounding China, and even manifests itself in how foreign policy experts understand their own roles in the discussion of China. Those who advocate for strong responses in the face of a rising China, who see China as a new global threat, are categorized in Western literature as "dragon slayers," while those who want to enforce a more diplomatic, softline solution are the "panda huggers" (Epstein). These sorts of descriptions are emblematic of the polarized and often mystical nature of the discussion generated by a rising China.

There are some exceptions to this rule, including Brookings Institute expert Cheng Li, whose voice features prominently in this debate, in his frequent scholarly writings as well as in numerous news articles, briefings, lectures, and other meetings in the DC foreign policy circuit. Improved discussion of China can be modeled after his writing, which invokes a more holistic view of China, including its own domestic issues, interests, and aspirations, without the exotic overtones (See "NSA Revelations Have Irreparably Hurt US Corporations in China" as an example).

By freeing the policy debate from these limitations, US policymakers can develop more nuanced solutions and policy responses to the issues that rise with China. Thus, such literature which takes a more nuanced approach to relations with China, and attempts to present or at least understand the Chinese perspective, is less limited and therefore stronger than literature which does not. Of course, many cybersecurity policy proposals are not specific to China, and so those which do not involve international collaboration or diplomatic overtures as a specific means to alleviate cyber concerns are not measured on this basis.

## Literature on Cybersecurity

Recent revelations regarding extensive cybersecurity operations in the US and cyber attacks against it have spurred production of policy proposals and analyses attempting to elucidate this issue. However, much of this cybersecurity discussion is arcane, mystified, and in some cases misinformed. Limitations on discussions of cybersecurity include a focus on some aspects to the exclusion of others and a profound ignorance or lack of commentary of the US's own role in cyber issues.

Each time the press and policy experts try to elucidate how far the United States government has gone in its surveillance and other cyber activities, new revelations expand upon this understanding, rendering previous discussions obsolete. Knowledge of extent of Chinese and other incursions on US cyber territory is also consistently updating. And the capability of nations, governments, and companies to protect themselves and attack or survey others is continuously advancing.

Discussions of the issue of cybersecurity need to include this understanding, and recommendations need to include a view to the future rather than attempts to rectify past mistakes and meet previous threats. Many such discussions vaguely speak in terms of improving

US cyber capabilities without defining clearly what that means and how cybersecurity is changing, and will continue to change in the future.

Recent leaks by Edward Snowden among others have shown the US, in particular the National Security Agency, to be guilty of spying on foreign targets and in some cases of outright cyber attacks (Gellman and Nakashima). The existing literature which does acknowledge this culpability is stronger for it, as responses to China's activities and the expanded cyber threat must include what actions the US already has taken and can take, not just potential new responses.

In that same vein, the historical context of cyber industrial espionage is also frequently ignored. China is a developing nation, trying to keep new industries afloat through aggressive means. In a historical sense this sort of industrial espionage is not new, only the means by which it is carried out are recent developments. Other developed countries, including the US and Great Britain, are guilty of similar, historically analogous acts of espionage and protectionism. Although the US must in its policies attempt to do what is in its own interest, as already discussed, understanding the Chinese perspective in this way can be useful for framing the discussion to meet causes, not symptoms, of cyber threats.

The right to privacy or lack thereof is the principle domestic political concerns extant in the cybersecurity debate in the US, but any mention of this point is largely one-sided. Privacy in this context refers to setting limitations on what individual data and correspondence the federal government can collect. Potential policies to respond to cyber attacks which account for privacy concerns are stronger than ones that do not, and are more viable for it. The Snowden leaks have made expansions to NSA capabilities politically toxic, and that is entirely due to the issue of privacy. No policy is truly viable or reasonable which intrudes further on the perceptions of individual privacy.

In evaluating policies in the realm of cybersecurity, a vital quality is their knowledge of and attention to details related to this issue. The more specific a proposal is, the more useful it is to policymakers considering it. One of the weaknesses of many policies and their authors in this arena is that the arcane and detailed problems are often confronted using broad, general solutions. Rather than to simply advocate for agencies to train more agents, for example, a better policy would explain in what they would be trained. Rather than suggesting the government support businesses, a better policy would explain what areas and means of support are needed. In short, the more specifically a policy purports to improve cybersecurity, the stronger that policy is.

## Literature on Political Likelihood of Foreign Policy

Examinations of foreign policy in terms of viability are limited in their ability to accurately predict passage through Congress. Most analyses focus on party politics, on a basic liberal-conservative spectrum, and on district influences, to determine how members will vote. However, a basic understanding of the layout of Congress and how Congress usually proceeds and votes on bills can help to demonstrate where bills might fail, to help show a lack of viability of certain legislation.

The prominence of uncompromising ideologies is also more pronounced today than ever before. In Congress compromise has become a dirty word, and members fervently stick to their ideological guns. This phenomenon is responsible for the decline in Congressional activity and the increase in vicious partisanship in the past years, and as a result makes a viable bill even more difficult than previously. A more successful bill would account for this shift in ideology by appealing to a mix of ideologies and preferences. Likewise proposals whose authors account for the preeminence of ideological hardliners in Congress are more likely to be politically viable as legislature.

## Contribution

The main contribution this research can make to existing literature on the subject is an enhanced and nuanced look and judgment of potential cybersecurity policies. Through analysis of the broader goals of US cyber policy and the means by which experts propose the US achieve those goals, a framework is formed in which these proposals can be judged for their possible efficacy. This contribution is not a single policy recommendation, but rather a broader understanding and aggregation of the nature of the issues related to cybersecurity and of the policies which address them, or not as the case may be.

Demonstrated in this study is an understanding of the threats posed by Chinese cyber attacks to the United States, both private and public interests, how these threats might best be addressed through policy, with an eye to how these policies affect overall national goals and standing, both politically and economically, and both domestically and abroad.

This understanding will make it easier also to observe how policies taken in response to these specific issues fall into certain patterns, and which patterns represent more preferable or useful policies. Analysis of these patterns of responses and of idealized solutions will elicit what goals the US should and does pursue, and why these goals are or are not actively pursued, and what this means for the future of US-China relations and the cybersecurity issue.

# Works Cited

Epstein, Gady. "Panda Hugger Vs. Dragon Slayer." *Forbes*. Forbes Magazine, 29 Jan. 2010. Web.

Gellman, Barton, and Ellen Nakashima. "U.S. Spy Agencies Mounted 231 Offensive Cyber-operations in 2011, Documents Show." *Washington Post*. The Washington Post, 30 Aug. 2013. Web.

Jordan, Amos A., William J. Taylor, and Michael J. Mazarr. *American National Security*. Baltimore, MD: Johns Hopkins UP, 1999. Print.

Lechner, Frank J., and John Boli. *The Globalization Reader*. Chichester: Wiley-Blackwell, 2011. Print.

Li, Cheng, and Ryan McElveen. "NSA Revelations Have Irreparably Hurt U.S. Corporations in China." *Brookings*. The Brookings Institution, 12 Dec. 2013. Web.

Romm, Joseph J. *Defining National Security: The Nonmilitary Aspects*. New York: Council on Foreign Relations, 1993. Print.

## Chapter 3: Methods and Data

### Methods

A variety of policy recommendations will be sampled and analyzed, both to ensure a thorough, holistic view of the cybersecurity issue and also to ensure that there are enough policy proposals sampled to help develop a nuanced, cohesive definition of how to protect US cyber infrastructure from aggressors such as China. The proposals surveyed are authored by an expert source and published by a think tank, active in the realm of foreign policy, the US-China relationship, and of global affairs in general. Using think tank-sponsored proposals also allows for easy analysis of the political ideology of the author and the likely potential support for that proposal as legislation.

Politics and ideology are unique characteristics of these policy proposals, separate from the actual quality of the proposal; they are useful for amassing a diverse selection of policies. The proposals selected reflect a variety of ideological backgrounds, and include left wing, right wing, and centrist policies, as well as other views: the more conservative American Enterprise Institute, and the bipartisan Council on Foreign Relations. Even in policies derived from similar ideologies there are differences in their foreign policy outlook; some experts advocate for stricter responses to China, while others propose more conciliatory approaches. These policymakers are the so-called “dragon-slayers” and “panda-huggers,” respectively.

To compare the practicality and value of hard-line and soft-line policies with each other, as well as with similar policies, can help to determine whether it is better for the US to take a more confrontational role against China, or not, and to help determine the best way to take such a role. An effective analysis can be drawn using both hard- and soft-line liberal policies, as well as hard- and soft-line conservative policies. The distinction between political ideology and foreign relations philosophy can demonstrate how policy experts and politicians may come to different conclusions based on different viewpoints, constituencies, and political pressures. By emphasizing this variety the analysis and discussion can be both more nuanced, and more effective in determining preferable policy responses.

## Data

The proposals to be reviewed consist of policy papers, articles, forums, and speeches published by a variety of think tanks, which reflect a wide spectrum of viewpoints, and whose authors represent various professional backgrounds, including academic and political. The policy papers and academic essays each present a response or set of responses to developing cybersecurity issues. Analysis will consider the policies therein, based on their viability in addition to their quality, to make comparisons and develop overall patterns present in useful and poor policies. Each expert subscribes to a certain political ideology; taking note of this ideology will help to more accurately understand the policies and why they might differ from each other and from the policies of elected officials.

The particular policies sampled derive from some of the leading think tanks based in DC, those which are of particular importance to the Republican and Democratic parties in providing policy advice. Choosing these think tanks ensures that the proposals surveyed are in fact likely to at least be readily available to and heard by political leaders and policymakers. These particular proposals were selected based first on the ideological spectrum, with an eye to diversity, including generally-considered conservative, progressive, moderate, libertarian, and nonpartisan institutions.

The United States General Accounting Office provides a useful framework for the design and evaluation of case studies (GAO) that helps to explain why these particular policies were selected and are useful for examining potential cybersecurity policies as a case study of US policy in general. These proposals are the instances of this case study, and fill the criteria laid out by the GAO report as a basis for selecting instances.

The proposals used were selected based on purposive criteria; they help to fulfill the purposes of this examination as a case study, including analyzing the bracketing, best cases, worst cases, cluster, representative, and special interest cases (GAO 26). These proposals include both specific, nuanced policies and broad, general policies to “bracket” the discussion (GAO 26); proposals that are strong and those which are not represent the best and worst instances, respectively, while “special interest” proposals reflect, as the GAO report states, a “particular circumstance” such as policies that reform privacy protections, a particular aspect of the overall cybersecurity issue.

