The Emergence of Cyber Deterrence by Economic Pressure:

An Examination of the Formation of the Policy Economic Cyber Deterrence in US Response to Chinese Cyber Activities

Dillon Zhou
International Relations Master's Program
McCormack Graduate School of Policy and Global Studies
University of Massachusetts, Boston
August, 2012

Abstract

This paper explores the formation of a emerging, but unofficial US policy in response to China's strategic activities in cyberspace toward the US and its international allies and partners – including the unlawful acquisition of intellectual property and collection of strategic political and economic intelligence from these countries through the cyberspace – by closely examining the context, and political ramifications of this emerging policy. This policy is tentatively called – for the purposes of this paper – the "Policy of Economic Cyber Deterrence" owing to the fact that the US appears to be using its cybersecurity concerns as the basis to impose economic countermeasures against China, while coordinating similar measures with its international allies and partners to protect the critical infrastructure of those affected by China's cyber activities. The paper will start by concisely illustrating basis and nature of the validity of US concerns by laying out the position of US policymakers and China's alleged cyber activities. Then, it will proceed by laying the theoretical roots of the policy through an overview of the theory of cyber deterrence, the body of thought from which the policy in question seems to be derived. Then, the actions taken under the Policy of Economic Cyber Deterrence will be presented followed by an argument for the possible policy implications of this policy. This paper will conclude with a list of policy recommendations for how this unofficial policy might be refined. Cumulatively, all of these components should paint a comprehensive picture of a nascent, but promising policy that will enable the US to effectively realize the idea of cyber deterrence and put itself in a more operative position to engage China on its cyber security concerns.

1.0 Introduction

With the advent of the information age, cyberspace has become the indispensable domain through which the world conducts its social, economic, and political relations between state actors and private individuals. It has also become the source of contention in world as the competing political interests for these forces as cyberspace has become a place where valuable information can be acquired without physical force and damage can done through attacks that have no physical form by motivated individuals sitting in front of a personal computer. The US and China are far from being exceptions to this development as this domain has become a major source of tension between the two states in recent years as a result of China's extensive cyber espionage activities directed at the US and its allies and partners resulting in a serious and persistent violation of national security for all these parties as Chinese agents have gained extensive and unauthorized access to their computer networks. This has allowed the Chinese to obtain economic and strategic secrets to further its own national interests and to strengthen its strategic position relative to the US and others by taking preparatory measures against potential challenges to its core interests – which include its territorial claim over Taiwan, the South China Sea, Tibet and Diaoyu Islands. This issue has prompted the US and its allies and partners to take notice of China’s strategic activities in cyberspace and to take policy actions against China to demonstrate their degree of concern and to take measures to prevent the Chinese from continuing its intrusive conduct through policies base on the notion of cyber deterrence.

1.1 Theme and Main Points

This paper aims explore the emergence of a unofficial US policy that has begun to take form, in recent years, in response to China’s cyber espionage activities to demonstrate that it can be a potent tool for US policymakers to use in response to the Chinese cyber threat. This policy will

be referred to, tentative, as the “Policy of Economic Cyber Deterrence” (PECD) as its apparent function fulfills many of the principles of the theory of cyber deterrence – which can be seen in its demonstrated and potential role as a means to leverage serious economic damage against China to force the Chinese government in Beijing to seek a negotiated agreement that enables the US to have more control over the cyber security of its and improve the overall cyber security of its international allies and partners in terms of the cyber threat posed by China.

The primary focal point, for this paper, is how and why the US has taken action against China – within the broad context of the contest in cyberspace in parallel with tensions in the real world between the two powers, the respective thinking on both sides on norms of operating in cyberspace – through the economic measures that constitute PECD. In the past few years, the US Government has imposed serious restrictions on the activities of Huawei Technology, a major multinational Chinese telecommunication company with suspected strong ties to the Chinese government, in terms of its capacity to conduct business in the US market due to concerns regarding the role and motives of the company in Chinese cyber operations – especially in terms of the security o. Thus far the US has banned Huawei from bidding on the US critical information and communication technology (ICT) infrastructure projects and partner up with and invest in US companies in possession of sensitive technologies based on the government’s security concerns over China's cyber espionage activities – resulting in the loss of billions of dollars resulting from the loss of economic opportunities and negative . Furthermore, the US has been working in concert with its allies on intelligence gathered regarding China’s cyber espionage activities, including what it knows about Chinese ICT companies who cooperate with and benefit from China’s cyber espionage operations – coinciding in the application of certain

elements of PECD, by US allies and partners, which compounds the economic damage. These developments have had a chilling effect on China's strategic goal of to nurturing its infant information and communication technology (ICT) industry to become a globally competitive and critically important component of its broader economic development strategy to transform the China's economy from an industrial-based model to a knowledge-based model.

The underlying themes for this paper will be to answer the following questions: (1) Can the unofficial US Policy of Economic Cyber Deterrence be effective in countering China's cyber espionage activities; (2) Can the US find sufficient support to create a coalition of concerned allies and partners willing to create a coordinated and multilateral regime based on PECD based on shared concerns regarding China's cyber activities?; and (3) Can PECD motivate or induce the Chinese Government to move towards an agreement on conduct in cyberspace affecting interstate relations with the US and its international allies and partners by adopting practices that reduce intrusive cyber operations – involving theft of intellectual property and state secrets and intrusion on critical infrastructure for strategic purposes – and to enhance openness for the security of the Global ICT supply chain?

After a thorough examination and analysis of the literature and facts surrounding this question, one can conclude that the unofficial US Policy of Economic Cyber Deterrence is a nascent, but promising policy that has shown to be a potent tool for imposing real economic costs to China's cyber espionage activities – which had had been largely negligible before this policy began to take shape – with the strong possibility of having a multiplied effect given the shared concerns over China's cyber espionage activities of America's international allies and partners that will

likely pave a path for a negotiated agreement on conduct in cyberspace between the China and the US and its friends that will significantly reduce the damage caused by Chinese cyber espionage. To be sure, this policy is far from being a fully formed policy, nor is it a full-proof solution to US cyber security concerns regarding Chinese cyber espionage activities. It is a policy under development, but it has shown promise by the effect that it has had on China's disposition regarding the punitive impact that PECD has had on Huawei and others. In order to achieve the goal of formalizing this agreement, the US needs to further develop the unofficial Policy of Economic Cyber Deterrence by making this policy more coherent, credible, and pragmatic in consideration of existing realities.

This conclusion is based on several underpinning findings derived from exploring the circumstances under which this policy came into being and how it has impacted bilateral relations between US and China as well US relations with allies and partners that have openly expressed security concerns over Chinese cyber espionage within a uncertain normative environment:

- First off, the US and others have legitimate reasons to believe that the Chinese State is engaged in conducting cyber espionage against the US and others and for being concerned about the negative impact of Chinese cyber espionage and other cyber operations on US national security as these activities involve the theft of intellectual property, state secrets, and intrusive actions against US critical infrastructure.
- Second, many US allies and partners have similar suspicions and concerns, and some have shown a willingness to act upon them in with policy prescriptions similar to PECD.

- Third, the US has justifiable grounds for taking the restrictive economic measures against Huawei as there is ample and fairly robust evidence that supports the view that the Chinese State is using companies like Huawei to further its cyber espionage activities by overtly adding features to the ICT products that it exports abroad and acquiring sensitive technologies under the guise of making investments in US IT companies and building partnerships with US companies.
- Fourth, America's international allies and partners have reached similar conclusions about the security risk posed by Chinese cyber espionage – which may allow for multilateral cooperation in dealing with this risk by sharing intelligence and coordinating a mutually agreeable response.
- Fifth, the unofficial Policy of Economic Cyber Deterrence has the qualities to be an effective tool to prompt a serious response from the Chinese Government – especially when it becomes a multilateral policy that is applied for a multiplied effect – given China's strong interest in nurturing its indigenous ICT industry as part of its grander economic development strategy.
- Sixth, diplomatic engagement can and should be the primary avenue for resolving the security concerns as there are other ongoing and potentially kinetic security problems – involving both the US and China – and politico-economic issues between the two states that requires a firm, but practical approach that sends a clear and measured message that clearly states the US
- Lastly, the US needs to work on resolve the attribution problems and legal norm problems involved in operating cyberspace and reacting to national security issues emanating from this domain.

The goal of US policy on the matter of Chinese cyber espionage is to reduce the threat of cyber espionage with a mutual agreement between the US and China that allows the US to mitigate the risks with increased transparency on dealing with security concerns. The ultimate objection of the paper is to prove that PECD has shown itself to be viable and necessary given current security conditions in cyberspace and the potentially expanded tool through diplomacy to create the conditions that induce China to sign a mutually agreeable treaty that affirm conduct between the signatories aimed at reducing cyber threats from China and promotes transparency in the Global ICT supply chain.

1.2 Overview of Capstone

This capstone is organized to provide a methodical narration and examination of why and how the US policy of Economic Cyber Deterrence Policy has emerged as a policy tool for the US and its allies and partners in the international system – and how this development has impacted China's approach to how it conducts its cyber espionage activities and its government's political disposition toward this new policy in terms of how it views the impact of the policy and what it can do in response. In taking a step-by-step method of exploring this policy, it will become clear that the thesis of this paper is based on sound and reasonable.

- To start, the general reasons and context for why PECD was conceived will be examined by presenting China's economic cyber espionage activities as a real threat that has created equally real security concerns in the US and the rest of the world. Furthermore, this part will also illustrate limited nature of other policies and
- Second, the theoretical sides of the prime topic for this paper – including the theory of cyber deterrence, the vulnerabilities in the IT supply chain, and legal challenges associated with not having norms for operating in cyberspace.

- In the third part will be the critical analysis, which will be the most important of this paper as it will: (1) Explain the current state of PECD in terms of the philosophy behind it and how it has been implemented thus far; (2) Lay out the facts and circumstance surrounding the US restrictions against Huawei and the ramification this course of policy action on similar companies and China's national interests; (3) The legal basis for PECD under current international norms.
- The fifth section explains the policy implications of the US policy of economic cyber deterrence on US-China relations, US relations with its allies and partners and political conditions in China and the timeframe for the emergence of a diplomatic solution on the Chinese cyber threat.
- The paper will be wrapped up by a synthesis of my research, an outline my policy recommendations for how the policy of economic cyber deterrence, and a brief summary of where further research may be pursued.

2.0 Context for Economic Cyber Deterrence

The emergence of the US Policy of Economic Cyber Deterrence towards China, in its current state, is primarily due to the fact that China has become one of the most active nation-states in cyberspace and the strategic aims that it has pursued in this operating domain and the concern that this course of action has evoked in the US and its allies and partners. First, this policy stems from security concerns raised by US policymakers regarding the nature and damage caused by Chinese cyber espionage and cyber operations. This concern is the basis for why the policy emerged in the first place and based on testimonies and reports produced by government

agencies and cyber security experts, both of who have cyber forensic evidence that link notable cyber-attacks.

It's necessary to comprehend three topics: (1) The security concerns of the US regarding China's role in utilizing cyber espionage to garner intelligence and technology from the US for both economic and political purposes; (2) The security concerns and responses of other governments in the international system; and (3) The implications of the current state and direction of the cyber capabilities and national cyber strategies of the US and China in terms of how the US can effectively respond. Each topic represents a critical element within the bigger picture for the policy in question by helping to demonstrate that China is perceived and capable of being a perpetrator of cyber insecurity through its cyber espionage activities for its strategic national interests. This section will reveal that PECD is not only necessary in the face of the size and growth of the Chinese cyber threat, but also one of the few options that can be applied considering the largely untested nature of the other cybersecurity initiatives and the

2.1 Beware the Dragon's Cyber Shadow

To understand the origins, current status and future of PECD, as a policy, one needs to understand several critical factors. First, one must understand that there is considerable and weighty concern in the US Government about the danger posed by China's cyber operations, which explains why PECD has emerged in the first place: China's is using cyberspace as a means of gaining strategic parity towards its favor by stealing secrets from the US and others and taking preparatory measures against possible future conflict. Second, there must be an understanding of where America's international allies and partners stand on China's cyber threat and on the efficacy of PECD. In understanding these underlying matters, one comes to understand why PECD

exists: to prevent China from being able to actively conducting cyber operations against the US and undermine the perceived low or no cost nature of cyberwarfare in China, which will be explained in a later section on China's strategic outlook on the use of cyberspace. Third, the strategic disposition of the US and China will be compared to demonstrate the contrasting outlook on the use of cyberwarfare – which will end up proving that the US is far more conservative and sensitive about the use of this avenue of international conduct than China and has limited options in responding to China's assertive use of cyberspace. Hence, by the end of this part of the paper, it should be amply clear that the US and friends have good reason to be concerned about the security threat posed by China through its activities in cyberspace.

2.1.1 The Dragon's Objectives

During the past five years or so, the US Government and cyber security experts have become increasingly wary of China's cyber operations in terms of how extensively China's exploits have come in penetrating the US and its international allies and partners. This course of action, taken by China, has three main goals, according to Magnus Hjortdal, which include: (1) To infiltrate critical infrastructure of rival states as a part of a deterrence strategy; (2) Conduct military technological espionage to gain military knowledge; and (3) Conduct industrial espionage to gain economic advantage.[1] The methods of achieving these range from day-to-day cyber-attacks coming from China to organized cyber campaigns aimed at acquiring information that China considers vital to its national interests. Publicly accessible reports made to Congress and other government agencies indicate that China has become very bold in its cyber operations and needs to be given the proper level of concern as any threat emanating from the real world. Based on open sources on reports and testimony made for the US Government, by US cybersecurity experts, on the subject of China's cyber operations, there are two primary concerns – which can be branched

out as there are many underlying issues. The purpose of China's cyber operations can be best summarized, according to Hjortdal as follows:[2]

> China…has an interest in avoiding exposure to political and military pressure from the West and the United States. Secondly, China also has an interest in accelerating its military development since it is still far behind the West in general. And finally, with regard to the third reason, China's general technological level is also behind that of the United States, which gives it an increased incentive for industrial espionage in order to achieve economic advantage.

In short, China has a greater interest in using cyberspace offensively than other actors, such as the United States, since it has more to gain from spying on and deterring the United States than the other way around.[3] The intent of the People's Liberation Army is clear in the aggressive attitude it has chosen to take in Track 1.5 Talks that the US and China engaged in during the past few years with simulated exercises testing real response thinking on a range of possible tense scenarios between the US and China.[4] The point, here, is that China is aggressively pursing strategic goals through cyberspace at the expense of the US and not conforming to US standards of conduct. Hence, the US has a need to counter this high level national security threat with appropriate force and energy through policies designed at discouraging such behavior – including measures of the economic nature.

2.1.2 The Dragon's Claws and Breath

China's methods for pursuing its three primary goals in its cyber operations incudes a repertoire of means including daily cyber-attacks, cyber campaigns that make up its options for exploiting weaknesses in US networks and elsewhere. The major exploits, according to a report published by the ONCIX in 2011, include the following cases:[5]

- In a February 2011 study, McAfee attributed an intrusion set they labeled "Night Dragon" to an IP address located in China and indicated the intruders had exfiltrated data from the computer systems of global oil, energy, and petrochemical companies. Starting in November 2009, employees of targeted companies were subjected to social engineering,

spear-phishing e-mails, and network exploitation. The goal of the intrusions was to obtain information on sensitive competitive proprietary operations and on financing of oil and gas field bids and operations.

