International Master's Program in International Studies
National Chengchi University
國立政治大學國際研究英語碩士學位學程

Cybersecurity and United States-China Relations: A Theoretical Perspective

網路安全與美中關係：理論的分析

JUAN MANUEL DE LA TORRE DAVILA
Advisor: Dr. LU, YEH-CHUNG

July, 2018

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Table of Contents

Abstract ..... **IV**

摘要 ..... **V**

List of Figures ..... **VI**

Chapter 1 Introduction **1**

1.1 Research motivation and Background 1

1.2 Research questions and design of the research 8

1.3 Research limitations 10

1.4 Structure of the Thesis 10

Chapter 2 Literature Review **13**

2.1 The current environment in IR and the transformation of the security concepts 13

2.2 Understanding the Cyber Space and Cyber Security 15

2.2.1 Definitions of Key Concepts 17

2.2.2 Neorealism 18

2.2.3 Liberalism 21

2.3 Development of the United States-China relations in the 21st century 23

2.4 Summary 25

Chapter 3 The US and China on Cybersecurity: One issue, two different approaches **26**

3.1 The United States and China: Domestic experiences on cybersecurity 27

3.1.1 The United States 27

3.1.2 China 33

3.2 The evolution of the concept of Cybersecurity 38

3.2.1 The United States approach to Cybersecurity 38

3.2.2 China's approach to Cybersecurity 40

3.3 Summary 44

Chapter 4 Thinking bilaterally: How does the US and China address each other? **45**

4.1 The International response: Do they listen to what some International Organizations say? 45

4.2 United States and China Cybersecurity Dialogue 47

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

4.3 Challenges and Opportunities for the US and China regarding Cybersecurity 57

4.4 Summary 60

Chapter 5 Walking towards the same goal: finding ways to avoid further conflict 62

5.1 The United States and China: how to arm the cyber puzzle 62

5.2 The role of leaders in reaching agreement in trying to set up some rules for the cyberspace. .66

5.3 The Process of Negotiation: Why did they decide to agree in such a conflictive matter?.....68

5.4 The 2015 agreement in perspective 72

5.5 Summary 74

Chapter 6 Conclusions 76

6.1 Future of the cyber world and IR: the case of the United States and China 81

Bibliography.....83

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Abstract

The rapid development of technology in the 21st century has dramatically changed the way actors in the international system interact, the internet and the threats challenges brought by it have created lack of understanding regarding the implications it has for security. Given this context, this thesis analyzes the impact of cybersecurity in United States-China relations using two of the main theoretical frameworks in international relations: neorealism and liberalism. Neorealism's offense-defense balance concept contributes to an understanding of the logic behind cyberattacks, while liberalism observes that there is a possibility to overcome conflicts by peaceful means, even in the cyberspace.

The importance of cybersecurity as a new threat in international relations has created unusual challenges for states around the world. In the case of the US and China, cybersecurity has generated, in a short period of time, more friction and engagement between the two countries than any other historical issue. Cybersecurity attacks in recent years have increased uncertainty in US-China relations, contributing to a deficit in economic and political trust between these two nations, nevertheless, why do these states still have reached an agreement? I suggest that the main reason behind this decision is the desire to avoid economic sanctions, nevertheless, neorealism and liberalism offer different reasons.

By answering four research questions the author gives insightful information about each country's view on cybersecurity. Furthermore, with the theoretical framework, I explain why they have reached such an agreement and what are the opportunities and challenges for the United States-China relations regarding cybersecurity. Finally I explain why all these actions have led to a "digitalization" of the practices of Foreign Policy of states such as the United States and China

Key Words: Cybersecurity, Cyberpower, Cyberspace, Cyberattacks.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

摘要

發展迅速的科技大大改變21世紀國際體系中的互動方式。根據此背景，本論文將使用兩個主要理論架構來分析網路安全對中美關係的影響，新現實主義的攻防平衡理論助於了解網路攻擊背後的邏輯，而自由主義認為可以利用和平的手段解決衝突，甚至在網路空間中。網路安全的重要性作為一個在國際關係的新威脅已經帶給許多國家不同尋常的挑戰。就美國和中國而言,網路安全在短時間內產生摩擦和衝突比兩國之間其他的歷史議題還更嚴重。近年來網路攻擊更加劇中美關係的不確定性，導致兩國之間在經濟和政治上互信不足，儘管如此，為何這兩個國家仍然達成協議？研究者認為這一協議背後主要原因是為了避免經濟制裁，對此，新現實主義和自由主義各有不同的觀點。研究者藉著回應四個研究問題，對中美雙方在網路安全的看法，提出具洞察力的見解。除此之外，在理論架構下，研究者解釋了他們會達成此協議的原因，以及中美關係在網路安全上會面臨哪些機會和挑戰。最後，作者說明這些行為導致美國和中國等國外交政策「數位化」的原因。