The most important purposes considered when selecting these instances of cybersecurity policy proposals were “cluster” and “representative” ones (GAO 27). The purpose of cluster is to answer the question “how do different types of programs compare with each other” (GAO 27) by selecting similar, comparable programs. In this case, several proposals which sought to directly alleviate the issue of cybersecurity represent a cluster of similar proposals, and their methods and potential efficacy can be used to examine how that goal might best be reached. Representative selection means choosing instances based on important, distinct variations (GAO 27). In this case, the proposals were selected to represent particular variations on how to respond to cyber threats, including direct improvements, international cooperation, and public-private partnerships, among others.

The think tanks selected are those which were found to have a significant presence in Washington, and which are frequently cited by journalists and policymakers alike. Aside from representing different points along the ideological spectrum, they also are those which publish and make publically available their research, articles, and policy papers, such that they were easily accessible for research and analysis. The selection was conducted in the spring of 2013, and those think tanks which were particularly active in the field of US-Asia relations and related international issues during this period, either by hosting seminars and other events or by publishing articles and policy papers related to that subject, are among those surveyed for policy proposals.

From these think tanks, the particular policy papers or articles selected were simply the most recently published by their respective think tanks that were publically accessible, devoted to the issue of cybersecurity, and contained recommendations for governmental action. Papers which analyzed the state of the cybersecurity issue without providing any suggestions for reform were not selected because they are not useful for this research and analysis, even if they were published more recently than those which did present suggestions.

These decisions, of selecting the think tanks most representative of different ideologies and most active in the US-China and cybersecurity policy sphere, and then from those think tanks selecting the most recent cybersecurity policy recommendations suitable for analysis and comparison, were made at the discretion of the author. As such, they represent a limitation for this study; sampling these proposals required the author to decide which think tanks, based on their activity, and which proposals, based on their addressing of the cybersecurity issue with analyzable suggestions, were most relevant and useful for this analysis.

## Methods of Evaluation

A large sample of literature will be taken; to increase the likelihood patterns can emerge and more nuanced conclusions be made. This literature is still new, and the issue itself still developing, so only by considering many solutions can this more developed pattern be understood, and the relative overall potential efficacy of the proposed solutions be properly understood.

The policy papers and opinion articles will each present a theory, that if a certain policy action is taken, a specific result will occur, with the result resolving to some extent the cybersecurity issue. Other results of the policy action taken, whether enumerated in the paper or implicit based on the actions themselves, are also useful in measuring the impact, viability, and overall quality of the policy proposed. In addition to their attention to cyber threats, these other results are important considerations when comparing the proposals.

These other results may pertain to the broader national interests, including such economic effects as changes U.S. Gross Domestic Product, unemployment and inflation rates, as well as broader security concerns, effects on regional conflicts, relationships with other nations, and on other issues between the U.S. and China, culminating in the United States' status in world politics. The policies must solve the issues at hand, but overall they should advance or at least help maintain overall US interests, without diminishing economic effects or threats to national security.

Specifically, the criteria that define a "strong" proposal are those which make it most useful to policymakers. Stronger proposals give more specific recommendations rather than broad or general strategies. They also emphasize, where possible, collaboration over confrontation, whether between government agencies, public and private organizations, or between countries. And stronger proposals, most importantly, are understanding of and tailored to the specific nature of cyber threats, and are well-suited to alleviating them as problems unlike any other security or intellectual property issue.

Analyzing the proposals in this way, with a focus on developing patterns of responses and observing their similarities and differences is a qualitative method that Charles Ragin calls “analytic induction” (Ragin). He describes analytic induction as an investigation that “focuses on a primary case, and among the commonalities among separate instances of the same phenomenon” (Ragin). In this investigation, the primary case is cybersecurity policy, and the various proposals to be analyzed are the separate instances, the commonalities and differences of which will be the focus of the investigation.

Analytic induction is useful for examining the cybersecurity issue because it allows for policies to be combined into groups based on similarities, with those similarities, as well as the disparities between those within and without the group, helping to better explain the issue. In particular, similarities between strong policies can help to elucidate what aspects make a policy preferable, and disparities can show where certain policy proposals are weak, or how they might be improved.

“These comparisons… help to define categories and concepts” (Ragin), in this case the categories that comprise strong and weak policies, or hard and soft line policies, or politically viable and unviable policies.  Ragin stresses that analytic induction is used by researchers to “pay close to evidence that challenges or disconfirms whatever images they are developing” and to “seek out contrary evidence because it sees such evidence as the best raw material for improving initial images" (Ragin). Thus the variation in policy choices plays an important role, to help expand or contract the "initial image" of what constitutes a strong policy by providing additional context.

## Comparing Literature

It is pertinent not just to look at the extent to which a policy would protect against or deter cyber attacks, especially if the author of the proposed response does not believe that most directly responding to these issues is in the nation's best interests. Instead, special attention should be given to how the author intends to improve the U.S.'s overall wellbeing, with particular attention to how that improvement deals with cyber issues. For example, an author might be willing to concede that rather than protect directly against cyber attacks, the country should instead engage China through different avenues in order to reduce these overtures. This might not immediately reduce cybersecurity threats but could, potentially, benefit U.S. interests in the long run.

Because of the complexity and profundity of the U.S.-China relationship, and of these issues in particular, and because of the inability of any expert to accurately predict the future of potential outcomes, comparing these sorts of proposals is especially difficult. Proposals should not be compared on a one-to-one basis, but rather taken together to formulate a more nuanced and broader view of how particular actions might play out, and to gain a better understanding of the many factors affecting these issues and the relationship between the two nations as a whole. The result of this sort of amalgamation of differing opinions can be reflected in patterns of effective and ineffective policies. Through this research more developed and general policy stances can be derived and analyzed.

## Broader Patterns

The idea of several understandings of the future and possible solutions of these issues stems from the finding of patterns in the literature. These patterns occur when some authors tend to agree, in theme as well as in substance, on policy stances and their outcomes and benefits for the United States. Patterns do not necessarily fall along political lines, although it is possible that they are influenced by politics. Rather, these patterns are the result of authors taking similar stances and advocating for similar solutions. That is to say, proposed policy responses may differ in their substantive and practical application, but they often tend to take the same views; many authors advocate direct, aggressive response to issues by the U.S., while others favor engagement and cooperation between the countries as a measured response. In other cases, patterns emerge among proposals which favor long-term goals over the short-term, and vice versa. The comparison of these patterns, rather than individual cases, will help to develop the aggregate understanding of the issues and their possible responses while being more useful in identifying common characteristics of the individual proposals. The sum of these patterns is a more egalitarian and balanced view of the United States' prospects as it deals with the emerging Chinese cyber threat. These patterns may reflect broader schools of foreign policy ideals, or may represent various political motives which affect multiple experts and policymakers. In each case, attention can be paid to the background and views of the author to help understand the causes of patterns and their implications for these issues and the U.S.-China relationship, and the reason for the formation of certain patterns.

## The Political Spectrum

Varying the political ideology of the authors is a fairly simple and straightforward means of diversifying policy proposals and understanding potential patterns. Ensuring that there is an adequate amount of both progressive and conservative policy experts sampled in the thesis will create a variety of policy responses to cybersecurity, as well as demonstrate the breadth of possible goals the US can pursue with regards to its relationship to China. The two conflicting ideologies also offer differing views on what is in the best interest of the United States, or rather, whose interest should the US promote in its interactions with China, and in this case in its attempts to alleviate cybersecurity concerns.

Leftist policymakers tend to favor attempting to protect workers and consumers from the negative effects of cyber attacks. This aim is embodied in President Obama's cybersecurity Executive Order, in which he prompted businesses to share cybersecurity concerns with the government but not user data, an incursion of privacy which threatens consumers. This attention to consumer protection has admittedly not always been a hallmark of the Obama administration, but those occasions in which consumer protection and privacy rights have not been prioritized have been considered more conservative actions of the administration; in general attention to consumer rights such as privacy have been attributed to progressives.

Conservative policies, on the other hand, tend to prioritize businesses. CISPA, though having bipartisan sponsorship, is generally considered to be a more conservative bill, and affords protections to businesses to share data with the government, at the expense of their clients. This policy would have granted greater protection from cyber attacks to US businesses while also providing legal protection should they choose to share sensitive data with the federal government.

Surveying a wide political spectrum allows the thesis to consider the issue from several points of view, and how the national interest in this case may comprise varying aims from a variety of domestic interest groups. The political ideologies of the policy experts analyzed in this thesis cannot simply be divided into progressive and conservative; the think tanks and institutions from which these papers are drawn fall under varying degrees of leftist and rightist, as well as include bipartisan analyses and third party, such as libertarian, policy proposals, which share some similarities with the two main political parties but emphasize an entirely different set of values and interests. There are, however, limitations in using the political ideology of a policy in its analysis, and policies should be analyzed on the basis of various qualities not limited to ideological.

Analyzing the political ideology of a policy allows for a discussion and better judgment of what is politically viable, and whether the political viability of a particular policy might contribute to its overall strength or weakness. Political viability is based not just one the current spectrum of representation and political ideology in Congress, but also on attention to interest groups and political pressures from the main interests affected by a particular policy. Attention can therefore be given to a policy's treatment of the telecommunications industry, on internet companies, on consumers, and on the defense industry.

This is not to say that the relative conservative or progressive ideology of the policy and its author is not important in measuring the viability of a policy, however. Extreme policies on either side are generally more unlikely to curry enough favor to be passed into law. At the same time, policies considered to be moderate may face enough opposition from particular political groups to decrease their likelihood of becoming law. Thus, political ideology is a more secondary means of distinguishing and analyzing policy, but is useful in developing a varied portfolio of policies from which to compare. The best way to analyze policies from a political viability standpoint is therefore to take into consideration on a case-by-case basis the political factors involved in the effects and execution of a policy, while accepting that there are more important factors in actually judging the policies.

## Hardline and Softline

The policy proposals chosen for analysis also exhibit varying views with regards to US foreign policy in general, and relations with China in particular. The debate of so-called panda-huggers and dragon-slayers does not fall squarely on party lines, and members of the same political ideology can differ in their understanding of how China is best handled, and whether the US should adopt hard-line or soft line policies. In addition to this debate is the growing trend in isolationism, which is evidenced in some policies seeking for the United States to distance itself from China, both in conflict and in cooperation, entirely. Although the viability of isolation in a globalized world is suspect, it is important to analyze that perspective as well to understand how the United States might at least extricate itself to some extent from complicated conflicts with China. In general, while political ideology helps to demonstrate whose interests and what goals are favored when attempting to solve the cybersecurity issue, the foreign policy preferences of the author help to demonstrate the means by which that author prefers the issue be tackled.