- In January 2010, VeriSign iDefense identified the Chinese Government as the sponsor of intrusions into Google's networks. Google subsequently made accusations that its source code had been taken—a charge that Beijing continues to deny.
- Mandiant reported in 2010 that information was pilfered from the corporate networks of a US Fortune 500 manufacturing company during business negotiations in which that company was looking to acquire a Chinese firm. Mandiant's report indicated that the US manufacturing company lost sensitive data on a weekly basis and that this may have helped the Chinese firm attain a better negotiating and pricing position.
- Participants at an ONCIX conference in November 2010 from a range of US private sector industries reported that client lists, merger and acquisition data, company information on pricing, and financial data were being extracted from company networks—especially those doing business with China.

Due to these individual exploits, China has taken on the role of "the world's most active and persistent perpetrator of economic espionage" through its intelligence gathering efforts of Chinese-born agents in the US and cyber espionage operations originating from within China.[6]

There are routine cyber attacks coming from China, which is also a cyber crime capital of the world, and they involve basic cyberwarfare tools like Trojans and other malware and techniques involved in phishing – social engineering in electronic form to gain information under false pretenses – to the detriment of the US and others.[7]

The Chinese also have extensive and complex spy networks that allow them to conduct surveillance on political and economic targets. Shadows in the Cloud and CloudNet are two such examples.

China also engages in massive and long-term cyber campaigns that target countries around the world with the aim to garner economic and political secrets from target states. In 2011, McAfee

– one of the top cyber security firms in the world – reported on two cyber espionage operations involving remote access tools (RAT) – a cyber tool that allowed the user to access information passing through major networks of firms by compromising the security of the network equipment and downloading malware allowing this surveillance capability that would remain undetected – which have been named "Nightdragon" and "Shady RAT."[8] In both cases, RAT were set up within private companies in sectors vital to China as it included the ICT industry, energy companies, government offices, and NGOs – including the US and Indian governments – to allow the user of the RAT to access the data and information passed along on the network and including trade and national secrets. The targets were largely focused on the ICT industry and government agents of the 72 targets identified by McAfee for Shady RAT and a significant number of energy companies in the case of Night Dragon. It was clear that these attacks could be traced back to China by using cyber forensics that traced the code used by the malware found on the network of the targets. Though there isn't anything that can be used to finger the Chinese government, the attacks have been all directed at targets that the Chinese have an interest in and in states that are prime rivals in China's economic interests with the US suffering the greatest number of attacks from these two cases – though the exact content extracted by these attacks cannot be discerned through open sources.

There were two other well-documented cases that were traced back to China for the same purposes as Shady RAT and Night Dragon. In January 2010, Google accused China of stealing some of the company's source code through a cyber-attack dubbed "Operation Aurora."[9] In this case, computer servers at two state-sponsored schools in China, Jiaotong University in Shanghai and Lanxiang Vocational School in Shandong Province, were found to have been used in the attack. Lanxiang was created with military support and continues training many of the military's

computer experts. (Ibid.) A report by Verisign iDefense suposedly determined that "Aurora" was directed by "agents of the Chinese state or proxies thereof."[1] Then there were the attacks against RSA – the security division of high-tech company EMC Corp – from March 2011 were traced to networks in Beijing and Shanghai with the help malware tool "HTran" – which Chinese hackers are known to bundle with their code in their cyber espionage efforts. [2] RSA's products are used to secure high-level computer networks throughout the US government as well as major corporations and defense contractors.

All of these reports have led most observers to conclude that cyber espionage is recognized "as much a state-sponsored activity as their military and civilian operations."[10] Though the traces and forensic research could not point to the Chinese state to be the perpetrator of the attacks launched against the non-Chinese targets across the world, the origins could always be traced back to Chinese servers in the national borders of China.

China has also engaged in a series of cyber campaigns against the US and its friends in the international system in an effort to further its strategic position in the international system by using sophisticated techniques and technical know-how to exploit the vulnerabilities of the US and others – all of which has been documented by the US Government and cyber security experts

In effect, there is a shadow struggle between the US and China to see who can gain the edge through exchanges between the cyber warriors – agents and soldiers responsible for protecting

---

[1] Ibid.

[2] Ellen Messmer, "RSA SecurID hack originated in China, says researcher," Techworld, http://news.techworld.com/security/3295222/rsa-securid-hack-originated-in-china-says-researcher/ [Accessed January 12, 2012].

and operating the networks of a nation in pursuit of said country's national interests – that call for them to launch cyber-attacks through common tactics of denial of service attacks, spyware, Trojan horses, and logic time bombs to gain intelligence on each other and preparing for one another's strategic measures and thinking.

2.1.3 Capitol Hill Ire at the Dragon's Shadow

These concerns has garnered a substantial response from US policymakers – who have answered China's widespread and persistent cyber operations by publicly addressing the mounting concerns regarding China's role in cyber intrusions. To begin with, US policymakers have become vocal about the need to confront China. Representative Mike Rogers, Chairman of the House Permanent Select Committee on Intelligence (HPSCI), noted, during a hearing on "Cyber Threats and Ongoing Efforts to Protect the Nation" on October 4, 2011, that China's cyber espionage needed to be challenged as such actions threaten the "technological leadership and national security" of America. In his prepared statement at the beginning of this hearing, he stated: [11]

> China's [cyber] economic espionage has reached an intolerable level and I believe the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they stop to this piracy…Combined, the United States and our allies in Europe and Asia have significant diplomatic and economic leverage over China, and we should use this to our advantage to put an end to this scourge.

Representative Rogers' effusive candor on China's economic cyber espionage reflects a growing view among US policymakers and based on a substantial list of evidence gathered by government and non-government cyber security experts. Both of Northrup Grumman's reports on "Chinese Capabilities for Computer Network Operations and Cyber Espionage" from 2009 and 2012 show that the Chinese state has close ties that involve Huawei's equipment and practices.[12] This gives ground to take action against China through firm action and policy. Policy

has not been forthcoming, but not because of effort. Rogers proposed the Cyber Intelligence Sharing Act of 2012.[13] The bill later failed in the Senate due to privacy and freedom concerns.

2.2 International Views on Chinese Cyber Operations

Like the US, many other nation-states – including allies and partners of the US – share a similar level of concern over China's cyber operations, which in turn make them opportune collaborators in broadening the US policy response to China. This is especially when it comes to PECD as the economic cost imposed on China for its cyber operations can be multiplied with each state that joins the US coalition. These nation-states range from mildly concerned to the highly concerned – which are reflected in their course of actions done behind closed doors and through public statements. They all share the same threat, as all of them have been victims of China's cyber campaigns and operations in the past.

2.2.1 Views of Strong Suspicion

In the case of the United Kingdom, Australia, India, and Taiwan there is a strong degree of concern over China's cyber operations illustrated by public acknowledgement of this concern by the respective governments. Each of these nations have directly identified China as a major source of cyber insecurity and adapted stances of active defense. Each have accused China of conducting cyber espionage among other cyber crimes against their national security interests.

2.2.2 Views of Reserved Suspicion

In Germany, Japan, and France, however, there is also shared concern about China's cyber operations, but the government response has not been as pointed in their public statements on China's cyber activities and tend to be more passive in nature. Each state have noted that China is engaged in cyber espionage and violated its security interests. But none have taken serious action.

2.3 The State and Implications of National Cyber Strategy & Capabilities

The US and China are among a small group of nation-states recognized as the leading powers in cyberspace owing to their extensive national cyber capabilities – that each country has developed – which allow them to operate in cyberspace as great virtual powers. For the purposes of this paper, the focus of this section will be focused on exploring US and Chinese cyber capabilities so as to keep the scope of this paper within a narrow focus. By looking at the strategic underpinnings of US and Chinese cyber strategy and cyber capabilities, one can discern the motivations of both sides as well as the basis of PECD given the limitations of the US approach.

2.3.1 US Strategic Thinking and Capabilities

The US has, thus far, been vague in its strategic outlook on cybersecurity, but has taken moves to shore up the capabilities of its cyber warriors in the Department of Defense (DOD), National Security Agency (NSA), and Department of Homeland Security (DHS). The only problem is that there aren't many options.

Strategic Thinking

Looking back in recent history of US policy, cybersecurity remains as a largely neglected national security issue given the fact that despite the attention given to the issue by the Chief Executive of the US Government during the last three administrations, the US still does not have a functional national cyber strategy to use to protect and pursue its national interests in cyberspace. This is precisely why PECD is unique as it is one of the few policy tools in effect that has been applied and continues to be adjusted to meet the changing conditions in both cyberspace and the real world as they affect US-China relations. The underlying principles have

been based on the idea that defense is key with resources provided to secure networks by training staff and installing security programs.

The challenge for US strategic thinking and capabilities in cyberspace is the creation of norms and legal guidelines for operating in this domain – which has, thus far, been intransigent given the nuanced nature of internet governance and the need to contend with the politics of this area of public policy, a concern that involves both foreign and domestic factors. What is clear is that while the US is devoting considerable resources to the protection of US networks, though there are some debates within Congress on how best to do so without compromising the fundamental civil liberties of US citizens in the process. The US has developed considerable offensive capabilities as well, but they remain largely unusable given the uncertainty within current strategic thinking on operating in cyberspace, which includes a largely secret cyberweapons program, which the DOD hopes to use as a matter of deterrence against foreign powers like China.

US Options and Capabilities

The US is currently engaged in the build-up of an extensive cybersecurity program – dubbed as "Plan X" by DOD planners – to give the US superiority in cyberspace by working on an arsenal of cyberweapons and improving cyber defense under the ostensible under the direction of the Defense Advanced Research Projects Agency (DARPA) – the same agency responsible for creating cyberspace in the 1970s.[14] This program promises to be critical. According to Herbert S. Lin, a cybersecurity expert with the National Research Council of the National Academies, "If they can do it, it's a really big deal. If they achieve it, they're talking about being able to dominate the digital battlefield just like they do the traditional battlefield."[15]

From a policy perspective, there is a "policy reboot" in the US that has helped the US to progress on updating its cyber policies and strategies, which can be boiled down to these qualities:[16]

- Basic Continuity: These policies generally continue to prioritize cyber efforts in similar ways to past policies. These include strengthening cybersecurity for federal systems, improving protections for consumers, and broadly increasing international cooperation.
- Some New Ideas: However, this essential continuity should be considered updated, as the US government has learned from the lessons of the past two decades. For example, the Department of Defense is no longer emphasizing offense or deterrence by punishment, and "regulation" is no longer quite as dirty a word as it used to be.
- A Light but Expanding Government Touch: Programs remain generally voluntary, though there is proposed new legislation calling for regulation of companies in critical infrastructure sectors.
- Inclusion and Balance of New Areas of Cyber Statecraft: Whereas past cyber strategies typically only covered security and, at times, innovation, the new policies are more holistic. The inclusion of new areas of cyber statecraft (including norms of international behavior, Internet freedom, and development) allows the government to better prioritize and balance between policies. The DoD has struck a better balance by emphasizing defense over offense, and all cyber strategy documents highlight the importance of the American values of free speech and commerce.

The US has few options as the strategy remains under development. Healey and others consider the strategic work to be insufficient with little detail and little action. The weapon program remains in the shop and needs more time to come out on the DOD's timetable.

2.3.2 Chinese Strategic Thinking

In contrast to the US, the Chinese operate on the notion that cyberspace is a domain where China can gain the most in consideration of the cost in resources required and potential political fallout over cyber activities

In the mind of policymakers in China, the US stands as main rival that stands as a single greatest potential threat to China; meanwhile, China's development as a nation – in terms of military, technological and military advancement – remains behind and inadequate to the task of meeting

such power in a hypothetical conflict involving the two nations. Hence, cyberspace has become one of the major areas where Chinese leaders hope to equalize the balance of power between the two nations has stepped up cyber-attacks as a means of gaining technological and intelligence materials to gain in strategic position against the US and other technologically superior states. Cyberwarfare offers China the chance to do this through the host of asymmetric methods – including all of the things that the US and its allies and partners are concerned with – while keeping true to traditional Chinese military stratagems.

Cyberspace, according to Chinese military thinkers, is a domain that offers China the opportunity to take the initiative against its rivals in the international system who compete with China on both a political and economic level. The Chinese see cyber warfare as:

> [A] struggle between opposing sides making use of network technology and methods to struggle for an information advantage in the fields of politics, economics military affairs and technology…[through] a series of actions like network surveillance, network attack, network defense, and network support by opposing sides using network technology in the area of combat command, weapons control, combat support, logistical support, intelligence reconnaissance, and combat management.[17]

Using this philosophy as an underpinning guide, China has adopted what one might call a quasi-strategy to guide its conduct toward other nation-states in cyberspace.[18] This long-term goal of this strategy is to "ensure [that China will have] eventual strategic parity with the United States in technological and military prowess." mag

The origin of this strategy begins with a controversial book titled "Unrestricted Warfare" published in 1999 by two PLA colonels, Qiao Long and Wang Xiangsui – which appears to have served as a "primary catalyst for a new mode of thinking in the People's Liberation Army."[19]

The US has a special place in China's strategy for cyberspace due to Beijing's belief that America represents the main strategic obstacle to its national interests owing to the superiority of conventional US military forces and the perceived strategic measures taken by the US to "contain" China's rise in Asia and its pursuit of its national interests. Due to tensions between the US and China, policymakers in Beijing have come to see the US as the main strategic rival to China's national interests. This viewpoint has motivated Chinese planners to take what it considers preparatory measures against the US to

China's current cyber operations – as noted by – fall under what Timothy Thomas, a senior analyst at the Foreign Military Studies Office, calls "China's Long-Range Electronic Patrol" or "Electronic Reconnaissance Applications."[20]

China is "[g]uided by a 15-year (2006-2020) development strategy, a priority of the Chinese Communist Party (CCP) and PRC government is the informatization of its national civilian and military infrastructure as a means to ensure sustained economic growth, compete globally in the ICT realm, and ensure national security." The origins of China's movement towards informationization is rooted in the government's aspiration for developing China's economic and military power.

3.0 Literature Review

While a great many facts of this paper are known and well-documented, to a certain degree, there are a number of critical issues that remain in the realm of the theoretical owing to a lack of hard evidence or documentation. The main theoretical underpinning issues of this paper are: (1) The theory of cyber deterrence; (2) The threat of a compromised global IT supply chain; and (3) The

Legal Norms for Operating in Cyberspace. PECD is based on the general theory of cyber deterrence as this emergent policy is based on the general principles of this general theory. The vulnerability of the global IT supply chain is one of the main reasons for why PECD is necessary as the hardware and software being used to build US and global ICT networks may be compromised by "backdoors" within their makeup as part of a deliberate course of action taken at the behest or direct guidance of the Chinese government. All of these issues, along with the security concerns mentioned in the previous section, stem from that fact that there are few if any legal norms governing how nation-states should behave toward one another through their actions in cyberspace.

3.1 Cyber Deterrence Theory Redux

The theory of cyber deterrence is the basis of US cyber strategy – as noted above – but it remains largely a nuanced, but untested theory that remains on the drawing board given the ongoing studies on how cyberspace will be managed by state actors. The important thing is that defense must be strong and that there is a clear policy through a public declaration.