關鍵字：網路安全、網路強國、網路空間、網路攻擊

National Chengchi University

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

List of Figures

Figure 3.1 Annual number of data breaches and exposed records in the United States from 2005 to 2017……..……..29

Figure 3.2 Cyber incidents, and rates, by industry……32

Figure 3.3 Types of cybersecurity incidents encountered by users in China……35

Figure 3.4 Alleged Chinese attacks on the United States…….37

Figure 3.5 Key Actors in Cybersecurity Policies in China…….……..41

國立政治大學
National Chengchi University

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Chapter 1 Introduction

1.1 Research motivation and Background

"Cyberspace challenges all historical experience (…) when individuals of ambiguous affiliation are capable of undertaking actions of increasing ambitions and intrusiveness, the definition of state authority may turn ambiguous" (2015) stated Henry Kissinger in his book *World Orde*r. In just two sentences we can clearly see that we have entered a new and complex era in the history of the World.

Although the "Year Zero" in the battle over cyberspace took place not so long ago its consequences have multiplied exponentially with time. Adam Segal states that the Year Zero in the battle over cyberspace is from June 2012 to June 2013 "It was by no means the first year to witness an important cyberattack" (Segal, 2016) acknowledged the author.

As years pass by, the world has become more and more interconnected, creating the perfect environment for the proliferation of this attacks all over the world. Boundaries seen from the perspective of the Peace of Westphalia are slowly losing importance, in the cyber era, it doesn't really matter where you are, you can think from one side of the world and perpetuate your plan on the other side of the globe simultaneously.

During the Cold War only countries with enough money to invest and create nuclear bombs were allowed to participate in the international concert. Everyone pretty much knew the other countries' capabilities, should any of them use the weapons the others would know their identity even before the missiles landed. Everyone was going mad after the Mutual Assured Destruction doctrine.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

But now, and especially since June 2012, the reality has changed dramatically. Almost any county or even groups of people can launch a digital assault targeting either governments or companies across the world, being not only a faster way to reach your enemy but also cheaper and anonymously.

There are only two countries considered to be the only two real cyber superpowers: The United States and China. According to Segal (2016) there are four main characteristics a country has to fulfill in order to be called a superpower in the case of cyber powers: first they must have a large or technologically advanced economy, second they are required to have public institutions capable of leading the public sector, third a powerful military and intelligence agencies and fourth have had enough experience regarding cybersecurity.

Both the United States and China, according to the United Nations specialized agency for ICT,s, The Telecommunication Development Sector, have the largest numbers of web users in the globe. China in the first place with 750M and The United Staes second with 250M. Besides their numbers, they also have competitive technology companies. Both Beijing and Washington have identified cybersecurity as a strategic priority.

China joined the internet in 1994 and since then the cyberspace has represented a new source of disagreements and tensions with the United States. When describing the bilateral relation in terms of cyber-relations there are four main stages in it.

The first stage of relations, according to authors such as Zhao Weibin, started in 1994 when China joined the internet until 2010 when Google withdrew from China. During this stage, many companies from the US like Microsoft, Google, and Cisco established operations in China.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

The second stage went from 2010 until 2013 when Edward Snowden exposed the US' PRISM project, which the NSA uses to gain access to communication of users of nine popular Internet services: Microsoft, Yahoo, Google, Facebook among other online companies. It was during this period in which the differences between the two countries approach to internet widened even more. The United States supports Internet freedom while China emphasizes cyber sovereignty. It was during this stage that the "Year Zero" as discussed earlier in this chapter, happened. The accusations against China over cyber espionage augmented exponentially.

The third stage was from 2013 to 2017, with the WannaCry ransomware attacks. This stage is composed of mutual suspicion, competition but also cooperation. This stage is quite important, historically the United States had a relative advantage in the cyber relation given the fact that they had more experience with it, but with Edward Snowden's leakage of US intelligence, China could consider themselves to be at a more equal stage. During this period there were increased talks between President Barack Obama and President Xi Jinping regarding the cyber issues.

The fourth stage is the one currently going on, and researchers argue that it will be, hopefully, marked by enhanced cooperation and coordination (Weibin, 2017). With such an unknown future for two important countries in the world like this, a theoretical perspective would help us identify commonalities and expectations for the future in an important area such as cybersecurity.