The soft-line policymakers favor cooperation with China and exhibit these characteristics in their policy recommendations: they are unlikely to support retaliatory cyber attacks and intrusions against Chinese targets by the US, and rather tend to advocate for cyber "disarmament" and diplomatic resolutions in which both countries agree not to engage in cyber hostilities. Such policy experts see cooperation with China as economically potent and a natural path to prosperity with both countries; the US can pursue its own interests, whatever they are in the eyes of the respective policy makers, by pursuing an amiable relationship with China. While some may favor bolstering the US cyber defense infrastructure, soft line policy proponents in general are opposed to more offensive measures, and diplomatic measures feature prominently among this group.

Hardliners, in contrast, are as their name implies much more combative. These policy experts see the conflict with China as a win-lose situation, where the US must triumph over China in order to solve the issue. Diplomacy is a possibility with hard-line advocates but generally involves making demands, threats, and coercion to demand concessions, rather than attempting to find a cooperative solution to the cybersecurity concerns. More likely than diplomacy is for the US to make more aggressive cyber overtures of its own, and to take steps to bolster its cyber defenses beyond even what soft line policymakers might support. However, hard-line policies also utilize conflict by other means to deter Chinese cyber aggression, whether through economic sanctions and protections, or through more military or security means.

By analyzing policies from both groups, as well as more balanced ones and policies which ignore these particular goals altogether, a variety of methods by which cybersecurity concerns can be alleviated can be compared for viability, possible additional effects, and ultimately the value of the solution which the policies claim to ideally provide. However, the foreign policy views of the policymaker must be analyzed alongside that expert’s political ideology to demonstrate and analyze exactly what interest or goal the expert is pursuing, rather than simply noting the methods and policy choices for comparison. This thesis can therefore also show that, depending on the goals and interests sought, differing degrees of hard-line and soft-line policies can be utilized to advance those goals.

Drawing conclusions such as these involves use of the “analytical narrative” method of approaching data analysis (Bates et. al.). This method involves, in the authors’ terms, developing “systemic explanations based on case studies” by developing a “significant understanding of the phenomenon” (Bates et. al.), in this case the issue of cybersecurity policy. This approach is derived from “commonalities… used by a number of scholars” (Bates et. al.) and is particularly helpful to elucidate the issue of cybersecurity by examining these particular instances of policy proposals.

## Evaluating Proposals

These proposals were chosen in several categories, so as to provide a broad framework in which to investigate the issue. The analysis and evaluation of the policies must also be broad-based and varied. What that means is that policies should be analyzed on a case-by-case basis, with each policy proposal judged first on its own merits. The first measure of a proposal’s worthiness, in any case, must be the degree to which it could actually alleviate cybersecurity concerns. To what extent would each policy actually prevent or inhibit the cybersecurity threat presented by China? Does it try to address the original causes of cybersecurity issues or does it attempt to prevent the damaging effects? This specification is the best way to compare policies on face value, as it uses the primary goal of these policies as a standard by which they can each be measured. However, there are other considerations which must be made which determine a policy’s efficacy beyond simply a measurement of reducing cybersecurity threats.

In addition to observing how cybersecurity concerns are ultimately addressed by a policy, it is helpful to evaluate the policy with an eye to additional effects, especially with respect to whose interests are best served by a particular policy. These effects can fall into economic, military, and diplomatic categories, in addition to less observable social, societal, and cultural effects. The economic effects of a cybersecurity policy, aside from its direct alleviation of cyber threats, will in many cases favor certain groups or aspects of society over others. Diplomatic and military effects are more straightforward, but are vital to include in an evaluation of the policy in order to demonstrate its more long-term, far-reaching consequences a policy might hold for the US.

Economic side effects of policies are evidenced in their attention to private firms and consumers whose data and intellectual property are threatened by cyber attacks. Policies may ameliorate the threat firms face with user data by enabling them to more freely share that data with the government and with each other, or they may extend governmental cyber protection to those firms. On the other hand, firms may face increased costs if a policy forces them to take greater care to protect consumer data, or which imposes stricter standards of cyber protection on businesses. Economic effects of policies can also be demonstrate in their direct costs to the government; for policies which involve improvements to key infrastructure and cybersecurity standards, a certain cost is paid by the government to enact these improvements.

Diplomatic effects are felt more indirectly, they are reflected in the US' changing relationship with China and other nations, and its overall standing on the world stage. More aggressive and hardline policies will likely have a more negative effect on US-China relations. This can of course have rippling economic effects, possibly resulting from decreased trade or increased protectionism which limits free trade, as well as military effects, resulting from the need for heightened security following soured relations. Policies which, on the other hand, improve diplomatic relations with China, either through cooperation or through concessions, will have the opposite effect, improving security by improving relations, and allowing for freer trade and decreased barriers. Thus it may be important to note how policies strike a balance between mitigating the cyber threat while maintaining a good relationship with China, except in cases where the author makes a reasoned case for why the relationship with China can be neglected in favor of punishing cyber attacks.

Finally, military and defensive repercussions are a central aspect of a policy's overall quality. Cybersecurity lends itself to the US's overall defense and national security, and so a policy must necessarily, in the process of mitigating cyber attacks, improve the US national defense structure and intelligence institutions. Policies that force the US toward a more militaristic standing, with regards to China or otherwise, might be considered more dangerous towards national security. A policy which inhibits a cyber threat but creates a different kind of danger is less impactful or viable a solution than one which maintains US national security holistically. Therefore, a policy which maintains a peaceful solution can be considered more practical, insofar as that policy actually solves the issue of cybersecurity.

In addition to attempting to qualify all of the effects of cybersecurity policy, judging a policy's potential efficacy requires looking at the potential that proposal has of actually becoming law. As mentioned earlier, a policy's political leaning is an integral part of that policy's analysis. It is also an important measure of the likelihood of that proposal becoming law, given prevailing political conditions and pressures. Policies which go too far towards antagonizing certain groups, whether powerful business interests or consumer advocacy groups, are less likely to be passed, as are those which are against the political ideology of either major political party. Policies considered to be extremely progressive in nature will be unlikely to pass the House of Representatives, and those which are extremely conservative will have a difficult time in the Senate, let alone surviving Presidential veto. Thus, political viability of policies helps to demonstrate their value; a policy which could never actually be implemented or become law is not useful for practical purposes.

## Works Cited

Bates, Robert H., Avner Greif, Margaret Levi, Jean-Laurent Rosenthal, and Barry R. Weingast. "The Analytic Narrative Project." *Digital Access to Scholarship at Harvard*. American Political Science Review, Sept. 2000. Web.

"Case Study Evaluations." *United States Government Accountability Office*. United States General Accounting Office: Program Evaluation and Accounting Division, Nov. 1990. Web.

Ragin, Charles C. "Using Qualitative Methods to Study Commonalities." *Constructing Social Research: The Unity and Diversity of Method*. Thousand Oaks, CA: Pine Forge, 1994. N. pag. Print.

## Chapter 4: Analyzing Policy Proposals

### Introduction to Analysis

This chapter will focus on the analysis of each policy proposal, both on an individual basis as well as in comparison with each other. As discussed in chapter two an important means of understanding these policies is in the context of the greater discussion in the US on dealing with a rising China. Additionally, given the relevantly recent prominence of cybersecurity as a national policy issue, the way that these policy proposals understand and treat the issue of cybersecurity beyond the specific objective of preventing Chinese intrusions is also analyzed. And attention is paid as well to how politically viable a policy is, given its ideology and the stakeholders involved.

Analysis of the contents of the policy itself, the actual methods by which the policy seeks to curb Chinese cybersecurity intrusions, focuses on the effects of the policy. This includes first and foremost how the policy seeks to reduce cyber attacks or bolster cyber defenses, and to what extent that policy can be considered effective at accomplishing those goals. Secondary effects, discussed more deeply in Chapter 3, include political, military, and economic results of the policy. Policies which do not hinder US diplomatic interests, defense goals beyond cybersecurity, or economic progress are favorable to those that do. When applicable, other effects are also noted, specifically those which involve social, cultural, and societal issues, both in the United States as well as in China and other countries.

Many experts do not account for US involvement in cyber attacks and culpability in this and other issues related to spying and industrial espionage, particularly considering extremely recent and ongoing revelations, at the time of writing, of US spying abroad, both in China as well as in other countries. These allegations do hinder the US' ability to effectively enforce policies which attempt to prevent cyber attacks, and the extent to which policies address this issue will be counted in their favor.

The following proposals are ordered according to political ideology. The ideology of their respective authors or publishing organization directly informs the proposals themselves, and this order serves as a means of creating a more coherent spectrum, and allows for comparison between policies, demonstrating similarities and differences. Additionally, analysis of the potential viability of these proposals is contingent upon their political influences, as well as the political makeup of the current Congress and the particular ideology of the Obama administration.

### General Keith Alexander at the American Enterprise Institute

General Alexander, director of the National Security Agency, offered a comprehensive analysis of the state of cybersecurity and a range of possible policy responses. Alexander's prescriptions derive from a knowledge of the issue that is both deep and broad. His primary goals are defense-based, he wants to demonstrate clearly the extent and potential damage of cyber attacks and exactly how the US can expand upon its own capabilities to prevent them. Alexander's prescriptions address the issues of intellectual property theft as well as direct attacks, and to his credit he promotes a Clintonian diplomatic response to China's rise in cybersecurity prominence.

One of the most notable assertions made by General Alexander is that the cyber attacks perpetrated against US companies represent "the greatest transfer of wealth in history." He cites numbers over $300 billion that represent companies' losses due to IP theft brought on by cyber attacks. Alexander notes that internet usage in the United States is extremely high, and therefore so is the threat potential of cyber attacks.

This sort of fearmongering may be justified, but lends itself to Alexander's total focus on security above all else. The general's spotlighting of defensive and corporate issues related to cybersecurity beget solutions based on US defensive and corporate infrastructure. It is worth noting that AEI, at which General Alexander is speaking, is a conservative think tank known for attention and promotion of these issues. General Alexander's solutions proposed at AEI reflect this ideology, though he does invoke some less conservative proposals for collaboration with China.