The primary function of deterrence as a strategy can be best summed up by Jonathan Solomon, who described it as "the art of convincing an enemy not to take a specific action by threatening it with intolerable punishment and/or unacceptable failure" – which is derived from Thomas Schelling's work "Arms and Influence." This is the most fitting definition given what the US has done in regards

In drafting a policy of cyber deterrence, there are several analytical steps to consider:[21]

1. Specify the deterrence objects and the strategic context
2. Assess the strategic calculus of adversary decisionmakers
3. Identify desired deterrence effects on adversary conduct

4. Develop and assess courses of action designed to achieve the desired effects
5. Develop plans to execute deterrence courses of action and to monitor and assess adversary responses
6. Develop capacities to respond flexibly and effectively as the deterrence evolves

By taking these steps, a design will emerge as the basis for a "clear and firm declaratory spelling out the US intention to deter cyber attacks."[22]

3.2 The Risks in the Global IT Supply Chain

The global supply chain for ICT goods is vulnerable in theory and in practice due to the limited ability of companies and governments alike in procuring economically sound supply of ICT goods, while trying to apply strict supply chain security – which is nearly impossible to do given the rapid pace of developments in the global economy and China. But the proof of a "backdoor" for the Chinese remains in the realm of the theoretical as current research cannot prove any intentional created "backdoors" within the chain.

3.2.1 The General Problem of Securing the Global ICT Supply Chain

Currently the Global ICT Supply Chain (GICTSC) is a recognized national security problem. The Government Accountability Office (GAO) has conducted an extensive investigation into the vulnerabilities of the GICTSC and the current readiness of the US government to address these vulnerabilities. The investigation determined that there are several ways that the supply chain can be compromised by a foreign power:[23]

- Installation of intentionally harmful hardware or software (i.e., containing "malicious logic");
- Installation of counterfeit hardware or software;
- Failure or disruption in the production or distribution of critical products;

- Reliance on malicious or unqualified service providers for the performance of technical services; and
- Installation of hardware or software containing unintentional vulnerabilities, such as defective code.

Normal hardware and software from the GICTSC go through multiple contractors who may in turn rely on subsidiaries to meet demand for ICT good like chips, programming, and IT equipment components and systems.[24] Counterfeit ICT goods – goods falsely marketed as brand name or proprietary goods from reputable companies – are particularly risky because the counterfeiters – who may be connected to legitimate dealers or producers – can modify such goods to add "backdoor" features that allow hackers to exploit.[25]

The GAO found that the security related agencies in the Federal Government – including DOD, the Department of Homeland Security (DHS), Department of Justice (DOJ), and Department of Energy – by their own admission and through its investigation that there isn't sufficient planning or protocol for protecting the supply chain and thus there is a strong need to protect and inspect the supply chain in critical infrastructure supply chain – including government and other vital areas.

3.2.2 Vulnerability in the Military ICT Supply Chain

The GAO also did a similar investigation of the DOD's supply chain and found that like the general ICT supply chain used by the Federal Government, there were serious vulnerabilities in this supply chain as well – in the form of counterfeit military grade microchips – and that the source came from.[26]

3.2.2 The China Factor in "Backdoor" Threats

China has the capability of adding features into the electronic products it produces. It has been reported that most, if not all, ICT products used for conducting business – including laptops, iPads, Blackberries, and other similar devices – in China have been compromised by a concerted effort by Chinese actors to lift information off of travelers in China. According to the New York Times and Washington Post, using "electronic surveillance that is sophisticated and pervasive" to gain intelligence on travelers – especially those of the corporate type or foreign government officials – which forces travelers to take high levels of precautions against such intelligence gathering efforts. The use of Bluetooth and Wi-Fi technology in many of the devices used by foreign travelers allow hackers to pick up vital information like passwords and other data from the IT devices that the travelers are using. While these cyber espionage efforts are not limited to China and cannot be linked to the Chinese Government, one generally finds that that such activity is less prevalent in places like the US and that such a insecure environment undermines the confidence in the Chinese Government's professed policy against cyber crime. Travelers have had to take precautions to ensure that their data is not stolen by using disposable cell phones, using "loaner laptops stripped of sensitive data", and using flash drives to protect sensitive information – which are all based, in part on the recommendation issued to travelers by ONCIX before the 2008 Beijing Olympics due to concerns with extensive electronic surveillance done by "Chinese security agencies" through the bugging of Chinese hotels. This situation is compounded by the fact that China has laws in place to prevent travelers from entering the country with "encrypted devices" without permission from the government.

Being the "factory of the world", China produces much of the world's manufactured goods – including ICT goods – that are exported all over the world – which includes the US and its allies

and partners. The threat of having a "backdoor" is a hotly debated issue among the insiders in the information security industry – especially when it comes to the Chinese factor – as the vulnerabilities within software and hardware are both

It has been reported that most, if not all, ICT products used for conducting business – including laptops, iPads, Blackberries, and other similar devices – in China have been compromised by a concerted effort by Chinese actors to lift information off of travelers in China. According to the *New York Times* and *Washington Post*, using "electronic surveillance that is sophisticated and pervasive" to gain intelligence on travelers – especially those of the corporate type or foreign government officials – which forces travelers to take high levels of precautions against such intelligence gathering efforts.[27] The use of Bluetooth and Wi-Fi technology in many of the devices used . While these cyber espionage efforts are not limited to China and cannot be linked to the Chinese Government, one generally finds that that such activity is less prevalent in places like the US and that such a insecure environment undermines the confidence in the Chinese Government's professed policy against cyber crime. Travelers have had to take precautions to ensure that their data is not stolen by using disposable cell phones, using "loaner laptops stripped of sensitive data", and using flash drives to protect sensitive information – which are all based, in part on the recommendation issued to travelers by ONCIX before the 2008 Beijing Olympics due to concerns with extensive electronic surveillance done by "Chinese security agencies" through the bugging of Chinese hotels.[28] This situation is compounded by the fact that China has laws in place to prevent travelers from entering the country with "encrypted devices" without permission from the government.[29]

Case Study: The Actel/Microsemi Pro ASIC3's Silicon "Backdoor"

In March 2012, Sergei Skobagtov and Christopher Woods published a draft of their paper on the "discover" of a "backdoor" in what they called a "military grade chip" that was manufactured in China, which could allow a hackers working on behalf of the Chinese government to "disable all security on the chip, reprogram crypto and access keys, modify low-level silicon features, access unencrypted configuration bitstream or permanently damage the [field-programmable gate array (FPGA)]."[30]

In the feedback that Skobagtov and Woods received, there was some serious criticism of the assertions made by the draft. Robert David Graham's criticism, in particular, was critical of the way that the draft was presented and the assertions about the backdoor.[31] What one should take away from the debate is that there are inherent vulnerabilities that can be built by design or not by manufacturers or the Chinese subsidiaries, highlighting supply chain security as a major issue.

3.3 Legal Norms for Nation-States Operating in Cyberspace

Much of the challenge in crafting cyber policy on the interstate level derives from the generally lawless nature of cyberspace and the technical challenges involve in attributing activities done by nation-state actors like the US and China.

3.3.1 The Pre-Westphalia Domain

As of this moment, there are no legally binding norms for how nation-states like the US – much less private individuals – operate on the international stage despite the fact that the internet has become a critical part of the global marketplace over the last fifteen years or so. In a nutshell, the

legal status of actions done through cyberspace can be described – according to the SecDev Group – as follows:

> Despite the plethora of international initiatives, positions, and statements concerning the inter-net, freedom of expression, and corporate social responsibility, there is a distinct lack of binding commitments in any arena. Broad, sweeping statements make for powerful rhetoric, but do not provide for specification.[32]

This is especially true for the US as a stakeholder and contributor to the broader effort by the world to gain a legal norm on operating in cyberspace on an international level. In the US, the applicability of international law "may be ascertained by consulting the works of jurists, writing professedly on public law; or by the general usage and practice of nations; or by judicial decisions recognizing and enforcing that law"; hence, one can argue that there is little binding guidance for the US in its approach to operating in cyberspace.

3.3.2 The Challenge of Attribution

One of the most challenging parts of dealing with cyber operations is attributing the source of cyber attacks. Work on this area has been limited and success is based on tracing back through multiple countries based on an analysis of the data in cyber attacks through the program code.

4.0 Critical Analysis

The US has known for a long time that China has been stealing industrial and economic secrets from the US and that cyberspace has become the primary domain through which these activities are being conducted through. PECD remains one of the few options that are being implemented to deter China from engaging in such a behavior by challenging the precepts of China's cyber strategy – which emphasized seizing the strategically superior position with the US to prepare for possible future conflict(s) – by taking critical action to reduce the effectiveness of this strategy. This section will closely examine the current tenets of PECD, where it comes from, how the US and others have implemented it, and explain why it's legal, effective, and can be further

developed. The purpose of doing so will demonstrate that PECD is a nascent, but effective policy that addresses the concerns expressed by US policymakers and cybersecurity experts by legally and effectively reduces the cyber threat posed by credible security vulnerabilities imposing an economic cost on China's cyber operations thereby lowering the incentives to engage in this type of activity. All of these assertions can be seen in the case study of Huawei Technologies as it has become both the prime example and trigger of PECD. Being a well-known Chinese company who holds the position of the world's second largest telecommunication equipment producer in the world as well as being a so-called "national champion" company, Huawei has the reputation of being both a global IT wunderkind company as well as being a suspected agent of China's PLA. The suspicion of Huawei's ties to the Chinese government has led to the US and others to take measures to reduce the possible threat emanating from this company by implementing the various policy actions that are now the principle provisions of PECD. What is notable about this situation is that this policy is legal and has the potential to be an increasingly effective political tool to be used against China by the US and its friends to legally and with a potentially multiplied effect as more and more nations join the coordinated effort to reduce China

4.1 Policy of Economic Cyber Deterrence

When closely examined, PECD represents a real and effective policy that realizes many, if not all of the principles of the theory of cyber deterrence through its duo purpose functions. In essence, by imposing restrictions on a suspected Chinese company's ability to con in the pursuit of reducing the cyber threat posed by China while imposing a discernible, effective and targeted cost to this type of operations.

Based on the policy actions taken thus far, PECD is built on using national security concerns regarding as this policy counters the potential threat of "backdoors" in Chinese ICT goods coming from the global IT supply chain by seeking to limit the vulnerability and by carefully restricting the business activities of companies suspected of being complicit in China's cyber operations – like Huawei Technologies, whose case will showcase the current state and future direction of PECD. This section will seek to enunciate the terms of PECD as a policy to set up the following exploratory parts of this paper – including the case study of Huawei Technologies, the chilling

effects of PECD, the impact of PECD on China's broad economic strategy, and the legal basis of PECD, all of which more fully

PECD is unique in that it's emerging during a renaissance for cybersecurity policy in the US as no serious attempts have been attempted since 2002. According to Jason Healey, the director of the Cyber Statecraft Initiative at the Atlantic Council, the US is in the process of a "policy re-boot" [3334]

4.2 Case Study: Security Concerns Regarding Huawei

As a rising superstar in the telecommunication Huawei has roots in the PLA and the Chinese state supports it through policy in exchange for facilitating Chinese cyber espionage through backdoors added in their software and hardware. Huawei has tried to enter the US market to no avail as the US has imposed heavy restrictions against Huawei. A important thing to note is that the economic pressure put on Huawei is selective and not across the board as previously noted by Borg on the futility of trying. What is important is that the US must take active measures to install protocols controlling and demanding transparency in the supply chains.

4.2.1 The National Champion's State Links

Huawei is widely recognized as being the wunderkind of Chinese ICT companies in the global telecommunications industry. Reuters, "TIME LINE – The Meteoric Rise of China's Huawei," *Reuters*, http://www.reuters.com/article/2009/07/01/huawei-china-idUSPEK24147220090701 [Accessed February 10, 2012]. Its status as a so-called "national champion" of the private sector has been a boon to its fortunes and also for China's interest in building up its own indigenous ICT companies. As a result of this status, Huawei was able to become globally competitive and expand its operations to the markets of the world.

Rise of a Champion

The story of Huawei's rise as a global telecommunications giant was based on humble beginnings. Years after its initial founding around 1987-88 by a former PLA officer Ren

Zhengfei – who was noted for his aptitude with ICT during his service – and his former PLA colleagues with an initial investment of 20,000 RMB to build up Huawei.[35] At the beginning, Huawei's business was "to distribute imported switches and to assemble and repair telecommunication-communications hardware for the domestic market."[36] Ibid. However, Mr. Ren believed that his privately owned and operated enterprise's future was in designing, manufacturing, and marketing telecommunication equipment of its very own – a goal realized by 1993 when Huawei brought its own unique design on a switch to market.
Breznitz and Murphree, 177-180; Harwit, 126-127.
Huawei's strength has been its ability to improve upon the engineering of others and suffer from a lack of originality in the equipment it's produced thus far – which has benefited from heavy R&D investment from up to 10% of Huawei's annual revenues. Such a course paid off allowing Huawei to produce more advanced products by the mid and late 1990s like the 3rd generation ICT Equipment (3G) in that timeline.

Huawei started walking down the path to become a so-called "national champion" when Mr. Ren got the opportunity to meet with Jiang Zemin – the CCP's Secretary General – in 1994 about the notion of making China self-sufficient when it comes to building ICT infrastructure with China-made goods produced by Chinese companies like Huawei. Ibid. As it became more successful in conjunction with the emergence of China's INE program of "informationizing" the Chinese economy, the Chinese government chose to give Huawei hundreds of millions in RMB in loans to fund its growth and capacity to produce as well as favoring it in government contracts and policy of encouraging private Chinese to "buy Chinese". Ibid. These measures helped Huawei to build up its base of operations across the world that spans to 130 states with factories, R&D labs, and divisions in all those countries and compete with low cost due of Huawei's wares created by the subsidies given by Beijing to promote the strength of Chinese ICT companies. This also helped China to build substantial part of its infrastructure as many major ICT contracts were filled by Huawei thus allowing China growing freedom and self-reliance in its goal of "informationization" to become a knowledge economy. Regarding security concerns arising from this matter, it's unclear if the Chinese government also acquired ownership in Huawei as there are conflicting sources on this matter with some saying that Huawei is privately owned for the

most part and others saying that Huawei has been bought to some degree that allows Chinese intelligence to have leverage – all of which will be explained in the next section.

Continued State Support

Huawei undoubtedly enjoys continued support from the Chinese state in political and economic terms, but the exact nature of this relationship remains unclear in the area concerning economic support. It is, however, no secret that the Chinese Communist Party (CCP) has people inside indigenous Chinese companies like Huawei. In fact, it's common knowledge – as reported by *The Economist* – for any common observer to know off-hand that the CCP posts party cells within Chinese companies in the private sector to oversee the operations and management of these companies.[37] The concern with telecommunications companies – like Huawei – is that the PLA and Chinese intelligence utilize their stakes in such companies – mainly stocks and favorable policies – to leverage the companies into adopting practices that would allow China to have a "backdoor" into the companies' operations and in the case of Huawei: their equipment.