Security in the field of International Relations is a concept that has shaped the way states interact with each other since Westphalia and probably even before that, nevertheless the definition of the concept and the implications that it has in policy making fluctuate according to

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

the current situation in the world. David Baldwin (1997) for example notes that: "security is an important concept, which has been used to justify spending civil liberties, making war, and massively reallocating resources". Twenty years later it seems that his words are still accurate.

The definition of security is often, if not always, entailed with threats. During a long period of time, a threat was merely related to military power, the number of soldiers, and even the size of the territory, Buzan, Wæver and de Wilde (1998) defines this as "the traditional military-political understanding of security. In this context, security is about survival", this is related to the fact that states were the only and most important players in the international arena, and the ultimate goal was to obtain power in a system were every actor is pursuing their own national interest.

John Baylis (2008) argues that traditionally most of the researchers have come to the conclusion that security "is a contested concept (…) it implies freedom from threats to core values but there remains a major disagreement about the primary focus of enquiry should be on 'individual', 'national', or 'international' security". As previously discussed, these views tend to focus at the national level mostly, defined largely in militarized terms. Nevertheless, as time passes and new issues appear, authors such as Barry Buzan (1983) proposed an expanded concept of security by adding political, economic, societal, environmental as well as military aspects. The disagreement on defining the word makes security a dependent term that has to be always related to a time context, a specific area, and specific actors, that can either be national international or individual. Political and scientific concepts, like security, are used within a complex context (Koselleck & Presner, 2002).

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Concepts as security reflect the reality of the time when they are used since they are influenced by perceptions and interpretations of events (Brauch, 2008). In the last century with the end of the Cold War, "a major reconceptualization of security has been triggered"(Brauch, 2008) we came from an era where the two antagonist states: The United States and the Soviet Union knew almost exactly the military capabilities and intentions of the other and vice-versa and ergo knew what to expect and how to react. This view of security is a really traditional and sometimes called Hobbesian view of security that was replaced by a more wide range of threats and security issues in the world.

Barry Buzan (2008) identifies four main stages in the view of security. The first one is the European Classical Great Power era which he notes happened from 1648 to 1945, a period in which basically the great powers were fighting against each other. War amongst great powers was a key institution of international society (Bull, 1977: 184-99) and also, colonization was a fundamental source of power and income to great powers. The Cold War was a turning point from this classical view of security, first, because the power structure went from being multipolar to bipolar, second, there was an ideological competition among the poles, third there were new inventions such as the nuclear weapons and fourth there was a process of decolonization. The end of the Cold War can be considered as the third stage because two of the defining features of the previous stage culminated: the bipolar system and the ideological competition. On 11 September 2001, the al-Qaeda attacks brought the third stage to an end, and it is exactly when the fourth stage started. This fourth stage brought war back to the centre stage given the fact that it was the first time in history that NATO invoked article 5.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Nowadays the range of threats and issues has widened even more. There has been an increasing number of terrorist attacks around the world, health and pandemic issues have arisen, massive migrations, environmental challenges, energy security, and with the information revolution that the Internet has brought, cybersecurity issues and its implications for international security.

According to the Worldwide Threat Assessment of the US Intelligence Community of 2017, Cyber threats appear at the top of the global threat list that they did. "Cyber threats are already challenging public trust and confidence in global institutions, governance, and norms, while imposing costs on the US and global economies. Cyber threats also pose an increasing risk to public health, safety, and prosperity as cyber technologies are integrated with critical infrastructure in key sectors"(Coats, 2017)

The Internet has become an essential tool for the economy and society and as it grows, the whole economy and society, including governments, have become increasingly reliant on this kind of infrastructure to perform their functions. The OECD notes that as this has happened, the consequences and failures of it can directly impact society as a whole. Cyber threats are evolving and increasing at a fast pace. When they started to appear online, hackers were focusing mainly on banks to steal money from them but now, the scope of their activities is broader, some of the most common are "hacktivism" (Anonymous), destabilization (Estonia in 2007), cyberespionage, sabotage (e.g. Stuxnet) and even military operations. (OECD, 2011)

The United States Department of Homeland Security (USDHS) stated in 2016 that:"[T]here are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

destruction would have a debilitating effect on [national security]. These sectors include: energy, defense, nuclear, transportation, food and agriculture, emergency services, communication, chemical, dams, finance, healthcare, information technology, commercial facilities, and government facilities" (USDHS, 2016)

In order to respond to this threat, the United States Department of Defense considered, since 2011, cyberspace a domain of war similar to the physical dimensions of air, land, and sea (Brownlee, 2015) This phenomena has created uncertainty for International Relations scholars, on the implications of this information revolution for national and international security. There is a school of thought that argues that the state is still the key player in the arena, maintaining (although adapting) its role as the supreme provider of security, even in cyberspace(Fountain, 2004). On the contrary, there is another one that says that this information revolution has increased the importance of non state actors such as social movements, firms, transnational networks and even individuals, in this sense “these non-state actors may be challengers to, as well as providers of, security”(Eriksson & Giacomello, 2006). Although they disagree on the source of security, the general observation is that the information revolution makes security an increasingly important concern in all sectors of society.