The proposals themselves cover a wide range of cybersecurity-related issues, including those based on intellectual property theft, direct cyber attacks, and growing possibility of conflict between the United States and China over this potentially definitive issue. General Alexander explains that to protect against intellectual property theft, companies need to be made more compliant with US defensive standards as well as brought into collaboration with defensive agencies, in particular the NSA. He explains briefly a warning system by which private companies can alert the government in the event of attack and work with the NSA and other agencies to mitigate the effects as well as to implement preventative measures.

Alexander also warns about the potential devastation of direct attacks, against basic infrastructure, against private networks, and gives examples in Eastern Europe wherein such attacks have already wreaked havoc. To prevent against this he proposes increases to the power and scope of the NSA and other organizations, implemented through legislation. In particular, he promotes increased funding to improve the quality and quantity of cyber intelligence experts, internal improvements to defensive networks including “backtracking,” amongst other hacking-preventive measures. As the current head of the NSA he is clearly interested in seeing that organization increase in its power and capability to respond to threats as well as expanding its reach in accordance with previous recommendations, collaborating with private companies, especially telecommunications giants, to protect US infrastructure.

General Alexander does support a more diplomatic approach to the issue, tempered with his more direct and practical recommendations for improving the US’s own cyber capabilities. In particular, he cited then-Secretary of State Clinton’s insistence that China and the US reach a clear definition of the limits of cybersecurity and the terms of acting in the cyber sphere, of standards in a new cyber age. This sort of treaty would represent a more collaborative effort with the US’s new rival to reduce the threat of cyber attacks and IP theft. However, given the emphasis on more defensive-based solutions it is clear General Alexander does not believe that a diplomatic solution can be effective in and of itself.

The proposals Alexander puts forward would take the form of legislation and a treaty. The former would have to pass through both houses of Congress and survive Presidential veto, and the latter would be ratified by the Senate, as long as the President would agree to sign it. In terms of political viability, these proposals present some issues. Increasing spending is difficult at best, even for defense spending. And increasing the NSA’s capabilities and adding a burden on private industries would dissuade both privacy advocates and internet companies alike, both increasingly powerful lobbies. And ratifying a treaty of this magnitude with China would elicit some hesitation in Senators, given a negative public perception of the Middle Kingdom. The Trans Pacific Partnership treaty currently being developed is also unpopular, both at home and with China, making this sort of collaboration with China difficult even without gaining ratification at home.

These proposals would definitely improve US cyber capabilities; General Alexander is the one person best positioned to understand how to do so. The defensive infrastructure and private companies' protections would both be improved. But General Alexander dismisses privacy protections, which would be weakened in the process, and it is likely that China would similarly ramp up its own cyber efforts even in the face of the sort of treaty Alexander presents, just as he proposes the US do. So what would result would be more akin to a cyber "arms race," but with the addition of a treaty that would be, for all practical purposes, mostly meaningless.

Although increasing collaboration between companies and the NSA may be innocuous in the long-run, in the short term it will seem untenable to privacy advocates wary of the NSA's ever-expanding reach. And internet companies already put-upon by existing NSA requirements will balk at additional regulations. Politically, increasing cyber defenses in this manner, especially while calling for increased cooperation rather than conflict with China, would be difficult, and would have negative consequences for supporting politicians, if many can be found. And diplomatically, proposing cooperation with China while also bolstering cyber capabilities would look disingenuous at best, and only provoke negative reaction from the US's rivals.

**Center for Strategic and International Studies**

The Center for Strategic and International Studies identifies itself a bipartisan think tank, with a very wonky and in-depth approach to policy ideas. In 2008, CSIS published what could be a "comprehensive cybersecurity plan," developed by two Congressmen, a retired Air Force lieutenant-general, and another expert. The CSIS plan, while dated, was designed to be useful to the incoming 44th President to deal with cyber threats, mentioning specifically rival states and "advanced terrorists."

The recommendations presented in the report are comprehensive and detailed, and despite the fact that they are a few years old they are very useful for guiding future policy making. The CSIS plan recommends Presidential leadership of an inter-agency collaboration to improve cybersecurity. These improvements, according to the commission, would include partnering with private companies to regulate cyberspace, with regulations not reliant on "prescriptive mandates… and overreliance on market forces." The commission also recommends buying secure infrastructure, modernizing laws regarding cybersecurity, and improving research and training to build on existing capabilities. The report goes into much more detail about these recommendations, but for the sake of brevity analysis can focus on the big picture.

One of the biggest perceived strengths of the CSIS commission's proposals are their attention to what the writers call DIME – "diplomatic, intelligence, military, and economic…the elements needed for a truly comprehensive solution." While most proposals focus only on improving cyber capabilities the CSIS commission notes that all of these effects are important. And with an eye on protecting privacy and civil liberties, the CSIS planners work to ensure political viability as well as ensure the improved cybersecurity directive will not infringe on these basic rights.

Politically, the CSIS commission's proposals are fairly simple to execute, since most of them are the purview of the executive branch. Partnership with the private sector, as evidenced by previously analyzed proposals, is popular in Congress, and as long as it respects privacy rights it will face little opposition. The risk in Congress is that this plan strengthens the executive branch unilaterally, and Congressional opposition to the current President is strong enough to prevent that sort of strengthening. The proposal mentions threats from advanced terrorists and rival states, but is not specific. However, failing to specifically include other countries or working with foreign governments might provoke negative diplomatic consequences. Despite the fact that diplomatic represents one of the focal points of this commission, it does not specifically address these concerns.

The CSIS commission focuses on military and security strengthening, and its proposals would definitely do so. Controlling identities, modernizing security laws, training agents and acquiring cyber infrastructure are all means by which the government can improve its cyber capabilities, but there is little mention of the economic and diplomatic consequences of these actions, not to mention the political problems that arise from such sweeping government action. The commission does claim that privacy and civil liberties need be respected, but amidst all these reforms it does not specifically elaborate any means of doing so – in fact, the one time privacy is mentioned, it is in the context of controlling online identities, a distinct invasion of same.

The principle flaws of this proposal are not in its age, but instead in the fact that it does not address all of the issues that it purports to, and instead only serves to advance a security-based agenda to the exclusion of these other issues, and is weak for it. The privacy protections promulgated by CAP could be used in tandem with most of the CSIS proposals, but the idea of managing online identities is completely detrimental to privacy concerns, and taking over of cyber infrastructure is distinctly dangerous to both privacy advocates and foreign governments eyeing NSA overreach.

**Woodrow Wilson International Center for Scholars**

The Woodrow Wilson International Center for Scholars is a think tank and additionally part of the Smithsonian Institution; it is in a unique position for a think tank, being government run and funded. The Wilson Center convened an expert panel in 2010 to discuss the issue of cybersecurity, and specifically how the executive and legislative branches can act to respond to rising cybersecurity issues.

The experts include Sachs, a former Bush advisor turned Verizon employee, who worries mostly about cyber theft and intellectual property issues that arise from cyber attacks. Sachs mostly warns about the dire consequences of cyber attacks, including carbon copy factories built in Asia using stolen copies of US blueprints, and notes that Congress and the Executive branch have to show “leadership” on the issue, though is unclear what that might be.

Lending a little clarity to Sachs’ statements is Parkinson, a current Senate staffer with the Senate Homeland Security and Government Affairs Committee. Parkinson notes that more resources are being devoted to cyber issues in the Senate, and scores of staffers are now present at meetings on cyber issues. Parkinson notes that Senator Harry Reid is interested in taking the lead on this issue, and that “taking the lead” in this instance means organizing committees so that a unified approach to cybersecurity be developed and put forward. Parkinson recommends that the executive branch collaborate with and be more transparent to legislators on this issue. She also presents two parallel recommendations, that the government impose regulations to tighter security standards in the private sector, but also partner with it, as well as with state and foreign governments, to better cyber capabilities.

Lt. Col. Hare, the third expert on the panel, warns of an increasingly interconnected world, where even “a child’s laptop in China” is remotely connected to critical infrastructure, in some way. Hare notes that different agencies of the US government have varying goals and understandings of different aspects of cyberspace, and that to strengthen its ability to defend itself the government must resolve those understandings into a unified front. He speaks specifically about the military, and its role in presenting a primary function for government in cyberspace, from which other agency actions and goals can be developed.

Finally, journalist Nakashima warns about privacy issues that result when the government is involved to the extent the other experts, including Hare, recommend. Specifically she remembers a Bush directive that noted how uncertain the threats were and how it was vital to maintain secrecy of government activities in this area. She noted that cybersecurity issues are increasingly the purview of the military, and even private companies are beginning to seek defensive protection from the US government. The military must more clearly define its role in cybersecurity, and, correlative to Hare’s suggestions must impose that role and direction on intelligence and other agencies of the federal government.

Much of the panel’s time seemed to be devoted to a sort of fearmongering, establishing through examples and anecdotes just how terrifying cyber attacks could be. The upshot of this fearmongering is that many of the policies supported by these experts are designed to strengthen military involvement in cyberspace and extend the reach of the federal government. This demonstrates how the sort of strengthening and increasing cyber involvement of the government is fairly unpopular, because to gain popularity with Congress and the public these programs need to be demonstrably necessary. But in and of themselves, increasing militarization of cyber policies are politically unlikely, and diplomatically toxic. Only briefly does one expert mention working with foreign governments, and then in the same vein as the federal government working with states in the US; not on equal footing, but as a leader prescribing protections to subordinates. The Wilson Center's panel focuses entirely on the federal government and its roles, with private groups and foreign governments being secondary concerns; this is a major flaw for this policy.

The main strengths of the panel's recommendations are in their attention to cohesiveness within the federal government. Aligning goals between agencies and improving on inter-department collaboration are important means of strengthening cyber capabilities without over extending the government into cyberspace or imposing greater additional costs. On the contrary, creating a more direct, consistent, and cohesive cyber standard throughout the executive branch is an excellent way to make cybersecurity more efficient and stronger overall. Involving the legislative branch would allow important oversight to be possible as well as ensuring that the cyber issue is continuously developing and moving forward through legislative review and action. As long as these recommendations are pursued in such a way that more constructively and substantially involve foreign governments and private collaboration, this sort of strengthening can be very helpful to improving cybersecurity and addressing related issues.

**American Foreign Policy Council**

The American Foreign Policy Council is another conservative, DC-based think tank, although as the name implies it focuses on foreign policy concerns. For the Fall 2012 issue of its *The International Economy* publication, the AFPC surveyed several experts and stakeholders in the field on their analyses of cybersecurity and recommendations to the US government. Among the more interesting examples of these experts include Jim Harper, of the libertarian CATO

Institute, Patrick Cronin of the Center for a New American Security, and Ajay Banga, CEO of Mastercard Worldwide. These three experts were picked for their differing and relatively unique positions, ideologies, and recommendations regarding the issue of cybersecurity.