What is problematic is that any "backdoors" created at the direction or direct involvement of Chinese intelligence services would be far more dangerous than any cyber-attack – in hardware or software – is that it would provide a more rewarding means of gathering intelligence. According to Northrup Grumman – in the case of "a successful penetration of a telecommunications supply chain such has the potential to cause a catastrophic failure of select systems and networks supporting critical infrastructure for national security or public safety" regardless of the technical savvy of any hacker attempting to steal information via cyberspace alone.[38]

By searching open resources on China's cyber espionage capabilities, it becomes clear that the connection between the Chinese Government and Chinese ICT companies is more than the standard politico-economic policy support given to national champions – in the opinion of government commissioned reports. At present, only reports from the US are available. This includes three directly related reports commissioned by the U.S.-China Economic and Security Review Commission (USCC) – completed by three defense consulting companies: Northrup

Grumman, Reperri LLC, and Invictus – China has been shown to have a more covert connection to companies like Huawei that serve the intelligence gathering efforts of the Chinese Government – including two reports from Northrop Grumman on Chinese Capabilities for Computer Network Operations and Cyber Espionage in 2009 and 2012, a report on the risks of allowing companies like Huawei to invest and integrate its business with the critical infrastructure of important rival states like the US, and a report on the direct hand that the state has in supporting cyber espionage for economic and political purposes.

The Intelligence Connection

In the reports, the authors stated Huawei has been contracted to produce command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) products for the PLA. This development with the PLA's need of C4ISR and the fact that most of China's cyber intelligence comes from the PLA's 3rd and 4th Departments – who use SIGINT and HUMINT and other means to secure intelligence for China. The "national champion" status is selected as the primary indication of the reasoning behind the suspicion of Huawei being a cyber-threat due to the nature of its relationship with the Chinese government – while providing no clear cut evidence that Huawei has in fact acquiesced to any intelligence operations or put any "backdoor" in their telecommunications gear, but only to note that there is a vulnerability in the US mobile networks that would raise the risk if Huawei were to get integrated into these and other networks critical to the US economy like those of major corporations that do business with the US government. In the report filed by Repetri LLC, it's noted that the Chinese have a motive for its MNC telecommunication companies – like Huawei – as the companies are often noted in creating joint ventures with companies from the target countries or acquired financially struggling ones.[39]

In all the reports, there is a notable concern raised about the strong possibility that Huawei and other Chinese ICT companies have incorporated intelligence gathering features in their hardware and software that makes them a high security risk to the US from both an economic and political perspective. In effect, the concern is over the "backdoor" features that allow Chinese intelligence services to gain access to US secrets – both political and economic – that would allow the

Chinese to have advanced knowledge of US intellectual property secrets, economic data, and intelligence that could be utilized to advance China's transformation strategy by supplying them with technologies created and produced by them for export to target markets. The important thing to note is that none of the reports provide direct evidence of the alleged threats, but rather they all point to Huawei's founder and his PLA roots along with the dealings that Huawei has with the PLA and government as a "national champion."

4.2.2 Entry Troubles with the US Market

Huawei's experience in the US has been, perhaps, the most significant challenge to its rise as a global ICT company as it has been repeatedly denied access to the market by deliberate US policy and the most telling illustration for how PECD came into being. This course of policy is not an officially acknowledged policy, but it has been implemented to great effect against all of Huawei's attempts to enter the US market. In sum, Huawei's problematic experience in the US stems from the following narrative:

> Huawei's frustrated attempts to make serious inroads in the US add up to more than just a corporate saga. They reveal deepening mutual distrust between China and America. In the US, there is growing frustration and alarm in the intelligence community and in Congress at its companies' dependence on China for critical components in highly sensitive industries. There are also concerns that US groups are placed at a disadvantage by hidden financial support from Beijing for their rivals. China, for its part, suspects that America is seeking to contain its rise on all fronts, including economic.

To be sure, the cyber security concerns highlighted by the reports by the USCC are not the only factors at play, but they remain a legitimate issue in the US approach to Huawei's business activities in the US. Furthermore, the US doesn't have an official policy for dealing with cyber-attacks whether it came from China or someplace else. The 2012 Northrup Grumman Report states that:

> Even if circumstantial evidence points to China as the culprit, no policy currently exists to easily determine appropriate response options to a large scale attack on U.S. military or civilian networks in which definitive attribution is lacking.

What the US Government has is a unofficial policy of limiting prominent Chinese national champions from the ICT industry from gaining a firm foothold. Though Huawei does have a North American branch headquartered in Plano, TX with a R&D office in Santa Clara, CA – along with other smaller offices doting the US – its business activities has been restricted.

Over the years, Huawei has been forced to abandon its plan to expand in the US as well as acquiring technologies within the US. Huawei had a chance to buy 3Leaf and 3 Com – two ICT companies with ICT network technologies and roots in the US – and was denied the right to buy them owing to security concerns. This was noted as a tried and noted tactics of Chinese intelligence gathering through proxies like Huawei. Huawei was also recently denied the right to bid on a national emergency network contract with Nextel.

Lastly, there is the danger perceived in joint ventures between Huawei and Symantec, called Huawei Symantec, which Kralek et al. deemed to be a serious national security risk in their 2012 report to the USCC on Chinese cyber operations and capabilities. The objection can be best summed up by the following description from the report:

> Collaboration between U.S. and Chinese information security firms, while not common to date, has raised concerns over the potential for illicit access to sensitive network vulnerability data at a time when the volume of reporting about Chinese computer network exploitation activities directed against U.S. commercial and government entities remains steady.[40]

It was not, therefore, surprising to find out that with Symantec was abandoned after concerns arose about the intentions that Huawei had with security software. After being denied the right to buy 3Leaf, Huawei's Deputy Chairman – Ken Hu – published an open letter to the US Government to clarify its security concerns and to limit the public relations damage done by the

public rebuff of Huawei. He noted that Huawei has never been guilty of violating the national security laws of any country that it has done business in and that the rumors that Huawei's equipment allowed the Chinese Government to spy on countries that used Huawei's equipment and/or services was due to a malicious spread by Huawei's rivals. No evidence has be put in public to prove it one way or the other than the USCC reports, which can only mean that it's due to US concern over China's rise and its cyber espionage operations. This is speculation, but what is clear is that Huawei has been denied on all its attempts to deepen its connections to the US market in any significant way.

Though Huawei's fortunes in the US have been dismal, things may turn for an even worse course. Beyond the troubles that Huawei has encountered in its attempt to enter the US market, it's also facing a Congressional investigation instigated by Chairman Mike Rogers and the HSPCI regarding "the threat posed to our nation's security and critical infrastructure by the expansion of Chinese-owned telecommunications companies – including Huawei and ZTE – into [the US] telecommunications infrastructure." At present, the investigation is still in the initial stages as no official findings or developments from the investigation have been published beyond a preliminary review commissioned by Chairman Rogers. This development – while unresolved – doesn't appear to bode well for Huawei as the language used by Rogers and his committee have shown grave concerns about the security liability presented by the presence of Huawei and its bids to get into the US market.

During this same time Symantec – one of the largest information security firms in the world – sold its fifty percent stake in Huawei Symantec – the Hong Kong-based information security

joint venture that Symantec started with Huawei to market storage, security, and network products. Symantec has denied that this decision was politically motivated. But the USCC's 2012 report on "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Huawei and Chinese attempts to enter co-opts was cited as a strong case for concern; hence there seems to be a very timely withdrawal by Symantec, who does business with the US government, as it seems to be a tactic to distance itself from Huawei – though certain IPR will remain in Huawei Symantec as it goes forward under Huawei's governance. Like the other failings, this one was also due to security concerns – as access to cyber security program coding is of interest to China for its own needs m but also for national security purposes. Like the Indian Ban, not much is known about the precise reasoning and timing of this failing, but one can speculate that Symantec wished to avoid losing its economic interests after it was informed that the US government was concerned about its co-opt with Huawei.

The US experience for Huawei was – like the Indian experience – fret with concern raised on the pretext of cyber security concerns and colored by national tensions between the two states over China's rise as a global power and economic competitor. But it seems to run deeper as the problem is that grave for the US as shown by its frequent victimhood as a target of cyber-attacks traced back to China and the research provided by the USCC and its contractors. There has been no clear evidence of the allegations made by either India or the US, but it is likely due to the sensitive nature of the issue that prevents public disclosure of such findings.

In spite of the "image problem", Huawei doesn't seem to be discouraged from deepening its roots in the US as it has increased its presence and investment in North America. In an interview with *Fortune*, John Roese, general manager of Huawei's North American R&D division, said that Huawei has been pursuing a strategy of "innovation" and

In response to a general question about Huawei's "legal issues" – which is another way of referring to the security concerns raised by US lawmakers – Mr. Roese stated that:

> There is a historical perspective and maybe even a biased and uninformed perspective of who Huawei is and what we do. We're now beginning to communicate our role around innovation. You can hear all of the noise, it's loud and very disruptive, but on the other side you start to hear a story about innovation…If someone were to try and protect the US market from foreign technology none of us would have a cellular network. We wouldn't be able to build these infrastructures because these infrastructures come from global companies…But we're very patient in the U.S. Even if you don't like us, at some point if the best technology and the best innovation is coming from Huawei, eventually it becomes a competitive disadvantage for your country to avoid it. We are just another global entity. We are just like any of the global entities that you know of. You just don't know us that well.

In other words, Huawei intends to stick to the story that they are just being misunderstood and being unfairly treated due to protectionist feelings in the US Government.

4.3 The Chilling Effect of Economic Cyber Deterrence

When Huawei was rebuffed again (case here?), its President noted that this course has a "chilling effect" on Huawei's ability to operate in the US – which seems to be the case for other Chinese companies in the ICT industry as well. Prominent among these currently unaffected companies – insofar as they have not been singled out – is ZTE. The list of potentially target companies includes Tencent and a number of smaller Chinese companies.

ZTE and a select group of Chinese ICT companies with business in the US have also be identified as potential sources of insecurity. They are all involved in the GICTSC and the business of selling telecommunication goods. Tencent, unlike the other target companies, doesn't have any notable economic interests in the US or global markets, as of now, but it has been connected to China's cyber espionage operations. In a recent report, Trend Micro

The effect of PECD may, however, change over the next few years as the HPSCI has started an investigation into Huawei and ZTE "to review the threat posed to U.S. national security interests by telecommunications companies with potential ties to the Chinese government [like Huawei and ZTE]."[41] The HPSCI's investigation has not made any substantive findings thus far as it has remained in the exploratory phase thus far. The Committee has met with the heads of Huawei and ZTE on a number of occasions during 2012 to privately discuss these issues. The Committee has also sent these executives letters requesting specific information regarding their relationship with the Chinese Government that would – in theory – tell the world whether or not Huawei or ZTE has consciously facilitated China's cyber operations.[42] The main objectives of the inquiry appear to be:

- Determining the degree to which the Chinese Government influences the conduct of the two companies.
- Finding out how far the two companies have succeeded in penetrating the US and Global markets with their products and services.
- Ascertaining the economic practices of the two companies in terms of how they compete for business in the US and around the world

These objectives are discernible based on an examination of the letters sent to the executives of Huawei and ZTE. The final outcome of this investigation is not yet clear as the response to these requests have not yet been made public and the investigation is not yet considered finished.

4.4 The Impact of Economic Cyber Deterrence

Given the "chilling effect" of PECD on Chinese "national champions" there is little doubt that the Chinese Government in Beijing will see this policy as a significant detriment to their long-term strategic economic goals as their economic strategy for the foreseeable future – especially when one considers China's plan to become a knowledge-based economy through the "informationization" of its economic infrastructure and paradigm that involves shifting away from a mechanized industrial economy based on exporting manufactured goods.

4.4.1 China's Flawed Economic Development Plan

China's long term economic goal for 2030, according to the World Bank and the Development Research Center of the State Council, is to become a "Modern, Harmonious, and Creative High-Income Society" by making social reform and also by encouraging and acquiring indigenous high-tech companies producing high end goods, in sectors like ICT, and similar areas as part of its broader plans. This leaves China open to pressure on the economic front as the growth of indigenous innovative forces are marked as crucial in the eyes of state planners.[43]

The first thing we must consider is the context of the Chinese strategy. To date, the extraordinary economic growth and prosperity that China has enjoyed since its historic shift from being a command economy to a market-oriented economy has largely been derived from the friendly investment business environment created by the national government in Beijing – through monetary, industrial, and financial policies – and the abundance of cheap labor in China, ample sources of raw materials provided by the global market, and practice of state capitalism – which is used by the government sustain China's economic growth by utilizing its power to directly

shape the economic path that it takes.[3] During its first transformation into a market-based economy – which started in 1978 – China utilized its greatest – but underused – economic characteristics to build its economy into the leading industrial state by becoming the world's largest exporter by 2010. These characteristics are: (1) China's abundance of low-cost labor; (2) China's market institutions; and (3) China's ability to modernize its technological capacity on a national level.[4] In short, China has been living on its success in becoming "the world's factory" by becoming the number one exporter in the world in 2010 after modernizing for some 22 odd years.[5] This success would not last as China's growth would require changes to the plan that would set the goal of becoming a knowledge-based economy.

The economic reforms that started after 1978 – after the death of Mao – ensured progress in generating growth and lifting living standards in China; but Chinese society remained vulnerable to the side effects of transition in the late 1980s. The social unrest experienced in China in 1989 in Tiananmen Square was a key factor in China's success as well – though it's not recognized by the Chinese Government – that is recognized by scholars who note that the uneven growth and socioeconomic tensions from transitioning from a command model to a market model caused grievances to arise over the lack job creation for the generation of college students coming out after the reform efforts of Deng Xiaoping and the workers at the state-operated enterprises suf-

---

[3] World Bank and Development Research Center of the State Council of the People's Republic of China, "China 2030: Building a Modern, Harmonious, Creative, and High-Income Society," World Bank, http://www.worldbank.org/content/dam/Worldbank/document/China-2030-complete.pdf [Accessed February 28, 2012], 3-14.

[4] Gregory Chow, Interpreting China's Economy [Princeton, NJ: World Scientific Publishing Co., 2010], 41-46; Barry Naughton, The Chinese Economy: Transitions and Growth [Cambridge, MA: MIT Press, 2007], 148-156.

[5] Ibid., 88-110; Associated Press, "China Becomes World's No. 1 Exporter," *Associated Press*, http://www.nytimes.com/2010/01/11/business/global/11chinatrade.html [Accessed February 28, 2012]. Ibid., 88-110.

fered due to slow economic reforms.[6] The liberalization the followed would be influenced by the rising influence of ICT – a trend that had caught on while China was transitioning in the 1980s.[7] More recently, China's economy has slowed down due to slowing global economy that has coincided with the fact that labor in China's heavily industrialized east coast has become more costly than what foreign investors are used to and more scarce.[8] The cost of wages in China had been on the rise since 2005 and has finally reached – according to a number of economists – the Lewis Turning Point – a condition that economist understand as a economic phenomenon that happens when:

> [A] society [like China] moves from an agricultural to an industrial economy, the balance of labor demand and supply shifts as well. In the initial stage of development, most people remain in rural areas, engaged in agricultural production. When this concentration of workers leads to underemployment in rural areas, the industrial sector can expand and increase its labor force with no pressure to raise wages. Thus there may follow a period of industrial growth with no rise in real wages. However, as the industrial sector develops to the point where the supply of labor from the agricultural sector becomes limited, industrial wages begin to rise quickly.[9]

---

6 Naughton, 98-100; Elizabeth Economy, Perry Link, Adam Segal, Cheng Li, Orville Schell, and Michael Anti, "Tiananmen Square and Two Chinas," Council on Foreign Relations, http://www.cfr.org/china/tiananmen-square-two-chinas/p19544 [Accessed December 1, 2011].

7 Jiang, "Report on an Inspection Tour of the US and Canadian Electronics Industries" in *On the Development of China's Information Technology Industry*, 59-72; Jiang, "Revitalizing Our Country's Electronic Industry" in *On the Development of China's Information Technology Industry*, 73-83; Jiang, "Gradually Explore a Chinese Style Development Path for the Electronics Industry" in *On the Development of China's Information Technology Industry* 85-112. As the Minister of Electronics Industry during the 1980s, Jiang was witness to the rise of ICT in the West and the rest of the world and recognized the need to have China's economy to utilize it as a means of modernizing China's backward economy through the development of China's own ICT industry and infrastructure to ensure that China would be competitive and economically successful in relative terms with the rest of the world during the global information revolution.

8 Kam Wing Chan, "A China Paradox: Migrant Labor Shortage amidst Rural Labor Supply Abundance," Eurasian Geography and Economics, 2010, 51, No. 4, pp. 513–530; Xiaobo Zhang, Jin Yang and Shenglin Wang, "China Has Reached the Lewis Turning Point," IFPRI, http://www.ifpri.org/sites/default/files/publications/ifpridp00977.pdf [Accessed November 14, 2011]; The Economist, "The end of cheap China What do soaring Chinese wages mean for global manufacturing?," *The Economist*, http://www.economist.com/node/21549956 [Accessed March 10, 2012]; Jamil Anderlini, "Chinese economy slows more than expected," *Financial Times*, http://www.ft.com/intl/cms/s/0/df83ef06-698c-11e1-9618-00144feabdc0.html?ftcamp=published_links/rss/world/feed//product#axzz1oroV3dF0 [Accessed March 9, 2012].

9 Zhang, Yang, and Wang, 1-5.

This conclusion was reached due to the uneven growth between the urban areas and rural areas of China in terms of pay and capacity to produce. The paradox is that there are skilled workers ready to work in the urban areas – despite being scarce in supply and at higher cost than their rural counterparts – but there is the lower cost of rural workers – which owes their low-cost due to their abundance in supply – which has the problem of being not as skilled as the urban workers with skills.[10] This has contributed to a problem of having a irregularity of labor shortages that shakes the confidence of investors and observers as a steady labor force is what is expected by most stakeholders.[11] The challenge in on a macroeconomic level would ultimately be a test of whether or not China could keep up with the rest of the world and meet its own challenges by utilizing the driver of development that would emerge in the 1990s as being a central: ICT – the thing that would drive the global information revolution. The importance of ICT for China's economic development came – according to the World Bank in 2002 – from the fact that China faced the following challenges to become a knowledge-based economy: (1) provide employment for a workforce of 700 million workers while dealing with labor shortages in its major industrial regions; (2) contend with labor unrest in its major industrial regions; (3) sustain high economic growth on a macroeconomic level; (4) increase the income per capita of ordinary citizens; and (5) protect the environment.[12] These challenges required that China have an economy that remained up to date with ICT technologies to build it as it had the potential to do all of these things and more for China's standing and need for internal stability.

---

[10] The Economist, "The end of cheap China What do soaring Chinese wages mean for global manufacturing?."

[11] Chan, 520-30.

[12] Carl Dahlman and Jean-Eric Aubert, *China and the Knowledge Economy : Seizing the 21st Century* [Washingotn DC: World Bank, 2002], 11-43.

As an emerging market-oriented Communist government within a globalized world economy – with a restless population and a strong interest in creating sustainable economic growth – Beijing was not been satisfied by resting on its considerable laurels. The growth that had provided growth from the early 1990s to the mid-2000s would eventually dry up due to rising costs of labor in China – and alternative labor markets in Southeast Asia with lower costs – and rising tensions among the industrial working class and college educated members of Chinese society. The decision to pursue the path of becoming a knowledge-based economy has been supported by all prognostics about the general pursuit of economic development in the 21st Century. The first issue was one of trends for development – which emerged in the 1990s. The World Bank explained it best in its World Development Report for 1998-1999 – which was incidentally entitled "Knowledge for Development" – when it said:

> For countries in the vanguard of the world economy; the balance between knowledge and resources has shifted far towards the former that knowledge has become perhaps the most important factor determining the standard of living – more than land, than tools, than labor. Today's most technologically advanced economies are truly knowledge-based… The need for developing countries to increase their capacity to use knowledge cannot be overstated. Some are catching on, developing national knowledge strategies, and catching up…Countries that postpone these tasks will fall behind those that move faster, and the unhappy consequences for their development prospects will be hard to remedy.[13]

The development of information and communication technology (ICT) within each developing state's economy is recognized as primary element in economic development in the 21st Century – which was echoed in the outlook reports put forward by the European Commission and United Nations Development Programme (UNDP) and aptly called ICT for development (ICT4D).[14]

---

[13] World Bank, World Development Report: Knowledge for Development, 1998-99 [Washington DC: Oxford University Press, 1999], 16-17.

[14] United Nations Development Progamme, "Human Development Report, 2001", United Nations Development Programme, http://hdr.undp.org/en/media/completenew1.pdf [Accessed February 1, 2012]; European Commission, *The Information Society and Development: A Review of the EC's Experience in Asia, Latin America and the Mediterranean* [Brussels: European Commission, 2001], 36-38.

The two principle features of technology – according to the UNDP – are: (1) it can directly enhance human capabilities and (2) technological innovation is a means to human development because of its impact on economic growth through the productivity gains it generates (See Figure 1).[15] ICT in particular – according to the OECD – has three distinct impacts on a country's economic growth and development:

> First, as a capital good, investment in ICT contributes to overall capital deepening and therefore helps raise labour productivity. Second, rapid technological progress in the production of ICT goods and services may contribute to more rapid multifactor productivity (MFP) growth in the ICT-producing sector. And third, greater use of ICT may help firms increase their overall efficiency, and thus raise MFP. Greater use of ICT may also contribute to network effects, such as lower transaction costs and more rapid innovation, which will improve the overall efficiency of the economy, i.e. MFP. These effects can be measured and examined at different levels of aggregation, i.e. at the macro-economic level, the sectoral or industry level, and the firm level.[16]

In other words, ICT contributes to the level of investment, labor productivity, efficiency of economic inputs and outputs, and the national income of countries that incorporate them into their economy.[17] What is notable about the impact of ICT is the effect that it has on the MFP of any given country in the developed world – which according to the US Bureau of Labor Statistics (BLS) will have the effect of granting that country the "ability to produce more with the same or

---

[15] Ibid; Sadayoshi Takaya, "The Evolution of ICT, Economic Development, and the Digitally-Divided Society" in Information Technology an Economic Development, Ed. Yutaka Kurihara, Sadayoshi Takaya, Hisashi Harui, and Hiroshi Kamae [New York: Information Science Reference, 2008], 1-10.

[16] US Bureau of Labor Statistics, "Multifactor Productivity," US Bureau of Labor Statistics, http://www.bls.gov/mfp/ [Accessed February 1, 2012]. The BLS says: "MFP measures reflect output per unit of a set of combined inputs. A change in MFP reflects the change in output that cannot be accounted for by the change in combined inputs. As a result, MFP measures reflect the joint effects of many factors including research and development (R&D), new technologies, economies of scale, managerial skill, and changes in the organization of production."

[17] OECD, "The Economic Impact of ICT: Measurement, Evidence, and Implications," http://browse.oecdbookshop.org/oecd/pdfs/free/9204051e.pdfl [Accessed February 1, 2012], 8-9; Utz Dornberger, Luis Bernal Vera, and Alejandro Sosa Norena, "The Influence of New Information and Communication Technology on Transaction Costs of Micro-, Small-, and Medium-Sized Enterprises" in *Information Technology and Economic Development*, Ed. Yutaka Kurihara, Sadayoshi Takaya, Hisashi Harui, and Hiroshi Kamae [New York: Information Science Reference, 2008], 165-172; Jianxiong Liu, Zhengming Xiao, Chabioa You, and Yufei Wu, "Application of Computer Technology in Mechanical Industry of China" in *Information Technology and Economic Development*, Ed. Yutaka Kurihara, Sadayoshi Takaya, Hisashi Harui, and Hiroshi Kamae [New York: Information Science Reference, 2008], 226-232.

less input" and improve the real hourly earnings while "not by requiring a proportional increase of labor time, but by making production more efficient" and subsequently improve the income of workers in the ICT industry.[18] This is especially convenient for China as its underdeveloped ICT infrastructure gave it an advantage for the 21st century as the investments and growth in its ICT industry and infrastructure would be based on up-to-date technology unlike that of more developed nations whose ICT required revamping or updating existing technology at a substantially higher cost.[19] Furthermore, OECD countries invested heavily in improving the ICT industry and infrastructure in their respective economies – while updating their existing ICT assets – and effectively setting the trend for development. To sum up, ICT provides a means of solving China's problems with its ability to foster internal stability by providing means of creating a knowledge-based economy whose feature would likely include lower rates of unemployment, improved levels of income, dynamic capacity to deal with labor shortages and need for sustainable growth – which may have some variance due to the characteristics of the country where ICT is used as a means of economic development. It's therefore not surprising that the strategy adopted by the Chinese – for the purposes of using ICT to transform the Chinese economy into a knowledge-based one – is uniquely suited to the conditions in China and also notable for the shortcomings that has emerged in the implementation of this strategy.

Next we must consider the strategy that China pursued in detail. China's strategy for transforming its economy has been an evolving one with an initial template based on China's need for sustainable economic growth and development to maintain internal socioeconomic stability as observers of China have noted the speed of economic reforms and subsequent growth after the Chi-

[18] Ibid; US Bureau of Labor Statistics, "Multifactor Productivity Frequently Asked Questions," http://www.bls.gov/mfp/mprfaq.htm#Q01 [Accessed February 1, 2012], 8-9.
[19] Dai, 10-12.

nese Government effectively suppressed the student demonstrators in Tiananmen Square whose grievances stemmed from the imbalances caused by a slow transition from a socialist economy to a market-based economy – which caused uneven growth and tensions in China's workforce. The changes made to the strategy – since the strategy took shape in the early 1990s – have responded to the increasingly apparent benefit of ICT as a source of economic growth as a general purpose technology (GPT) that promotes innovation and development infrastructure that help to promote the emergence of a knowledge-based economy. What has not changed is the fact that China has remained an export-oriented economy that relies on its industrial capacity.

In a nutshell, the Chinese strategy for transforming the economy has been to use the power of the state to aid the "pillar" industries of China – including ICT among others – while maintaining its role as the leading industrial power in the world while implementing reforms that help to "informationize" the Chinese economy so that it can gradually transform into a knowledge-based economy that relies on innovation and ideas to generate growth as opposed to relying on low-cost labor. This transformation is defined by the distinctive features of "informationization" – which Christine Zhen-Wei Qiang of the World Bank, defines as "the ICT-driven transformation of an economy and society – a complex development process in which a country increases its capacity to exchange and apply information and, in turn, generate knowledge."[20] As such the Chinese response to the economic development trends – as seen in the previous section – was to pursue a dual track strategy of "informationization" and industrialization that was called the "Informationization of the National Economy" (INE) Program – which was later incorporated into

[20] Christine Zhen-Wei Qiang, China's Information Revolution: Managing the Economic and Social Transformation [Washington, DC: World Bank, 2007], 11-12.

the Tenth Five-Year Plan for China's economic development between 2001-2005.[21] This program has several priorities:

- Build up China's ICT infrastructure by expanding access to the internet, mobile phones and landlines, computers, and other ICT technologies that allow for an efficient distribution of information
- Build up China's ICT industry so that it can
- Create an ICT workforce that utilizes ICT for innovation through education
- Create new technology for China's modernization and for export purposes and to improve the MFP of the industrial processes of China
- To create a full employment ICT workforce that can manufacture the ICT products needed to maintain high GDP growth via export and modernize the ICT infrastructure

Though it may seem daunting, it's something that China has always been working to obtain. It should be noted that the pursuit of high-technology is not a new venture for China as during the Cold War, "despite being a low-income country, pursued a high-technology effort strategy" in order to be competitive as a political power in the world through the development of the atomic bomb, intercontinental ballistic missiles, and industrial production technology.[22] The point of doing these measures is to start the developmental phase of "informationizaiton", which Qiang notes is a three phase process including:[23]

1) Phase One – Build ICT infrastructure and acquire technology in a decentralized manner between the state and private sectors and within civil society

---

[21] Xiudian Dai, "ICTs in China's Development Strategy" in China and the Internet: Politics of the Digital Leap Forward, ed. Christopher Hughes and Gudrun Wacker [New York: Routledge, 2003] 8-11.
[22] Naughton, 353-354.
[23] Qiang, 12-15.

2) Phase Two – ICT development strategy begins to become a unified process between the three sectors of the nation by cooperation
3) Phase Three – The social and economic structure become transformed due to the level of cooperation reached

Thus far, the Chinese economy and society remains firmly within Phase One – as most countries pursuing "informationizaiton" are – with a great deal of progress to be made – as shown in the next section – along with some shortcomings in the pursuit of "informationization." It's clear however that China will be actively pursuing this path given its support for the development of ICT as it has undertaken the policy of raising "national champions" through policies and public capital – which will be explained in more detail in the Huawei case. The impact of PECD is that the negative publicity will cost money in terms of contracts and a bad image will hinder the growth of companies like Huawei. The continued growth and expansion of PECD could multiply the effect what has happened thus far.

4.4.2 China's Response via Official Protest and Media

After Huawei was denied the right to bid, Huawei vigorously protested the move and made a concerted effort to change its image – including an offer to have the US Government investigate its background as noted earlier. These frustrations have been reflected in the official newspapers in China, all of whom have bemoaned the US policy as being unfair and hurtful to the public image of Huawei. Though these words of protest are not coming from a government official, one can reasonably say that they are indirect protests from the Chinese Government. However, it's well-known that both *The People's Daily* and *The Global Times* are both owned by the Chinese

Communist Party, who uses the two papers as platforms to informally express their position on sensitive issues.[44]

The Chinese Government has remained largely silent during previous rebuffs of Huawei, but it became apparent that this was a notable concern when the Australian ban was on the table. In what seems to be the most vocal protest of actions done to "setback" the "national champions" of China, the Ministry of Commerce issued a statement that stated:[45]

> [T]he rejection by Australia was beneath impartiality and China is deeply concerned about it…[A]ccording to our information, Huawei has provided broadband network equipment and service to many countries. Huawei Australia, which participated in the tenders, is a company that has a staff of whom 90% are Australian citizens, and that are doing business in Australia for nearly ten years without any bad record. Australia has no reason to reject an enterprise in fair competition in pretext of security, when there is no fact of evidence… China and Australia have signed bilateral investment protection agreement, and bilateral trade and economic cooperation has been developing well these years. China and Australia should adopt an open, cooperative and constructive attitude, and create an impartial market environment without discrimination for enterprises of the two countries in carrying out trade and investment, so as to promote the healthy development of China-Australia trade and economic cooperation.

No further public actions have been taken as of July 2011 by the Chinese Government in regards to the restrictions placed on Huawei. The tone taken by the Chinese official media informs us that the Chinese are quite serious about the economic pressures place by PECD measures and even more so with the official statement from the Ministry of Commerce, but given that the Ministry of Foreign Affairs has yet to issue any official statement in public. One can only speculate that PECD has gotten the attention of the Chinese government, but has not yet become serious enough that Beijing feels an absolute need to act. The one thing that may prod the Chinese to act in favor of US interest in cybersecurity and the ultimate goal of PECD is the creation of a broad coalition based on this nascent policy's provisions.