Jim Harper, from the CATO Institute, is focused primarily on curtailing government overreach in this area. Harper's main point is to demonstrate, through various potential cyber attacks, that bolstering and expanding cybersecurity capabilities is realistically pointless. He notes that smaller states would not bother attacking the US through cyber means, because of the potential for a disproportionate response, and the low possibility of causing the US any lasting damage. Additionally, he notes that the US's rivals and non-state actors who target the US do not have the capability for this sort of attack. "Cyberwar is something we're doing to them. It's not the other way around." Harper's ultimate prescription, then, is to leave cybersecurity alone; he closes by noting that there is no need for a physical standing army, and so a digital one would be pointless as well. If anything, Harper's comments speak to decreasing cyber capabilities, based on his own understanding of the issue.

Patrick Cronin, of the Center for a New American Security, forms a completely opposing opinion, noting that cyber security has altered the understanding of national security, changing how security as a whole must be approached. Cronin notes that, with cyber being a new front for war, and China becoming a global leader in this arena, the US's national security is increasingly at risk. Chinese telecom companies, he points out, are infiltrating many areas of cyber infrastructure, and have been accused of spying by the House of Representatives. Cronin, contrary to Harper, suggests that there are a myriad of ways China, smaller states, and even non-state actors could harm the United States through cyber attacks. In response, Cronin does not support improving US Cyber Command or other cybersecurity infrastructure. Instead, he asserts that cyber attacks are more likely to be prevented by diplomacy and physical military systems, and so it is these means that he would argue for improving, not US cyber capabilities.

Ajay Banga, CEO of Mastercard Worldwide, concerns himself with the availability and vulnerability of private citizens' and companies' data to cyber attack. He notes "the global economy is coded in ones and zeroes," meaning that the entire world economy is tied to cyberspace and information systems. He notes a monthly increase in the number and scope of cyber attacks, and puts the cost of this type of cyber crime, that on the personal and private rather than on governments, at $114 billion. According to Banga, since global corporations such as his own are the primary targets for attackers, they also serve as the "first line of defense" against them. Banga, then, supports collaboration between companies and the government, in the form of policies which promote that. In particular, he supports technical support by the government to these embattled companies as well as cooperation with foreign governments in capturing and arresting cyber criminals. Banga notes that the government nor private companies can alone manage this threat, and that "inflexible mandates and unilateral programs" are ineffective against evolving capabilities. Unlike either Harper or Cronin, Banga insists that cybersecurity is a critical part of national security, and should itself be bolstered through these means, rather than relying on traditional military and diplomatic apparati alone to solve a new and unique problem.

In terms of directly changing the cybersecurity landscape, each of these proposals would have vastly differing effects. Harper claims that no country that could muster the capability for cyber attack would want to draw the ire of the US and no non-state actor could be sufficiently deterred to make improved cyber standards worth the cost. However, this analysis ignores the basic truths of cybersecurity, the increasing attacks emanating from China and from nonstate actors, both against the US government and more numerously against private corporations. By at best ignoring the issue and at worst decreasing the US's own capabilities, Harper's proposals would most likely be detrimental to cybersecurity in the long run, and therefore to national security and military strength. It would be diplomatically negligible due to being entirely US-centric, at worst making the country look weak globally.

Cronin's insistence on focusing on diplomacy and traditional military to deter cyber attack also ignores the more specialized problems posed by cyber attacks. In particular, despite the US having a far higher military capability than any other single state, including China, there are still cyber incursions occurring against the US federal government and against corporations, continuously increasing, as Banga says, in severity and number. Using diplomatic overtures to deter attacks has its merits, but Cronin is not specific as to how this sort of solution might be brought about. If it were to be similar to Alexander's Clinton-quotation, a sort of treaty outlining the terms of cyber space and cyber security, then as a solution it could be useful, in the case of China. But his invoking of military presence in the Pacific as a means of enforcing this sort of diplomatic solution is hawkish, and its ability to have significant effect on decreasing cyber attacks is unproven, and uncertain. This sort of focus on traditional military would be detrimental to cybersecurity-specific threats, and would be diplomatically dangerous as increasing the US military presence in Asia will entangle the country in conflicts there.

Banga has, among these AFPC-published experts, the most specific and direct attempt to address the issue. As a CEO of a global corporation Banga has the most experience dealing directly with the problems and damages caused by cyber attacks, and so is most aware of the necessity of addressing this issue and the potential requirements for doing so. Banga's recommendations for collaboration between government and private industry, and a focus on cracking down on cyber criminals, would most directly contribute to raising cybersecurity standards and protecting against future attacks. But this sort of collaboration, in the wake of the NSA revelations, is politically toxic. Additionally, numerous Internet companies have complained about government overreach in this area, so trying to involve such companies in this sort of collaboration could be difficult without imposing politically unwelcome requirements. Involving other developed countries in this solution, and expanding cooperation between disparate companies and governments could be diplomatically beneficial. This solution focuses on the threats posed to private companies by cyber attacks, and does not address military or government needs, except as they coincide with those of private companies. For example, increasing collaboration and the government's reach in cyberspace would most likely improve the military's ability to protect cyber infrastructure and telecommunications.

In terms of viability, for these policies the most beneficial to actual cybersecurity capabilities is also the least viable. Banga's proposals would be difficult to pass through Congress, given opposition of civil liberties groups to government intrusion into cyber data, opposition of Internet and telecom companies to stricter requirements and regulations, and the simple fact that increasing capabilities in this way would be more costly. Both pro-consumer and pro-business groups might find it difficult to stomach increased requirements and intrusions, unless they are structured in such a way as to be optional for companies, and protective of user data. But Banga does not explicitly address these concerns.

Cronin's focus on military and diplomatic solutions, rather than specific cyber ones, are more viable than what Banga suggests, but they also present some issues. After two unpopular wars there is little support for entangling the US in any additional conflicts, which would easily be possible given an increased military influence and presence in Asia, as tensions simmer there. Additionally given prevailing anti-China and isolationist sentiments, engaging in diplomatic, broad-based solutions to this issue would also be politically difficult. Already opposition is forming to the Trans Pacific Partnership, and that agreement is with countries with which the US has generally genial relations.

Harper's proposals are the easiest to follow through with, because of course he advocates doing nothing to expand cyber capabilities. Even if the US tried to reduce spending in this area, there may not be much opposition; the NSA and its surveillance programs are increasingly unpopular, so if decreasing cybersecurity were seen as the government divesting itself from this sort of program, then such legislation might find support. But there is also the fact that a majority of Americans view Edward Snowden's revelations negatively; this majority believes these NSA programs as at least important to US security, and so decreasing them rather than doing nothing would present its own set of challenges in Congress.

What the AFPC's published analyses show is that the most significant and directly contributory solutions, in these cases, are also the most difficult to enact in actuality. They also show that the issue is viewed in a different light by experts of various ideologies, who present different responses as a result. But those most directly connected to the issue, in this case Ajay Banga, understand that the threats presented by cyber attacks merit a real focus and a proportionate response. For him, that response is best led by the private industry and supported by the government. Other proposals may be more government-centric, but it is important to note that the most useful proposal in this case comes from someone directly connected to the issue who understands the specific implications and threats that cyber warfare poses.

## Brookings Institution

The Brookings Institution’s Ian Wallace provides another unique perspective on the issue. Wallace previously served at the British Ministry of Defense as a senior official, helping to develop UK cyber strategy. In his writings and analyses Wallace delves into the broader implications for the emerging cyber sphere of conflict – which he claims cannot be called a “war” – to understand how governments can and should act in this sphere.

Brookings is well-known as a left-leaning think tank, but Wallace’s ideas are not tied to a particular ideology. He contends that cyber is a “game-changer,” but the conflicts taking place in the cyber sphere do not constitute war. These conflicts are more related, he says, to subterfuge and espionage, and to crime, than to war. Modern wars are waged by coalitions, but each nation maintains its own cyber command center, and keeps cyber capabilities highly classified. So if cybersecurity is about espionage and crime, then how should nations act in this sphere? Wallace insists that despite cyber not being used for war itself, it has become a vital supplement to military strength, and so nations, in particular the US, which seek to advance in the cyber sphere must militarize, to some extent, their cyber capabilities. By that, he means nations need to centralize their cyber commands, and reconcile the need for subtlety in cyber espionage with the need for collaboration in actual war

In particular, Wallace insists on integrating cyber intelligence and technical capabilities with traditional military planning. He also calls on the “Five Eyes,” consisting of the US, UK, Australia, New Zealand, and Canada, to be more cooperative and open to each other in the cyber intelligence area. A goal of this cooperation that Wallace outlines is the “preservation of the global internet,” referring to cyber infrastructure upon which all of these nations are dependent.

Wallace’s solutions are flawed in their lack of clear, definitive goals. But as broader, more long-term ideals for the cyber sphere, and a means for framing the future of cyber discussion and policymaking, Wallace’s ideas are a useful basis. Collaboration has been promoted by many policymakers, for different government agencies, between the government and private sector, and between companies, but Wallace most clearly advocates for governments and militaries of different countries, in particular the Five Eyes, to collaborate. Sharing intelligence could lead to increased transparency, while also improving cyber capabilities and the reach of the US’s influence in the cyber sphere. Additionally, sharing responsibility for protecting cyber infrastructure would help to prevent attacks against that infrastructure while also taking some of the burden off of the US for being a sole protector of cyberspace. Assuming Wallace’s nebulous goals are met by more concrete policy, then cybersecurity standards and protections would certainly be bolstered in the US.

From a political standpoint it is difficult to predict the viability or potential effects of policies when they are not definitively outlined. But at the very least policies which seek to increase collaboration and reliance on other countries in the “Anglosphere” would be difficult to sell to Congress, with the aforementioned trends of isolationism and protectionism in the US, including in the Senate. But increasing transparency and cybersecurity simultaneously would be a more welcome and salient policy response, and would make for legislation more likely to be passed by Congress and signed by the President.