4.5 The Legality of Economic Cyber Deterrence

The legality of the core components of the US Policy of Economic Cyber Deterrence is matter that needs to be addressed in light of criticism of "unfair" treatment by the Chinese media and the Chinese Ministry of Commerce. National security concerns serves as a legitimate basis for restricting bilateral economic interaction, according to the World Trade Organization, so long as the imposes requirements are applied in a transparent manner and under review by a panel. The current international regime governing trade or economic restrictions, like those imposed by PECD, seems to be permissive and supports the use of national security. The same seems to apply when examining existing US laws governing trade with national security as a factor.

4.5.1 International Norms

Under international legal norms, there are two unique provisions that support the use of national security as a pretext for imposing economic restrictions on economic dealings among nations. First, under Article 2.2 of the Agreement on Technical Barriers to Trade states:[46]

> Members shall ensure that technical regulations are not prepared, adopted or applied with a view to or with the effect of creating unnecessary obstacles to international trade. For this purpose, technical regulations shall not be more trade-restrictive than necessary to fulfill a legitimate objective, taking account of the risks non-fulfillment would create. Such legitimate objectives are, *inter alia:* national security requirements; the prevention of deceptive practices; protection of human health or safety, animal or plant life or health, or the environment. In assessing such risks, relevant elements of consideration are, *inter alia:* available scientific and technical information related processing technology or intended end-uses of products.

In short, the use of "national security requirements" as the basis for implementing the policy is on legitimate grounds in technical trade barriers being put in place by PECD. This provision provides latitude to national governments regarding its explicit statement regarding the use of

national security concerns, but is conditional as the Agreement on Technical Barriers to Trade also notes that limits restrictions for legitimate purposes, which include:[47]

- protection of life/health (human, animal and plant)
- safety (human),
- protection of national security,
- protection of the environment, and
- prevention of deceptive marketing practices.

PECD is justified in that almost all of these exceptions can be used to defend this new US policy. Cybersecurity is a vital national security issue and unsafe or tainted goods goes against good marketing practices.

Second, GATT Article XXI explicitly states that:[48]

> Nothing in this Agreement shall be construed:
> (a) to require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests; or
> (b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests
> (i) relating to fissionable materials or the materials from which they are derived;
> (ii) relating to the traffic in arms, ammunition and implements of war and such traffic in other goods and materials as is carried on directly for the purpose of supplying a military establishment;
> (iii) taken in time of war or other emergency in international relations; or
> (c) to prevent any contracting party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.

Since the adoption of GATT, only four cases where Article XXI has been invoked and reached a panel for review. In these case, it is shown that there is a strong probability of policies like PECD being reviewed if a complaint is brought up by the complaining party – which would be China in this case – and may be rejected. If the US should make cybersecurity a major national security issue through a declaratory policy explaining the nature of its concern about cyber-attacks and insecurity in the GICTSC, there may be grounds for PECD to continue. At this point the

feasibility in the international sphere is uncertain, but promising to a degree given that PECD could be construed as a reasonable protection if stated clearly and publicly.[49]

4.5.2 US Laws

The critics of PECD have dubbed its underlying policy actions "protectionist" and implying that it's an unfair practice. Upon closer examination of the current laws and practices governing the US Government's economic policies, PECD is most likely on solid ground given the leeway given to national governments on the grounds of "national security" as a basis for imposing trade barriers and other economic measures restricting the operations of Chinese companies. This section will attempt to illustrate a possible legal justification for PECD; it does not purport to be a comprehensive brief on how the US Government might justify this emergent policy as the research done for this section can only be considered. When one examines US Laws governing international trade – in particular those concerning foreign investment and capacity to operate in the US – there is support to be found for allowing the PECD to be implemented in conjunction with GATT. First, there's the Exon-Florio Amendment (Exon-Florio) to the Defense Production Act of 1950. Second, there's the Foreign Investment and National Security Act of 2007 (FINSA). Together, these two laws provide primary basis of legislation that give the US Government the prerogative to carry out PECD.

The purpose and function of FINSA is to build upon Exon-Florio by doing the following things:[50]

- Heightening the scrutiny of any transaction where a foreign government or an entity controlled by a foreign government is a party, or whenever a transaction would result in the foreign control of "critical infrastructure."
- Defining "critical infrastructure" broadly to include "systems or assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems

or assets would have a debilitating impact on national security." This definition expands the types of transactions subject to CFIUS review to include energy generation and transportation.

- Including an "evergreen" provision. Under the new law, if the investigation of a transaction results in a mitigation agreement, and at some later date, a party to the mitigation agreement intentionally commits a material breach of the agreement, either CFIUS or the President may reopen the review if "there are no other remedies or enforcement tools available to address such breach." A reopened review can result in additional mitigation agreements or even the unwinding of the transaction. Previously, CFIUS could reopen a review only when it discovered a material omission or misstatement by one or more of the parties to the transaction made during the initial review period.
- Codifying the role of CFIUS in the review process.
- Designating a lead agency, depending on subject matter expertise, to review each transaction. The lead agency is granted the authority to negotiate, monitor, modify, and enforce mitigation agreements.
- Appointing the director of national intelligence as an ex officio member of CFIUS. The director must perform a national security threat analysis for all proposed transactions.
- Requiring a full 45-day review for transactions by companies owned or controlled by foreign governments unless the treasury secretary or deputy and the head of the lead agency determine that the transaction will not impair national security.
- Increasing the role of congressional oversight by requiring CFIUS to provide an annual report to Congress as well as a certified notice to Congress specifying its determinations, decision-making rationales, and actions taken.

In essence, FINSA gives the US Government – in particular Congress and CFIUS – broader powers and explicitly control foreign acquisition of US companies especially those considered vital to US national security. Based on the facts garnered from the legal perspective, the lawful justification for PECD can be made by citing WTO rules and GATT Article XXI as the basis for using national security as a justification for taking economic restrictions on trade relations – while being conscious that the WTO may not see the "threat" the same way given the past record of this defense. Meanwhile, Exon-Florio and FINSA allows the US to continue implementing PECD, with or without backing from the WTO. But in the end the important thing to note is that the initial look at the legal view of PECD seems largely justified as US interests are clear in the economic and political angle for needing to protect the GICTSC and critical infrastructure.

4.6 Diplomacy in PECD

The US approach – through PECD – seems to have traction among US allies and partners as India and Australia have both demonstrated both the political awareness and will to implement similar policies. This section examines the use of diplomacy in US-China cyber relations as well as other angles to illustrate current initiatives in the area of diplomacy for the cyberspace domain.

4.6.1 The Cyber Red Phone for Russia and the US

In December, 2011, it was reveal that the US and Russia had concluded a bilateral agreement that, among other things, set up a emergency line of communication between Washington DC and Moscow to quickly resolve international emergencies for "technical threats" including emergencies that take place in cyberspace.[51] Little is know about the exact nature of the agreement as it has yet to take effect and the details have not been released based on a search through open sources. This story is mentioned because the tensions caused by cyber attacks are likely to continue and the top leaders in both states – the US and China - have a stake in resolving potential emergencies arising from cyber operations conducted by either side. More research on this issue could help further cyber norms of managing cyber emergencies and affecting cyber relations among the active nation-states in cyberspace.

4.6.2 Working Toward Cyber Norms with China

The issues of cyber espionage and cyberwarfare, as matters of international relations, have largely remained a gray area for most, if not all nation-states, given the lack of norms for operating in cyberspace. Track II diplomacy has been going on for the last four of five years with talks be-

tween the Center for Strategic and International Studies (CSIS) and China Institutes of Contemporary International Relations (CICIR) to better promote relations in cyber related issues.

As of June 2012, the Track II talks between CICIR and CSIS are currently stalled due to a fundamental and shared mistrust between the participants about each other's motives and actions.[52] The US has raised the issues of industrial espionage through cyberspace and greater openness in how China operates in cyberspace, while the Chinese protest the US hegemony over the internet.[53] The Chinese have also protested the lack of recognition for the work of their National Computer Network Emergency Response Technical Team/Coordination Center of China (CN-CERT), US-CERT's Chinese counterpart, in contributing to global cybersecurity and criticizing the US for being silent on the proposal.

Other issues of disagreement include the following:[54]

- What's an act of war when it's done through cyberspace?
- Internet governance dominated by US control of major bodies controlling or managing the internet.
- Attribution seen as a major source of disagreement on standards.

At present, the Track II talks between the US and China on cyber issues is not the most pressing concern for either government given the more pressing issues of disputes in the real world. These talks will definitely need more time or pressure from the participants (either side) to force a change and get past the impasses that have arisen. The important thing is that there is a open channel for discussion of the controversial issue of cybersecurity among nations. Future exploits or pressure from PECD could be helpful in moving these talks along as steam picks up with

more nations joining the collation for PECD to get cybercurity from talks with China to manage cyber activity construed as national threats.

5.0 Policy Implications

Given the current state and impact of PECD – as measured by the Chinese reaction to it – there will be no major public fallout or decisive changes in either US-China Relations or collective action on the part of the US and its allies and partners. We must consider the immediate problems that may stand in the way. This section seeks to briefly explore the existing problems and obstructive issues that may prevent or delay the settlement sought by PECD as the long term objective of this new policy.

5.1 Immediate Regional Security and Internal Problems

There are currently two pressing areas of concern for the US and China, which will likely delay and/or reduce the possibility of a mutually agreeable settlement on conduct in cyberspace and related security concerns regarding economic relations in the ICT sector. First, there is the pressing matter of territorial disputes between China and the Philippines, Vietnam, and Japan – all of whom are either an ally or partner of the US – that may very well threaten the regional security of a broad part of East and Southeast Asia.

5.1.1 Regional Security Problems

At present, there are several regional security issues in oceans surrounding China and US allies and partners in the Pacific Ocean, which demand more direct impact on the topics discussed by the US and China on issues of security.[55] This includes the brewing dispute over territorial disputes in the South China Sea between China and the Philippines and Vietnam over three chains of islands and islets that all three parties claim part of or all them – principally China –

and the US has become involved and may have real world or kinetic repercussions going forward as tensions remain high and escalation is a rising probability in conflict between the directly involved Asian countries. Both Japan and the Philippines have pushed for the US to have greater involvement and to supply them with the needed military equipment and political backing for their claims. The situation remains tense and conflict is a distinct possibility given exchanged remarks between the involved parties – including the US.[56]

5.1.2 Internal Problems

In 2012, China is facing the challenges of a once in a decade transition of national leadership on top of the most significant political scandal with the CCP since the end of the Cultural Revolution with the dramatic downfall of Bo Xilai, all of which make it unlikely for any major changes made to Chinese policy.[57] There is a great deal of uneasiness as there seems to be an internal shift of power among the factions within the Chinese Communist Party (CCP) with the current administration's faction taking the lead in dominating internal politics in China. Given the past history of political changes in balance of power from within during the Cultural Revolution and the other times when power changed hands, there doesn't seem to be a great deal of willingness or possibility of a deal or breakthrough coming on resolving US concerns on the Chinese cyber threat.[58]

5.2 Impact on US-China Relations

Within the broad context of the bilateral relationship, PECD is unlikely to be a major factor in shaping how the US and China approach their dealings with one another. The policy actions taken under PECD have not elicited any formal complaints or actions against the US from the Chinese Government with the exception of words of protest of unfairness in official Chinese news-

papers. Other than a statement of protest after Australia banned Huawei from bidding on its National Broadband Network, the Chinese Government has not shown any significant reaction toward the growing suspicions toward Huawei. This situation, however, may change depending on how PECD evolves over time. The Foreign Ministry has been silent on the issue and complaints have been confined to complaints in official media stories over the years since 2009.

5.3 US Relations with Allies and Partners

Being a non-military response, PECD has great appeal of a policy tool for the purposes of cyber deterrence – a matter which has broad interest among developed and developing states – that can be used to multiply the effect of what the US has done to further PECD. Many of America's allies and partners have become aware of the fact that China is a major cyber threat. Given that most of these nations – identified earlier – are developed or have a great deal invested in cybersecurity given their interdependence on cyberspace. One can only speculate that there would be interest in forming a coalition based on mutual coordination and discussion of how to go about pressuring China given individual dispositions of national leaders. Little is known outside the concerns discussed earlier in this paper.

5.4 Progress in Track II Talks

The impact of PECD on the Track II talks will likely be limited, if not treated as a negative factor and given the current stalled state of these talks that will not produce the desired agreement for resolving mutual concerns at least in the short term. For now, the exact implications of implementing PECD are unknown, but it may not be much given the response from China thus fare it's not much to discuss as little has been revealed about the proceedings at the Track II talks. It is worth noting that the actual impact of these internal problems arose, the "expectations for a

breakthrough [on making headway on diplomatic talks regarding cyber security between the US and China were considered] low…[as p]rogress in the talks between the US and China has been glacial."[59] The only thing left is to consider how PECD evolves in the future given a possible expansion of this policy across the board with US allies and partners over time.

6.0 Conclusion

As a nascent policy, Economic Cyber Deterrence has a ways to go in terms of substantive development in becoming fully fledged policy. PECD has shown itself to be a set of policy options that may have broad appeal for the US to openly practice and for its allies and partners to adopt as a broadly coordinated multilateral policy that can prompt or motivate China to negotiate a settlement that reduces the cyber threat emanating from China and resolve mutual differences in the new domain of cyberspace. Therefore, further steps taken by the US to solidify the main components of this policy – by seeking to make PECD a coherent and more effective policy tool to achieve its strategic interests in reducing the Chinese cyber threat in terms of the degree to which its economic and state secrets are stolen and reducing the risk to fully tap into its apparent usefulness as a bargaining tool – as note in the policy recommendations below – but one can be certain of the underpinning facts surrounding the validity, potency, and in the matter at hand. The US and the world have a sound understanding of China's extensive cyber espionage activities and capabilities, international awareness and readiness to confront China on cyber security concerns, and the potent leverage that can be gained by employing the emerging Economic Cyber Deterrence – while noting that there are many shortcomings in bringing credibility given the unofficial nature of PECD as seen by the silence on the connectivity between the various policy action that underlies this nascent policy.

The paper will conclude with three parts. First, the major findings of the paper will be presented to recognize the limits and potential of PECD given the importance of cybersecurity in US-China relations and the need to improve PECD given the shortcomings or lack proper conditions for PECD to realize its potential. Second, a corresponding list of policy recommendations will be offered to remedy the shortcomings and strengthen PECD. Lastly, areas of further research will be examined to highlight a distinctive group of issues found and briefly examined, in this paper that will and should be critical to the story of PECD and how it will evolve in the future as each issue unfolds. By the end, it should be clear that this paper has thoroughly explored PECD as it stands and where it might go under ideal conditions to improve upon its effectiveness and

6.1 Synthesis of Findings on PECD

The policy of economic cyber deterrence remains a work in progress as the US ban and restrictions on major Chinese companies with suspected ties to China's cyber espionage activities – like Huawei and ZTE – remains an ongoing developments in US-China relations. Neither the Chinese nor the US has raised cyber espionage as an issue for bilateral relations – though both countries are engaging in diplomatic dialogue on this matter – this issue may remain under wraps for some time between the two states. Conversely, the policy of banning may bring the underlying issues to a head as China has become more vocal the issue of citing security concerns as a pretext for taking such drastic economic measures as other states – like Australia in particular – which is a strong sign that economic cyber deterrence may have a future as a means of pursuing US cybersecurity interests. This paper has shown that:

- PECD remains an unofficial policy in the US and among its allies and partners due to internal politics, the asymmetric nature of cyberwarfare, and the insufficient information on the exact nature of the Chinese cyber threat from its indigenous ICT companies.

- PECD can be effective given China's reaction to how this policy has been implemented, the role of high tech companies in China's economic development strategy to become a knowledge-based economy, and the real potential to extend PECD by coordinating similar policies with US allies an partners.
- There is some willingness among US allies and partners to implement PECD in some form as seen in the case of Australia and India, though domestic political considerations must be considered in the sustainability of such a mutual enterprise.
- By being a potent political tool for pressuring China – with reasonably strong legal foundation according to GATT and existing US laws – PECD stands as a means to produce a mutually agreed upon treaty that will establish a regime of a secured GICTSC through an affirmation of transparency and security in standard practices of ICT companies and reduce the threat of cyberwarfare by affirming limited use of techniques under this branch of warfare.
- Supply chain security will depend on a careful regime that promotes accountability in supply chain in promoting a public-private partnership that examines the making and shipping of all components in critical infrastructure sectors like telecommunications and others like power grids to guarantee safety.
- An agreement may happen in the long term, but not in the short term and will likely be limited in how much is verifiable given troubles with attribution and the current lack of readiness to address supply chain problems involving security vulnerabilities.
- Attribution is still a challenge and so is the options available to the US and others in countering the cyber threat.

6.2 Policy Recommendations

This paper has shown that US cyber deterrence has made significant progress in becoming more credible notion in terms what it stands to accomplish through economic pressure as PECD has undoubtedly shown itself to be an effective and viable means of achieving US interests and the overlapping interests in reducing the cyber threat from China. The goal of implementing and expanding PECD is, ultimately, to induce China into agreeing to sign a negotiated agreement that reduces the threat of Chinese cyber espionage, while easing restrictions on Chinese companies according to the reciprocation of US interests in reducing the cyber threat from both cyberspace and the GICTSC.

First, the US needs to issue a strong and coherent declaratory cyber deterrence policy that clearly states the US approach to acts of cyber espionage directed at its economic security to make US cyber deterrence more credible. In doing so, the US will have taken one of the most critical steps in implementing cyber deterrence, because this course serves to provide a clear interstate framework for how cyber relations will be conducted on terms informed by US national interests. Like the Cold War, cyber deterrence needs to be credible and well-structured to have the desired impact given that the deniability by the Chinese government is strong and that the US has been largely silent on the US in its official communications on cyberwarfare.

Second, the US needs to strengthen its cyber defense and capabilities for improving economic security and cyber deterrence by reducing America's vulnerability to cyber espionage. Despite the failure of the Cybersecurity Act of 2012, the issue of cybersecurity has taken a more prominent US national security issue. There needs to be more guidance on the US capacity to respond to the cyber threat from China and other nation-state actors in the cyberspace domain.

The priority should be setting up a clear line of communication and coordination between the public and private sector in addition to addressing supply chain security protocol for the Federal Government and US Military. A key part of cyber deterrence is to operate on a stable defensive footing in the domain of operations. Hence, it's necessary to address the major issues of cyber defense.

Third, the US should seek collaboration with its allies and partners to implement a global cyber deterrence strategy to make cyber espionage a costly and punitive enterprise for states that supports this type of activities. Given the shared concerns among the highly and reservedly concerned nations alike, it would be practical to seek the creation of a coalition of like-minded nations to multiply the effect of PECD – in its basic form – and thereby creating conditions that will pressure China to seek a negotiated settlement that will achieve the ultimate purpose of PECD. Australia shows that there is a reasonably strong possibility of creating a multilateral coalition of willing US allies and partners that will take up PECD in its basic form to create suitable conditions for the ultimate goal.

Fourth, the US should seek to resolve the attribution problems involved in determining the origins of cyber-attacks aimed at furthering China's economic cyber espionage activities to construct a basis for establishing international norms for operating in cyberspace. Though considerable work has been done in this arena – as seen in GhostNet and Shadows in the Cloud – there needs to be continued work on preparing for the fast pace of change in the cyber threats to the US. Hence resources should be appropriated in working toward improving and standardizing attribution investigations.

If these recommendations are pursued in good faith by US policymakers, the Chinese will eventually come to the table to reach a agreement on cyber conduct to achieve the ultimate goal of PECD. These recommendations are meant to be a short to long range goals that are all vital to the security of the US and friends as they represent the greatest flaws in PECD and the whole enterprise of cybersecurity today.

6.3 Further Research

Being an emerging policy, the Policy of Economic Cyber Deterrence has great potential and need to evolve, but there are many important components and related aspects that require further research as the information remains unavailable because the details of that particular issue remains largely classified or is undergoing certain processes. Therefore, it is necessary to follow up on these issues as they develop relative to one another and with the narrative illustrated in this paper.

The first issue is the question of the current HPSCI investigation into the cybersecurity and commercial practices of Huawei and ZTE and where it leads US policymakers on the issue of Chinese cyber operations. The response from the heads of the two companies will likely play a critical role in how PECD will be applied given the intelligence connections discovered or not discovered between these companies and Beijing. The second issue is the matter of willingness among US allies and partners, outside of Australia, to adopt a version of PECD as a part of a multilateral coalition working to coordinate cyber policy to induce China to negotiate on an agreement leading to greater cybersecurity in the US and elsewhere through a reduction of the cyber threat from the GICTSC and from cyberspace through progress made by the Track II talk

that may eventually leads tor formal talks for an agreement on norms of operating in cyberspace and security protocol for the GICTSC. The third issue is the process behind the bilateral agreement between the US and Russia that helped to create an emergency link between the two capitols. Very little details are known about this agreement other than the general information and function of this agreement and line of communication. The important thing to watch is how the agreement is drafted and how it has been implemented as it may provide clues on how the US can manage cybersecurity problems it has with China, while fully appreciating the fact that there will be differences in the outlook between Russia and China. Finally, there is the daunting task of exploring what it means to have a cyber treaty. There are many naysayers who argue that a cyber-treaty would largely be unenforceable and unrealistic given the speed at which the threat environment evolves and difficulty of verifying the adherence to any terms. The verifiable aspects – including the security of the GICTSC and attribution of major cyber campaigns – will be a focal point relative to the development of a safe supply chain and safer commons in cyberspace.

In following up on these topics, one will see whether or not PECD can be continued and expanded to multiply and prolong the effect of this nascent policy as these matters continue to evolve and change over time. The scale and impact of PECD as a policy will be decided by the findings of the investigation into Huawei and ZTE and the rest will inform how effective or ineffective PECD will ultimately turn out to be depending on the expansion of this policy among US allies and partners. The feasibility of a cyber-treaty is another issue of great importance in what is achieved through PECD given that there are limits to what can and cannot be verified by a written agreement.

Bibliography

Alperovitch, Dmitri. "Revealed: Operation Shady RAT." McAfee, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf [Accessed January 12, 2012].

Back, Aaron and James T. Areddy, "Hacking Probe Elevates Lanxiang School," *Wall Street Journal*, http://blogs.wsj.com/chinarealtime/2010/02/22/hacking-probe-elevates-lanxiang-school/tab/article/ [Accessed January 12, 2012].

Branigan, Tania. "Google attacks traced back to China, says US internet security firm," *The Guardian*, http://www.guardian.co.uk/technology/2010/jan/14/google-attacks-traced-china-verisign [Accessed January 12, 2012].

Borg, Scott. "Securing the Supply Chain for Electronic Equipment: A Strategy and Framework." The Internet Security Alliance, http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Securing%20the%20Supply%20Chain%20for%20Electronic%20Equipment.pdf [Accessed March 23, 2012].

Boyle, Rebecca. "Secret Cyber War Games Between U.S. and China Let Countries Role-Play Their Frustrations." *Popular Science*, http://www.popsci.com/technology/article/2012-04/cyber-war-games-between-us-and-china-let-countries-role-play-their-frustrations [Access April18, 2012].

Clarke, Richard. "How China Steals Our Secrets." *New York Times*, http://www.nytimes.com/2012/04/03/opinion/how-china-steals-our-secrets.html [April 1, 2012].

Clarke, Richard and Robert Knake. *Cyber War: The Next Threat to National Security and What to do About it*. New York: Harper Collins Publisher, 2010.

Grow, Brian and Mark Hosenball. "Special report: In cyberspy vs. cyberspy, China has the edge." Reuters, http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414 [Accessed March 30, 2012].

Hagestad II, William and James Mulvenon. "Chinese Information Warfare Event." The Potomac Institute, https://www.youtube.com/watch?v=h4qlHMJkbs8&feature=plcp [Accessed March 30, 2012].

Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." The Atlantic Council of the United States, http://www.acus.org/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF [Accessed March 23, 2012].

Healey, Jason. "The US Cyber Policy Reboot." The Atlantic Council of the United States, http://www.acus.org/files/publication_pdfs/403/041812_ACUS_CyberReboot.pdf [Accessed March 23, 2012].

Healey, Jason. "The Government's Four Cyber Silences." USCC, http://www.uscc.gov/hearings/2012hearings/written_testimonies/12_3_26/healey.pdf [Accessed March 23, 2012].

Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal for Strategic Studies*, http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss [Accessed March 23, 2012].

Knake, Robert. "Untangling Attribution: Moving to Accountability in Cyberspace." US House of Representatives, http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/071510_Knake.pdf [Accessed February 23, 2012].

Kramer, Franklin, Stuart Starr and Larry Wentz, *Cyberpower and National Security*. Washington DC: National Defense University Press, 2009.

Krekel, Bryan, George Bakos and Christopher Barnett. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation US-China Security and Economic Commission." US-China Security and Economic Commission, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf [Accessed January 30, 2012].

Krekel, Bryan, Patton Adams and George Bakos "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage." US-China Security and Economic Commission, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf [Accessed January 25, 2012].

Kugler, Richard. "Deterrence of Cyber Attacks." In *Cyberpower and National Security*, Edited by Franklin Kramer, Stuart Starr and Larry Wentz, 309-340. Washington DC: National Defense University Press, 2009.

Lebow, Edward. "The Foreign Investment and National Security Act of 2007." Haynes and Boon LLC, http://www.haynesboone.com/files/Publication/4722930e-9846-412f-a566-eceb8c6dc6c0/Presentation/PublicationAttachment/bf01cc5b-b7a8-4fbb-bd80-505fdc680f34/Lebow_CFIUS%20Article%20International%20Law%20News_01-2008.pdf [Accessed May 1, 2012].

Maloof, F. Michael. "China Tech Company Brags: We hacked U.S. Telecoms." World Net Daily, http://www.wnd.com/2012/06/china-tech-company-admits-hacking-u-s-telecoms/ [Accessed June 14, 2012].

Markoff, John and David Barboza, "2 China Schools Said to Be Tied to Online Attacks." *New York Times*, http://www.nytimes.com/2010/02/19/technology/19china.html?_r=1 [Accessed January 22, 2012].

Meet, Zulu. "DEFCON 17: PLA Information Warfare Development Timeline and Nodal Analysis." www.youtube.com, http://www.youtube.com/watch?v=kqzgL_XyLxs&feature=related [Accessed June 13, 2012].

Melvin, Jasmin. "Hopes fade for new U.S. cybersecurity law in 2012." *Reuters*, [Accessed August 2, 2012].

Menn, Joseph. "Agreement on cybersecurity 'badly needed'," Financial Times, http://www.ft.com/intl/cms/s/0/e595e568-f4dc-11e0-ba2d-00144feab49a.html#axzz1t7F2R4eF [Accessed March 29, 2012].

Ministry of Commerce People's Republic of China. "MOFCOM Spokesman Commented on Australia's Rejection of Huawei's Bidding for its National Broadband Network Project." Ministry of Commerce People's Republic of China, http://english.mofcom.gov.cn/aarticle/newsrelease/policyreleasing/201204/20120408064948.html [Accessed March 20, 2012].

Nakashima, Ellen. "In China, business travelers take extreme precautions to avoid cyber-espionage." *Washington Post*, http://www.washingtonpost.com/world/national-

security/in-china-business-travelers-take-extreme-precautions-to-avoid-cyber-espionage/2011/09/20/gIQAM6cR0K_story.html [Accessed March 1, 2012].

Nakashima, Ellen. "In U.S.-Russia deal, nuclear communication system may be used for cybersecurity." *Washington Post*, http://www.washingtonpost.com/world/national-security/in-us-russia-deal-nuclear-communication-system-may-be-used-for-cybersecurity/2012/04/26/gIQAT521iT_story.html?hpid=z1 [Accessed April 30, 2012].

Nakashima, Ellen. "Pentagon to fast-track cyberweapons acquisition." *Washington Post*, http://www.washingtonpost.com/world/national-security/pentagon-to-fast-track-cyberweapons-acquisition/2012/04/09/gIQAuwb76S_story.html [Accessed April 9, 2012].

Nakashima, Ellen. "With Plan X, Pentagon seeks to spread U.S. military might to cyberspace." *Washington Post*, http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html [Accessed May 30, 2012].

Office of the National Counterintelligence Executive. "Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011." Office of the National Counterintelligence Executive. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [Accessed March 21, 2012].

O'Keefe, Ed and Ellen Nakashima. "Cybersecurity bill fails in Senate." http://www.washingtonpost.com/world/national-security/cybersecurity-bill-fails-in-senate/2012/08/02/gJQADNOOSX_story.html [Accessed August 2, 2012].

Perlroth, Nicole. "Case Based in China Puts a Face on Persistent Hacking." *New York Times*, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CEcQFjAA&url=http%3A%2F%2Fwww.nytimes.com%2F2012%2F03%2F30%2Ftechnology%2Fhacking-in-asia-is-linked-to-chinese-ex-graduate-student.html%3Fpagewanted%3Dall&ei=E2AjUInCCYf40gHPsoDADQ&usg=AFQjCNGxUdV_152PQU_ms1ecxeV9GmMZ3Q [Accessed March 30, 2012].

Perlroth, Nicole. "Traveling Light in a Time of Digital Thievery." *New York Times*, http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?pagewanted=all [Accessed March 1, 2012].

Rogers, Mike. "Chairman Mike Rogers Opening Statement for Open Hearing on Cyber Threats and Ongoing Efforts to Protect the Nation, October 4, 2011." House Permanent Select Committee on Intelligence, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/100411CyberHearingRogers.pdf [Accessed March 21, 2012].

Rogers, Mike. "H.R. 3523: Cyber Intelligence Sharing and Protection Act." www.govtrack.us, http://www.govtrack.us/congress/bills/112/hr3523 [Accessed April 13, 2012].

Rogers, Mike and C.A. Dutch Ruppersberger. "Letter to Lixin Chen on Investigation into ZTE, June 12, 2012." House Permanent Select Committee on Intelligence, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/ZTELixinChen12JUNE2012.pdf [Accessed June 12, 2012].

Rogers, Mike and C.A. Dutch Ruppersberger. "Letter to Ren Zhengfei on Investigation into Huawei, June 12, 2012." House Permanent Select Committee on Intelligence, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HuaweiRenZhengfe12JUNE2012.pdf [Accessed June 12, 2012].