Diplomatically this policy would provide valuable allies in the escalating cyber conflict; tying the military capabilities of the US to those of the other four countries would pressure China to improve its behavior in the cybersphere without actively provoking its enmity. In this sense, then, a policy of international cooperation is most helpful to the US’s diplomatic status, and by taking action to establish a sort of "cyber alliance" the US can take the lead on this issue and influence the process of cybersecurity building. However, by only involving the Anglosphere nations as Wallace suggests, the US does contribute to an imperialistic image and negative influence in the global south. To improve upon this policy, the most basic steps Wallace could take would be to propose the US opening itself to cyber cooperation with nations outside of the so-called Anglosphere, to friendly countries and governments outside of Europe and the rest of the developed world.

**The Council on Foreign Relations**

The Council on Foreign Relations' *Foreign Affairs* publication includes many foreign policy recommendations, including one in 2009 written by Wesley Clark and Peter Levin. Clark was a US Army General, and Levin a professor and writer of many technical articles. Together they present a nuanced view of cybersecurity as both a military and a technically complex issue. CFR is a nonpartisan think tank, and the solutions presented by Levin and Clark do not reflect a specific ideology, but are instead completely security-oriented.  Levin and Clark recognize, as participants and experts in the field, the unique potential for damage that cyber attacks pose. And their solutions are equally nuanced, based primarily on viewing the issue of cybersecurity as similar to preventing the spread of disease; they take a "biological" approach to attempting to solve the issue.

The solutions presented by Levin and Clark are entirely driven by the US government; they do not invoke the private sector or foreign governments as do many of the other experts. The focus here is on the US defense system improving itself, and while the focus on strengthening from within is helpful to understanding what makes cybersecurity stronger, it is weaker in that it does not attempt to address the diplomatic and economic concerns related to cybersecurity, except as they arise from potential attacks.

Given their presentation of cyber attacks as biological diseases, the solutions Levin and Clark propose are also based on biology. They recommend utilizing additional resources to strengthen the US’s digital infrastructure, specifically by diversifying its component devices and systems. They decry the overreliance on a few operating systems and “basic hardware architectures” that makes the US more vulnerable to attack. An additional weakness that Levin and Clark seek to rectify is the unsecured nature of hardware manufacturing; most of the chips that comprise this architecture are, according to the authors, manufactured at unsecured facilities outside the US, making them targets for attackers. Clark and Levin recommend securing these manufacturing processes, not by having the government take over and manufacture these components itself, but through “elegant” means of tightening safeguards and authentication codes into the devices, ensuring that the security agencies have some control over the supply chain.

Much of the information regarding these processes is, as the authors point out, classified, but they recommend making digital security systems, to some extent, open source and collaborative. This is a useful means of promoting cybersecurity improvements in addition to transparency. But making security systems more intricate and controlling production processes is likely to be politically unpractical, given the unpopularity of these programs overall. Additionally, attempting to control supply chains in foreign countries would be diplomatically toxic, especially if not done openly. Clark and Levin’s proposals are strongest, however, in their attention to strengthening digital systems and infrastructure from within, and noting the greatest flaws in these systems that make them most susceptible to attack. Most of the experts surveyed recommend solutions that involve private sector and foreign collaboration, but do not fully involve internal solutions. But the weaknesses that Clark and Levin point out make US digital infrastructure vulnerable regardless of the amount of collaboration. And to improve military capabilities in this way would be extremely useful, especially if combined with additional proposals such as that of the Center for American Progress that invokes privacy rights and Brookings' recommended collaboration with other nations.

### The Center for American Progress

The Center for American Progress, as the name suggests, is a far more progressive organization than even the Brookings Institution. Peter Swire, a senior fellow at CAP, testified to a Senate Committee about potential legislation and other Congressional action conducive to advancing a cybersecurity agenda. However, Swire's priorities are not focused only on improving cyber defenses, but more clearly on improving privacy protections and ensuring proper oversight. And to that end, his proposals are specific and potentially effective.

Swire provides four main points, or proposals, to the Committee, all of which are Congressional actions which could begin in that committee. He recommends first that the Senate confirm nominees to the Privacy and Civil Liberties Oversight Board, so that entity would be fully staffed and capable of properly overseeing relevant organizations and limiting incursions of privacy rights by cybersecurity organizations. Secondly, he advises appointing a single privacy czar to centralize this oversight and coordinate with all relevant agencies to promote privacy protections. He specifically mentions "transborder concerns" which refer to diplomatic issues that emerge with cyber spying on other leaders.

Swire also recommends improvements to the E-Government Act of 2002 in line with his previous proposals, improving standards for privacy protections and bolstering transparency by allowing for privacy protection assessments to be published to the public, and for each agency to be effectively rated and burdened with acceptable standards of privacy. While the other proposals provide for a privacy agency infrastructure, this one most effectively applies stricter provisions to the cybersecurity agencies themselves. The same is true of his final proposal, for clear delineation between identifiable and deidentifiable data; meaning setting clear standards for agencies for data that is specifically identified to a certain user, and data that is not. These standards are helpful to ensuring proper privacy protections are implemented; Swire assures in his testimony that these protections have helped to prevent this sort of data from being traced back to users in the private sector, and could be effectively implemented by defense agencies as well.

In terms of strict cybersecurity improvements, these measures are not particularly helpful. But the true value of Swire’s proposals is in their ability to assure privacy protections without compromising cyber defense; all of these proposals could be carried out simultaneously with any of the aforementioned cybersecurity legislation and collaboration, and may even make that legislation more likely to pass through Congress. These proposals do constitute substantial inroads to protect privacy, as well as addressing lack of collaboration and oversight in the cybersecurity complex. Given that there are few costs imposed on the government, and constraints are reasonable and with the goal of protecting privacy, such legislation is politically viable, especially now given changes to the filibuster process that make confirming non-judicial nominees much easier in the Senate.

More practically, Swire’s suggestions are a way to provide positive diplomatic and political coverage for cybersecurity agencies and efforts in the US, by proving that the government is willing to take privacy and civil liberties concerns into consideration while advancing a new cybersecurity agenda. Opponents would be more willing to consider improving cybersecurity standards if they could be confident that privacy would be protected, and foreign governments would be more willing to collaborate knowing that these limitations would apply to their leaders as well, averting the significant crises that have plagued the US since Edward Snowden revealed the extent to which the NSA is involved in cyber snooping of foreign dignitaries.

It is vital to protect privacy while advancing cybersecurity standards, and Swire provides a way to accomplish the former without compromising the US’s ability to pursue the latter. These policies are a starting point, however, and will in no way completely satisfy the privacy advocates currently lobbying for more protection. But by being willing to provide for some oversight and define certain limitations, Congress can show itself willing to meet the demand for privacy protections, currently the main source of public opposition to cyber programs. The best way to improve political viability and stability for policies aimed at improving cyber standards and preventing cyber attacks is to address these concerns, and Swire’s proposals provide an excellent starting point.

While these policies may not in and of themselves contribute directly to improving cybersecurity, they make other direct advances to cyber defense and infrastructure more politically viable and less likely to have the negative consequences that arise from infringing on privacy rights.

### Patterns

The following part of this analysis will utilize the patterns in policies considered to be weak and strong, determining what makes those policies weak and strong respectively, from those patterns draw conclusions about this policy debate. Thus, the components that most contribute to making a policy strong or weak can be better elucidated. With these components in mind it can be easier to chart a course for future policymakers and leaders in the United States, as the cybersecurity issue continues to develop. Finally, analyzing the consequences of following through with strong policies can help to demonstrate how best the issue of cybersecurity might be resolved, or at least dealt with, and legislated on a global level. Cybersecurity in the future will likely continue to be a divisive issue, a new front for conflict, or it could reach a sort of resolution, a détente where the interests of China and the United States, as well as other countries, might be accounted for and to a certain extent protected.

### Weak Policies

The weaker policies surveyed in the prior chapter are those which underestimate the severity of the cybersecurity issue, or misrepresent the nature of cyber attacks. Harper of the CATO Institute, for example, describes the threat of cyber attacks as negligible, especially when considered against the threat of government overextension and infringement on individual rights as a response to cyber threat. Harper asserts that weaker states would not dare to attack the US directly, and nonstate actors lack the capability to do substantial damage. This assertion, however, flies in the face of common understanding, and directly contradicts the established knowledge upon which most other experts base their own recommendations.

Those that misrepresent the issue usually do so in such a way that underestimates the threat that is posed, or identify it as similar to if not an extension of traditional military threats. Neither, however, is true. Cronin, of the Center for a New American Security believes in the latter – that rather than focusing on cybersecurity specifically, the US government should invest in and maintain its traditional military strength, deterring potential rivals from considering cyber attacks. He insists that nonstate actors lack the capability to cause real cyber harm, to overcome the intricate US defensive system. Both have been shown to be untrue.

Other policies, while relatively strong, have weaknesses that limit their usefulness. Many of these weaknesses have to do with not collaborating enough with foreign governments or with private sector actors, or otherwise limiting improvements only to US security infrastructure and institutions. More successful policies are less narrow in scope, and call upon the advantages offered by engaging with allies as well as with telecom corporations in improving cyber security. In the latter case, the critical infrastructure managed by private corporations is left completely unaltered by policies which focus solely on the public sector.

The CSIS prescription unilaterally focuses on improving the powers of the executive branch to achieve this goal, and setting aside the issues of political viability inherent in this proposal it ignores the threats posed to privately owned cyber infrastructure and data, as well as puts the entire burden of addressing global cyber threats on the US government. Collaborating, demonstrated by those policymakers who do include means for advancing it, allows for broader reach of cyber defense and spreads the cost of cyber protections beyond the US defense budget alone.

Otherwise strong policies are flawed by ignoring additional effects beyond defense alone. Those which overextend US influence to infringe upon privacy rights or upon sovereignty of other nations have diplomatic and political consequences that are detrimental to the US, perhaps outweighing the benefit of improving cyber protections. Levin and Clark's comprehensive plan is an excellent strengthening of cyber capability, and could be strengthened only by including measures to contend with political and diplomatic implications of unilaterally improving US cyber defenses and offenses.

Finally, there are policies which could be made stronger by extending their scope. Collaborating with the "Five Eyes" of the Anglosphere is an excellent way to strengthen cyber defenses and effect a more global cybersecurity standard, but Wallace at Brookings could just as easily have included more friendly nations, or extend the invitation of collaboration to any government which would be willing to work together to improve cyber protections and prevent cyber attacks. Additionally, this relationship could be extended to private corporations, and those policies which already promote that could benefit by including foreign governments as Wallace attempts to.

Weaker policies, then, in general ignore the side effects of increasing security measures, are unilateral and narrow in scope, or otherwise fail to adequately address the cybersecurity issue and its many dimensions and detriments. Those policies which are incompatible with privacy protections, collaboration, or other diplomatic and transparent solutions are less useful for it.

## Strong Policies

More important to understanding the cybersecurity issue and how it might be addressed by the government are the stronger policies sampled. In most cases the stronger policies are simply those which succeed where weaker policies fail, and meet the specific and varied challenges posed by cyber threats. In contrast to the weak policies outlined earlier, these policies do account for privacy concerns and transparency, they enforce collaboration, and they are tailored to the unique problem they purport to solve.

One notable feature of these policies is that they are often designed and published by notable experts who work in the field, for example Banga writing at the AFPC is an executive at Mastercard and knows firsthand the danger private organizations face from cyber attacks. Clark and Levin are a former general and Department of Homeland Security staffer, respectively, and are experts on the more technical aspects of cybersecurity. While such a background is not required for the creation of strong policy, a more thorough and concrete grasp of the issue by the policymaker allows for a more well-rounded and complete policy.

Clark and Levin’s proposal reflects the strongest response to cyber attacks on a purely security-centric basis. They acknowledge that the threat of cyber attack cannot be mitigated by traditional defensive options, and must instead be treated with innovative solutions. In particular, they note the “biological” quality of cyber threats and assert that responses must be similar in nature, including diversifying infrastructure and securing the manufacturing process, among other actions. This represents the most comprehensive and direct plan of defense the federal government can take to respond to cyber threats.

While it does not account for the other aforementioned dimensions of the issue, its strength lies mostly in the direct and nuanced method by which it seeks to ameliorate these threats. And Clark and Levin leave room for improvement; there is no part of their policy that prevents additional privacy and transparency regulations and collaboration, international or otherwise. In short, this policy provides a means to strengthen in various ways US cyber defenses without compromising individual rights, decreasing transparency, or inhibiting the US's ability to work diplomatically with other countries.

Banga's proposal, which recommends strengthening the private sector's own defensive infrastructure, is strong due to his secure understanding of the scope of the potential threat. He notes first that much of the global economy is dependent on data supported by cyber infrastructure, which is operated primarily by private companies. So his suggestion that the private sector must be bolstered with government support and collaboration is well-founded. He decries government mandates and restrictions, insisting that instead the government must work with companies in the cyber sphere to create more nuanced engagement with the issue. This follows the same pattern as Clark and Levin's proposal; policies are strengthened by recognizing and accounting for the peculiarities of cyber security as opposed to traditional security. And Banga's suggestions are particularly useful for their demonstration of the need for and possibility of private-public partnership on this issue, coupled possibly with the government's own improvement as laid out by Clark and Levin.

Peter Swire's policy proposals represent another type of strong policy – one which deals specifically with the privacy issues that emerge from implementing cybersecurity plans. While Swire's policies do not directly combat cyber threats, they provide a specific framework for addressing privacy concerns without causing undue detriment to US cyber defenses. Therein lies the strength of his four points: while they provide specific means by which privacy can be better ensured, they do not inhibit, at least in theory, the ability of agencies involved in cybersecurity to complete their assigned tasks. Their flexibility and the relative ease of implementation, assuming legislative success, also make these proposals especially useful for cybersecurity policymakers.

Since political viability of policies requires homage to privacy protections, these relatively unobtrusive assurances can greatly improve more defense-oriented measures.

The most common quality of each of these relatively strong policies is that they each address a specific sphere of the cybersecurity issue, rather than introducing broad or sweeping changes. This speaks to the nuance of the issue and of the need for very specific and targeted policies to properly defend against cyber attacks. A number of policies that are implemented in tandem is a more fruitful and balanced way to approach the issue than to utilize one wide-reaching policy that lacks depth. Improving integration of various agencies and strengthening infrastructure constitutes one area, while expanding collaboration and public-private and international partnerships represents another. And policies such as Swire's, that address non-security issues related to cyber defenses, including privacy but also economic, political, and diplomatic dimensions, are also vital to improving overall cybersecurity effectiveness without compromising other important aspects of national policy and defense.

# Works Cited

Alexander, Keith. "Cybersecurity and American Power." Cybersecurity and American Power. American Enterprise Institute, Washington, DC. 9 July 2012. *AEI*. Web.

Clark, Wesley K., and Peter L. Levin. "Securing the Information Highway: How to Enhance the United States' Electronic Defenses." *Foreign Affairs*. The Council on Foreign Relations, Nov.-Dec. 2009. Web.

Harper, Jim, Patrick M. Cronin, and Ajay Banga. "The New Cold War?" *The International Economy*. American Foreign Policy Council, Fall 2012. Web.

Langevin, James R., Michael T. McCaul, Scott Charney, and Harry Raduege. *Securing Cyberspace for the 44th Presidency*. Rep. Center for Strategic and International Studies, Dec. 2008. Web.

Sachs, Marcus, Deborah Parkinson, Forrest Hare, and Ellen Nakashima. "Congress, the Executive Branch and the Cyber Threat | Wilson Center." Congress, the Executive Branch and the Cyber Threat. Woodrow Wilson International Center for Scholars, Washington, DC. 17 May 2010. *Wilson Center*. Web.

Swire, Peter. "State of Federal Privacy and Data Security Law: Lagging Behind the Times" *Center for American Progress*. Center for American Progress, 31 July 2012. Web.

Wallace, Ian. "Cyberwar: Leveraging Old Ties For New Threats." *The Interpreter*. Lowy Institute for International Policy, 24 Sept. 2013. Web.

## Chapter 5: Conclusions

### Conclusion and Implications for Policy

What conclusions can be drawn from an analysis of the cybersecurity policy debate? The more "security-focused" thinkers focus on bolstering US capabilities, defensive infrastructure, and other security measures. This group focuses on strengthening existing agencies and adding new ones to the US security apparatus, and in some cases, giving more power and responsibilities to corporations engaged in what these experts describe as a "war," and more specifically, and radically, the next Cold War. Therefore they do not believe in common ground with China, nor diplomatic solutions of any kind.

In contrast, those ideals are held by the more "softline" policymakers, those who tend to prefer attacking the root of the problem – the motivation for hackers both state-aligned and otherwise to engage in cyber attacks. Deterrence is key to these experts, as well as openness and often cooperation. These policies involve greater engagement, collaboration, and development rather than conflict. Of course, the softliners' ideas only work as long as China and other actors are willing to work with the US government. And, predictably, the softliners tend to ignore the US's role in cyber conflict, and proposals for agreements or treaties end up placing most of the blame and most of the pressure on China, which makes its cooperation on these policies unlikely.

The distinct policy choices seem to present a paradox for leaders in the United States. The country can increase its cyber defenses to meet the threat, but by doing so might only escalate it. And any attempt to mitigate the threat will force the US to lower its own protections in kind.  The interplay of economic problems, diplomatic issues, security, and social concerns makes devising a policy choice to combat cybersecurity particularly difficult. In particular, policies need to protect the interests of powerhouse US companies to preserve economic dominance, while also enabling government defense operators to function effectively. Policies need also balance the interests of the nation as a whole with those of individuals; concerns over privacy have become more widespread and more prominent, but the policies which actually address these concerns are difficult to implement alongside more security-minded ones. And when considering China as a primary cyber aggressor, policies must meet the threat without overtly antagonizing the US's rival; the countries share an interdependent economic relationship, as well as a contentious political one, that makes managing an issue that has both economic and political qualities difficult.

## What Needs to Happen

To address these rising threats, based on this analysis, the US government needs to improve cybersecurity standards in several areas: through direct improvements, public-private collaboration, diplomatic efforts, and through privacy protections and oversight. Until recently these areas have been addressed only minimally, and in some cases leaders have done no more than pay lip service to the idea of reform. If the mandate for comprehensive change is present, then there are preferable actions in each area that lawmakers can take.

As has already been stated, in terms of improving cyber infrastructure and taking more decisive action on defense, Clark and Levin's "biological" proposal is the most comprehensive, and potentially the most effective. By taking firmer control of the equipment manufacturing process for cyber infrastructure, US defense agencies can have more oversight of all potential entrances and attack points for potential threats. This and Clark and Levin's other proposals would help to ensure an improved standard of cybersecurity among federal agencies without taking an overtly aggressive stance or infringing on privacy rights.

The Obama administration's recently published Cybersecurity Framework is useful for its security guidelines and collaborative suggestions for companies, but it does not go far enough. The Framework encourages companies to meet those standards for security but it neither demands them nor incentivizes them. By requiring the companies that control much of American data, intellectual property, and cyber infrastructure the US can better ensure that these targets are protected by their respective stewards. Banga is right that the government should collaborate with and support companies in improving their cyber protections, but it should also require companies to meet heightened stances and share potentially vital information as necessary.

The US government is a combatant in a cyberwar with China, and has been revealed to have been spying on leaders and organizations in other countries as well. To attempt to ameliorate the threat while improving its global image the US should also consider cybersecurity treaties, for which leaders in both Washington and Beijing have called. While an agreement to end cyber espionage, or at least to mitigate it, might be difficult to hold either country to, it can at least demonstrate condemnation for cyber attacks and theft, and provide a more stringent framework in which cyber aggressors could be challenged.

In the midst of this reform, privacy cannot be ignored. Swire's excellent proposals for oversight bodies and privacy standards are possible starting points. The more transparent the cybersecurity measures can be, particularly those which utilize user data, the more viable the policies. And as long as the new standards and practices account for civil liberties concerns without unduly compromising their stated goals, they can be more permanent, stable government policies.

**Political Viability**

An important point of contention in this policy debate is the viability of the various policies. Although a policy being unviable does not preclude it from being a strong policy, it does prevent it from being seriously considered as being potentially put into place. For the purposes of analyzing what is likely to occur in the cybersecurity policy debate, and how the issue is likely to evolve over the next few years, it is better to focus on the analyzed policies which were found to be politically viable. Such policies are those more likely to pass through a highly divisive Congress, and those which the President would approve of and sign.

For unviable policies, it can be helpful to note what needs to change in the current discourse and in public opinion to make them possible, and how such change might occur. Significant cyber breaches or attacks in the near future might increase public awareness of the issue, and further devotion of resources towards mitigating it. But as long as revelations continue to pour out regarding the extent of NSA cyber spying measures, those advocating for reductions in cyber capacity will have a prominent soapbox on which to stand.