Segal, Adam. “US, China Butt Cyber Heads.” *The Diplomat*, http://thediplomat.com/china-power/u-s-china-butt-cyber-heads/ [Accessed June 19, 2012].
Skorobogatov, Sergei and Christopher Woods. “Breakthrough silicon scanning discovers backdoor in military chip.” University of Cambridge, http://www.cl.cam.ac.uk/~sps32/Silicon_scan_draft.pdf [Accessed July 20, 2012].
Stokes, Mark A., Jenny Lin and L.C. Russell Hsiao. “The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure.” Project 2049 Institute, [Accessed March 25, 2012].
The Economist. “Where’s the party? How the Communist Party is trying to expand its influence in the private sector.” *The Economist*, http://www.economist.com/node/21543575 [Accessed January y15, 2011].
The Economist. “Who’s afraid of Huawei?.” *The Economist* [August 4-10, 2012]: 19-23.
Thomas, Timothy. *The Dragon’s Quantum Leap: Transformation from a Mechanized to an Informatized Force*. Fort Leavenworth, Kansas: Foreign Military Studies Office, 2009.
Thomas, Timothy. “Nation-State Cyber Strategies: Examples from China and Russia.” In *Cyberpower and National Security*, Edited by Franklin Kramer, Stuart Starr and Larry Wentz, 465-488. Washington DC: National Defense University Press, 2009.
United Nations Conference on Trade and Development. “Dispute Settlement: World Trade Organization, 3.10 Technical Barriers to Trade.” UNCTAD, http://unctad.org/en/docs/edmmisc232add22_en.pdf [Accessed March 12, 2012].
US-China Security and Economic Commission. “The National Security Implications of Investments and Products from the Republic of China in the Telecommunications Sector.” US-China Security and Economic Commission, [Accessed June 12, 2012].
Wilshusen, Gregory C. “IT SUPPLY CHAIN: Additional Efforts Needed by National Security Related Agencies to Address Risks Government Accountability Office.” Government Accountability Office, http://www.gao.gov/assets/590/589617.pdf [Accessed May 1, 2012].
Wingfield, Thomas. “International Law and Information Operations.” In *Cyberpower and National Security*, Edited by Franklin Kramer, Stuart Starr and Larry Wentz, 525-542. Washington DC: National Defense University Press, 2009.
Wolf, Jim. “U.S., Russia work to expand cyberspace cooperation.” *Reuters*, http://www.reuters.com/article/2011/12/10/us-russia-usa-cyber-idUSTRE7B901N20111210 [Accessed April 3, 2012].
World Trade Organization. “Agreement on Technical Barriers to Trade.” WTO, http://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm [Accessed March 2, 2012].

Endnotes

[1] Magnus Hjortdal, “China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence,” *Journal for Strategic Studies*, http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss [Accessed March 23, 2012].
[2] Ibid.
[3] Ibid.
[4] Boyle, Rebecca. “Secret Cyber War Games Between U.S. and China Let Countries Role-Play Their Frustrations.” Popular Science, http://www.popsci.com/technology/article/2012-04/cyber-war-games-between-us-and-china-let-countries-role-play-their-frustrations [Access April18, 2012].

[5] Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," Office of the National Counterintelligence Executive, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [Accessed March 21, 2012].

[6] Ibid.

[7] Context Information Security, "Crouching Tiger, Hidden Dragon, Stolen Data," Context Information Security, http://www.contextis.com/news/articles/targetedattacks/targeted_attacks_whitepaper.pdf [Accessed March 20, 2012].

[8] Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf [Accessed Januar y12, 2012]; McAfee, "Global Energy Cyberattacks: 'Night Dragon'," McAfee, http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf [Accessed Januar y12, 2012].

[9] Aaron Back and James T. Areddy, "Hacking Probe Elevates Lanxiang School," Wall Street Journal, http://blogs.wsj.com/chinarealtime/2010/02/22/hacking-probe-elevates-lanxiang-school/tab/article/ [Accessed January 12, 2012]; John Markoff and David Barboza, "2 China Schools Said to Be Tied to Online Attacks," New York Times, http://www.nytimes.com/2010/02/19/technology/19china.html?_r=1 [Accessed January 12, 2012]; Tania Branigan, "Google attacks traced back to China, says US internet security firm," The Guardian, http://www.guardian.co.uk/technology/2010/jan/14/google-attacks-traced-china-verisign [Accessed January 12, 2012].

[10] Invictis Information Security Limited, "Commercial Espionage: The Threat from Chinese Cyber Attacks," http://www.invictis.com/downloads/IRIS_China_Report_Summary_170311a.pdf [Accessed February 28, 2012].

[11] Mike Rogers, "Chairman Mike Rogers Opening Statement for Open Hearing on Cyber Threats and Ongoing Efforts to Protect the Nation, October 4, 2011." House Permanent Select Committee on Intelligence, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/100411CyberHearingRogers.pdf [Accessed March 21, 2012].

[12] Ibid.; Bryan Krekel, George Bakos and Christopher Barnett, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," USCC, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf [Accessed January y15, 2011].

[13] Mike Rogers, "H.R. 3523: Cyber Intelligence Sharing and Protection Act," www.govtrack.us, http://www.govtrack.us/congress/bills/112/hr3523 [Accessed April 13, 2012].

[14] Nakashima, Ellen. "With Plan X, Pentagon seeks to spread U.S. military might to cyberspace." Washington Post, http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html [Accessed May 30, 2012].

[15] Ibid.

[16] Ibid.

[17] Timothy Thomas, "Nation-state Cyber Strategies: Examples from China and Russia" in *Cyberpower and National Security*, Ed. Franklin Kramer, Stuart Starr, and Larry Wentz [Washington DC: National Defense University Press, 2009]: 466-7.

[18] Timothy Thomas, The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force [Fort Leavenworth, KS: Foreign Military Studies Office, 2009]: 468. I used the term "quasi-strategy" because the concept of strategy differs in China from the one used in the US and the West. Whereas the US defines "strategy" as a "prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives," China defines it as "the analytical judgment of such factors as international conditions, hostilities, in bilateral politics, military, economics, science and technology, and geography as they apply to the preparation and direction of the overall military/war plan."

[19] Ibid., 10-1.

[20] Thomas, Timothy. The Dragon's Quantum Leap: Transformation from a Mechanized to an Informatized Force. Fort Leavenworth, Kansas: Foreign Military Studies Office, 2009.

[21] Timothy Thomas, "Nation-state Cyber Strategies: Examples from China and Russia" in *Cyberpower and National Security*, Ed. Franklin Kramer, Stuart Starr, and Larry Wentz [Washington DC: National Defense University Press, 2009]: 466-7.

[22] Ibid.

[23] Gregory C. Wilshusen. "IT SUPPLY CHAIN: Additional Efforts Needed by National Security Related Agencies to Address Risks Government Accountability Office." Government Accountability Office, http://www.gao.gov/assets/590/589617.pdf [Accessed May 1, 2012].
[24] Ibid.
[25] Ibid.
[26] GAO, "DOD IT Supply Chain, DOD, http://www.gao.gov/assets/590/588736.pdf
[27] Nicole Perlroth, "Traveling Light in a Time of Digital Thievery," *New York Times*, http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?pagewanted=all [Accessed March 1, 2012]. Ellen Nakashima, "In China, business travelers take extreme precautions to avoid cyber-espionage," *Washington Post*, http://www.washingtonpost.com/world/national-security/in-china-business-travelers-take-extreme-precautions-to-avoid-cyber-espionage/2011/09/20/gIQAM6cR0K_story.html [Accessed March 1, 2012].
[28] Ibid.
[29] Perlroth, "Traveling Light in a Time of Digital Thievery."
[30] Sergei Skorobogatov and Christopher Woods, "Breakthrough silicon scanning discovers backdoor in military chip," University of Cambridge, http://www.cl.cam.ac.uk/~sps32/Silicon_scan_draft.pdf [Accessed July 20, 2012].
[31] Robert David Graham, Bogus story: no Chinese backdoor in military chip" Errata Security, http://erratasec.blogspot.com/2012/05/bogus-story-no-chinese-backdoor-in.html
[32] SecDev Group, "Collusion and Collision: Searching for Guidance in Chinese Cyberspace," SecDev Group, http://www.scribd.com/doc/65531793/Collusion-Collision [Accessed March 21, 2012].
[33] Jason Healey, "The US Cyber Policy Reboot," Atlantic Council of the United States, http://www.acus.org/publication/us-cyber-policy-reboot [Accessed April 19, 2012].
[34] Ibid.
[35] Dan Breznitz and Michael Murphree, Run of the Red Queen: Government, Innovation, Globalization, and Economic Growth in China [New Haven, CT: Yale University Press, 2011] 177-180; Eric Harwit, China's Telecommunications Revolution [New York: Oxford University Press, 2008], 126-128; Jiang Dianchun and Zhang Yu, "Industrial Characteristics and Technology Spillover of FDI: The Empirical Evidence of Chinese High-tech Industries," Journal of the World Economy, http://en.cnki.com.cn/Article_en/CJFDTOTAL-SJJJ200610003.htm [Accessed January y15, 2011]. There are some conflicting information of which year Huawei was founded. Harwit lists the founding as 1988 and Breznitz and Murphree and most other sources cite 1987 as the year of the founding.
[36] Ibid.
[37] The Economist, "Where's the party? How the Communist Party is trying to expand its influence in the private sector," *The Economist*, http://www.economist.com/node/21543575 [Accessed January y15, 2011].
[38] Knake, 1-5; Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," USCC, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf [Accessed January y15, 2011].
[39] Reperi LLC, "THE NATIONAL SECURITY IMPLICATIONS OF INVESTMENTS AND PRODUCTS FROM THE PEOPLE'S REPUBLIC OF CHINAIN THE TELECOMMUNICATIONS SECTOR," USCC, http://www.uscc.gov/RFP/2011/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf [Accessed January y15, 2011].
[40] Krekel et al., "Occupying the Information High Ground."
[41] US House of Representatives Permanent Select Committee on Intelligence, "Rogers and Ruppersberger Intensify Investigation of Huawei and ZTE," US House of Representatives Permanent Select Committee on Intelligence, http://intelligence.house.gov/press-release/rogers-and-ruppersberger-intensify-investigation-huawei-and-zte [Accessed June 13, 2012].
[42] Ibid. The letters can be accessed by clicking the links on the page.
[43] World Bank and Development Research Center of the State Council of the People's Republic of China, "China 2030: Building a Modern, Harmonious, Creative, and High-Income Society," World Bank, http://www.worldbank.org/content/dam/Worldbank/document/China-2030-complete.pdf [Accessed February 28, 2012], 3-14.

[44] Global Times, "Australia's bid ban on Huawei "unjust"," Global Times, http://www.globaltimes.cn/NEWS/tabid/99/ID/703733/Australias-bid-ban-on-Huawei-unjust.aspx [Accessed April 1, 2012]; Global Times, "Huawei scales back payroll in US," Global Times http://www.globaltimes.cn/content/715720.shtml {Accessed March 23, 2012]; Xinhua, "Chinese firms seek overseas expansion in crisis, lending hands to global recovery," People's Daily, http://english.people.com.cn/102774/7691168.html [Accessed March 23, 2012]. There are many other stories that involve Huawei's "unfair" treatment in the US and Australia where PECD has taken some form or shape.

[45] Ministry of Commerce People's Republic of China, "MOFCOM Spokesman Commented on Australia's Rejection of Huawei's Bidding for its National Broadband Network Project," Ministry of Commerce People's Republic of China, http://english.mofcom.gov.cn/aarticle/newsrelease/policyreleasing/201204/20120408064948.html [Accessed March 20, 2012].

[46] World Trade Organization, "Agreement on Technical Barriers to Trade," WTO, http://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm [Accessed March 2, 2012].

[47] United Nations Conference on Trade and Development, "Dispute Settlement: World Trade Organization, 3.10 Technical Barriers to Trade," UNCTAD, http://unctad.org/en/docs/edmmisc232add22_en.pdf [Accessed March 12, 2012].

[48] Susan Rose-Ackerman and Benjamin Billa, "Treaties and National Security," Yale University, http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1601&context=fss_papers [Accessed March 1, 2012]; PETER LINDSAY, "THE AMBIGUITY OF GATT ARTICLE XXI: SUBTLE SUCCESS OR RAMPANT FAILURE?," Duke University, http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1192&context=dlj [Accessed February 12, 2012].

[49] Ibid.

[50] Edward M. Lebow, "The Foreign Investment and National Security Act of 2007," Hayne and Boone LLP, http://www.haynesboone.com/files/Publication/4722930e-9846-412f-a566-eceb8c6dc6c0/Presentation/PublicationAttachment/bf01cc5b-b7a8-4fbb-bd80-505fdc680f34/Lebow_CFIUS%20Article%20International%20Law%20News_01-2008.pdf [Accessed June 1, 2012].

[51] Nakashima, Ellen. "In U.S.-Russia deal, nuclear communication system may be used for cybersecurity." Washington Post, http://www.washingtonpost.com/world/national-security/in-us-russia-deal-nuclear-communication-system-may-be-used-for-cybersecurity/2012/04/26/gIQAT521iT_story.html?hpid=z1 [Accessed April 30, 2012]; Wolf, Jim. "U.S., Russia work to expand cyberspace cooperation." Reuters, http://www.reuters.com/article/2011/12/10/us-russia-usa-cyber-idUSTRE7B901N20111210 [Accessed April 3, 2012].

[52] Adam Segal, "US, China Butt Cyber Heads," The Diplomat, http://thediplomat.com/china-power/u-s-china-butt-cyber-heads/ [Accessed June 19, 2012].

[53] Ibid.

[54] Ibid.

[55] BRIAN SPEGELE, "New Tensions Rise on South China Sea," Wall Street Journal, http://online.wsj.com/article/SB10000872396390443659204577570514282930558.html?mod=googlenews_wsj [Accessed August 5, 2012]; Council on Foreign Relations, "Tensions in the South China Sea" CFR, http://www.cfr.org/southeast-asia/tensions-south-china-sea/p28772 [Accessed June 1, 2012].

[56] Ibid.

[57] FT Reporters, "Chinese infighting: Secrets of a succession war," Financial Times, http://www.ft.com/intl/cms/s/2/36c9ffda-6456-11e1-b50e-00144feabdc0.html#axzz234FcSQ7O [Accessed March 4, 2012]; Keith B. Richburg, "Courtroom spectator: Gu Kailai, wife of Bo Xilai, confessed to murder at closed trial in China," Washington Post, http://www.washingtonpost.com/world/gu-kailai-wife-of-bo-xilai-does-not-contest-murder-charge-at-closed-trial-in-china/2012/08/09/24153ebc-e206-11e1-ae7f-d2a13e249eb2_story.html [Accessed August 8, 2012]; BBC, Bo Xilai scandal: Timeline," BBC, http://www.bbc.co.uk/news/world-asia-china-17673505 [Accessed June 27, 2012].

[58] Robert Sutter, *U.S.-Chinese Relations: Perilous Past, Pragmatic Present* [New York: Rowman & Littlefield Publishers, 2010]; Denny Roy, *China's Foreign Relations* [New York: Rowman & Littlefield Publishers 1998]; Warren Cohen, *America's Response to China: A History of Sino-American Relations* [New York: Columbia University Press, 2010].

[59] Joseph Menn, "Agreement on cybersecurity 'badly needed'," Financial Times, http://www.ft.com/intl/cms/s/0/e595e568-f4dc-11e0-ba2d-00144feab49a.html#axzz1t7F2R4eF [Accessed March 29, 2012].