The greatest current obstacle facing stricter cybersecurity policies are these privacy concerns, and will remain so until these are addressed, or public opinion sufficiently swayed that these concerns are not so prominent an issue. However, at least in the near future, policies which are attempted to be made into law must account for privacy rights; those stricter policies which strengthen or lend further power without restraint to cybersecurity operators such as the National Security Agency are extremely unlikely to pass the legislature, and President Obama has publicly vowed to veto such legislation should it arrive at his desk, unless it sufficiently protects individual liberties. Beyond being a factor in a policy's viability, privacy protections are important in the overall strength of that policy; it is pointless to address one issue by creating another. For example, the recommendations of Peter Swire at the Center for American Progress are very useful in this respect, as they provide a reasonable means by which privacy and individual rights can be protected during escalating cyber conflict. If another, more security-focused policy can be used easily in conjunction with these recommendations, and without undermining their essential goals, then these policies taken together might represent a more viable policy option.

From a practical standpoint, the political viability of these proposals is useful for determining which are most likely to be actually implemented. Those policies which are better suited to the current political climate are much more likely to survive legislative procedure and avoid a presidential veto. Given the historically low rate of passage of bills through the current Congress, especially those which promise broad changes, only narrow and specifically-targeted bills are likely to progress, and avoid the ire of interest and advocacy groups. For this reason the stronger proposals as described earlier are also more viable to pass than weaker ones; the stronger proposals are themselves more specific, targeted, and less likely to raise objection as more sweeping changes advocated by General Alexander, to name one example. But they would face an uphill battle nonetheless.

Clark and Levin's proposal, with its specific improvements to cybersecurity infrastructure and oversight, exemplifies the type of update to cyber defenses that is most likely to pass through Congressional process. While it does strengthen cybersecurity and improve aspects of data collection and protection, it does so in a way that does not directly infringe on privacy rights by any definition, and does not provide additional mandate or regulations for businesses. These are the two main sources of opposition to increases to cyber policies in Congress and by avoiding them this proposal can provide a means for legislators to satisfy the pressures they feel to make headway into protecting against cyber attacks, in particular from China.

This proposal, or one like it, is more likely to become legislation without a privacy stipulation in Swires' style. Those pressures that lawmakers in general feel to respond to the escalation of cyber threats with updated cybersecurity standards provide the impetus for policies such as Clark and Levin's, which directly contribute to cyber defenses. But for privacy policies such as Swire's, even ones which do protect privacy without unduly compromising security, that motivation is almost non-existent, except in the case of the most progressive, civil-liberties-minded legislators. Privacy protections, even strong ones such as Swires', are therefore unlikely without concentrated efforts made to pressure more lawmakers to consider them.

For collaborative policies, such as Banga's or Wallace's, the possibility of action is dependent on actors outside Congress alone. Banga advocates for government support of private corporations against cyber threats, without extending regulations or standards to constrain them. This sort of policy is likely to be popular with large corporations and the legislators who support them, but to receive the sort of support necessary to drive action and surpass the legislative "pivot" points, it would require significant lobbying action and advocacy by the corporations themselves. Unilateral expansion of corporate power and government support for it would likely be unpopular among constituents, so legislators would need a more significant driving force to influence this sort of policy than, for example, Clark and Levin's. A significant cyber breach in the private sphere, or clear evidence of threat to US businesses beyond what has already been revealed, might provide that necessary pressure.

In the case of collaboration with other countries, the treaty or agreement required would necessitate presidential advocacy and Senate approval. Strong diplomatic overtures, especially nonmilitary ones, are likely to garner support, but once again a motivating factor is necessary to provide the impetus for the type of policy Wallace recommends. Both the "Five Eyes" of the Anglosphere, as well as US domestic leaders, must have significant reason and support at home to embark on a partnership; once again, the driving force is most likely to derive from a significant cyber attack or cyber threat beyond those that have already occurred.

An examination of political viability of these policies, then, shows that in many cases, acting on the issue of cybersecurity beyond simply directly expanding US governmental cyber defenses requires pressure from outside Congress itself. Without the necessity of decisive action, from domestic pressures or from an escalation in the cybersecurity issue, inaction is much more likely than action. This is true even of policies like Clark and Levin's that provide direct improvements to cyber defenses without undue additional effects; in Congress, and in particular in the historically inactive modern Congress, a lack of legislation is much more likely than any significant or meaningful reform.

## Implications for Future Reform

What does this likelihood mean for the future of the cybersecurity issue, for the United States, and for China? In the near term, only superficial improvements are likely, and in fact such potential policies have already begun to accumulate. In February 2013 the Obama administration implemented the executive order Improving Critical Infrastructure Cybersecurity ("Executive

Order – Improving Critical Infrastructure Cybersecurity") to advance such direct protections as have been demonstrated to be most politically viable  - those which only affect federal government infrastructure and minimize any toll taken on organizations or individuals.

This order is general, and merely instructs the relevant officials and institutions to begin moving towards taking stronger and more sufficient security measures. By its nature, this policy has only established the basis of a framework, loose guidelines for officials to follow that are "prioritized, flexible, repeatable, performance-based, and cost-effective" (Executive Order – Improving Critical Infrastructure Cybersecurity). The order also does include allowances for the protections of privacy rights, as well as advising increased collaboration with private sector organizations to develop that framework.

The culmination of that development was announced a year later, when the Obama administration's cybersecurity framework was launched February 12, 2014 ("Launch of the Cybersecurity Framework"). This framework lays the foundation for increased communication and collaboration between the private sector organizations which assisted in its development and which control parts of critical infrastructure and the government. But the framework itself remains bare-bones, with few specifics, and is voluntary. It remains to be seen whether true cybersecurity standards for private companies to be held to will follow, and also whether additional advances to US government cyber capabilities will be pushed to improve upon the executive order.

A more significant cyber threat, or an actual attack, might expand upon pressures on lawmakers to begin proposing those changes. As companies continue to lose user data, the need for collaboration with the government becomes stronger. But absent significant damages to the companies themselves there is little to compel the currently conservative Congress to enact stricter regulations.

On the other hand, the impetus for more stringent government security may be found in such reports on the state of cybersecurity as one from March 2014 by the Federal Energy Regulatory Commission, that suggests attackers need only destroy “nine of the country’s 55,000 electric-transmission substations” to effect a more-than-yearlong blackout across the country (Smith). As several of the policy proposals analyzed have pointed out, such physical damage is possible through cyber means, making cybersecurity a highly critical and urgent issue. Direct improvements to US cyber infrastructure may not only be the path of least resistance for policymakers seeking reform, but may also be the most important immediate improvement to make to cybersecurity policy.

With China’s skyrocket to global prominence, the issue has become all the more pressing. As a smaller, industrializing economy China’s cyber overtures could be overlooked; the harm they caused to US businesses was miniature. And historically, industrializing nations have made good use of industrial espionage along the lines of current intellectual property theft to spur domestic industries. But with China’s increased economic power and ability to compete with the United States in a variety of fields, protecting that intellectual property is a matter of ensuring competitiveness for US firms.

The need for intellectual property protections is growing, hence the framework and the call for more collaboration on cybersecurity between the government and private companies. The government has a vested interest in ensuring the protection of critical infrastructure, and due to pressures from companies facing stiffer competition from China, it now has an interest in protecting these private companies themselves.

At the same time, the US is feeling pressure to reform its own cyber offenses. Edward Snowden’s revelation that the NSA has conducted cyber espionage into Chinese firms, notably telecom giant Huawei, has led to calls from China for the US to abandon these attacks and to “halt the practice of cyberespionage” (Jacobs). By taking these offensives the US is culpable of exactly the sort of cyber attacks of which US leaders have accused China, and which the policies outlined in this essay have sought to prevent. As such these actions have hampered the Obama administration’s ability to effectively challenge Beijing on cybersecurity issues.

However, the fact that the US is launching its own hacking initiatives into Chinese companies may help enact those policies which seek collaboration with China and other countries. Chinese officials have “called on both countries to step up efforts to end the spying” (Jacobs). If both countries are guilty of cybersecurity violations, then perhaps both countries can more easily find common ground to bilaterally reduce them. “Recently, both sides have promised to hold regular high-level talks and negotiate new standards for cybersecurity and commercial espionage” (Jacobs).

This sort of solution, which is a more inclusive and direct alternative to Wallace’s proposal, does not preclude the type of cybersecurity improvements outlined by other experts, namely Clark and Levin. Their standards for improved cyber defenses would mitigate the threat of cyber attacks and hackers, but would not represent an offensive step – many if not all of the measures they propose are entirely defensive in nature.

As the dangers of cyber attacks continue to mount, as the US's own cyber forays are called into question, and as the threat to US economic power sharpens, reforms become more likely, and more politically viable in Congress. The movement towards reform of critical infrastructure has already begun, spurred by the reports of potential threats. Various industries have become more embattled by stiff Chinese competition, making intellectual property a more precious resource for firms. With these pressures mounting, legislative action will continue to become more likely, and the policies that seek to address these without compromising on privacy rights or infringing on businesses gain the viability to be successfully implemented.

# Works Cited

"Executive Order -- Improving Critical Infrastructure Cybersecurity." *The White House*. Office of the Press Secretary, 12 Feb. 2013. Web.

Jacobs, Andrew. "After Reports on N.S.A., China Urges End to Spying." *The New York Times*. The New York Times, 24 Mar. 2014. Web.

"Launch of the Cybersecurity Framework." *The White House*. Office of the Press Secretary, 12 Feb. 2014. Web.

Smith, Rebecca. "U.S. Risks National Blackout From Small-Scale Attack." *The Wall Street Journal*. Dow Jones & Company, 12 Mar. 2014. Web.

## Works Consulted

Harper, Jim. "Assessing Cybersecurity Activities at NIST and DHS." *Cato Institute*. Cato Institute, 25 June 2009. Web.

Kissinger, Henry. *On China*. New York: Penguin, 2011. Print.

Peterson, Andrea, and Sean Pool. "U.S. Cybersecurity Policy in Context." *Center for American Progress*. Center for American Progress, 22 Feb. 2013. Web.

Sanchez, Julian. "CISPA Is Dead. Now Let's Do a Cybersecurity Bill Right." *Cato Institute*. Cato Institute, 26 Apr. 2013. Web.

Swire, Peter. "Getting Online Privacy Policy Right." *Center for American Progress*. Center for American Progress, 28 Jan. 2011. Web.

Wallace, Ian. "Is There Such a Thing as Cyberwar?" *The Brookings Institution*. The Brookings Institution, 27 Sept. 2013. Web.