Considering the importance of the issue in the current transformation of the traditional security approaches all over the world and the impact a lot of scholars of International Relations are increasingly taking into consideration, it might be helpful to join the discussion and conduct a research of the approaches two of the most prominent states in the International Arena have used to deal with cybersecurity issues. It might be helpful to study how these two states react to this

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

problem and their ability to adjust to this issue that is in constant movement and in constant transformation.

China and the United States, as discussed before, are states with a huge economical and political impact in the world nowadays, so choosing them to analyze this issue could help better understand the situation and make better conclusions on how states address this issue. A closer study of these countries may help us illustrate how different or similar the policies of each country are, and see if what they're doing is enough to keep up with the emerging threats. We have to keep in mind as well that a very distinctive history, culture, geography, political context, society, and institutional structures are present among these countries.

1.2 Research questions and design of the research

1. How the United States and China view cybersecurity?
2. Why has cybersecurity become a national security priority for states such as the United States and China?
3. In 2015 the United States and China reached a Cybersecurity Agreement, why did they decide to do so?
4. What are the future challenges and opportunities for the US-China relations regarding cybersecurity?

For the purpose of conducting this research, two variables will be used to contrast with the hypothesis. The relation between the new cyber world and its cyber anarchic environment around the globe (IV), that has characterized and became an intrinsic tool for governments all around the

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

world since the beginning of the twentieth century, and the Foreign Policy decisions (DV) of superpowers such as China and the United States domestically and bilaterally in relation to these changes will be central for this thesis.

For the purpose of the study, the qualitative research method is the most appropriate approach. The anonymous nature of the cyberattacks makes it hard to collect statistical data to conduct a quantitative analysis, because it is almost impossible to know for sure the exact number of incidents. This research will use a combination of primary and secondary sources to address the questions. Foreign policy documents, official statements, and joint agreements will be of utter importance.

The hypothesis of the thesis is that the new cyber world and its cyber anarchic environment have produced a huge impact on the Foreign Policy Decisions on superpowers such as the United States and China which resulted in a "digitalization" of the practices of Foreign Policy domestically and bilaterally, nevertheless bilaterally they are still skeptical of each other on this matter but for some reason they still cooperate. This thesis will try to provide answers to the questions posed above and try to prove the hypothesis true or false.

In order to prove this hypothesis right or wrong, the scope of the thesis will focus mainly in the bilateral relation of the United States and China starting in 2009 when President Obama came to power until 2017 when he finished his presidency. The starting point of this period aligns when the cyberattack issues became a real problem and triggered instability in the bilateral relation with actions such as the intellectual property theft or the expulsion of Google from China and it stops at the end of the Obama presidency because after, with Trump, the rhetoric towards China changed.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

1.3 Research limitations

One of the research limitations of this research is conceptual. When defining most of the terminology to talk about cybersecurity numerous definitions can be found in the literature concerning the topic given the nature of the cyberspace and its impact. A lot of these concepts can be ambiguous since the area of research is still new.

There is a long list of states that are concerned and that have to deal with cybersecurity issues nevertheless only two very specific states have been selected to conduct this study which will narrow the research and generalize the findings.

Another research limitation is the little amount of specialized literature about the topic since its a relatively new one. Besides that, the research might be limited to the employment of English written publication when analyzing China as the author is not able to read Chinese, especially in foreign policy issues such as this.

1.4 Structure of the Thesis

The thesis consist of 6 chapters which are also divided into several parts to organize the information and accomplish the goal of the research.

The first chapter is the Introduction, and it serves as the chapter to portray the motivations and background of the study. The questions guiding the research are discussed here together with the hypothesis. Another key element of this chapter is the description of the methods used to do the research, the research limitations are also denoted here.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

In the second chapter, the current environment in International Relations and the transformation of the security concepts is the first part discussed. Then, a part where I will define the relevant concepts for the thesis and how authors understand it. Since the thesis is a theoretical approach, in this next part I will use two of the main schools in International Relations to study what they have to say about cybersecurity.

The third chapter provides an overview of the American and Chinese Cybersecurity Policies, respectively, first I briefly discuss the history of cybersecurity in their agendas and then I review their respective changing views on security and how they have both adapted differently the cyber approach in their policymaking process. To finish the chapter, I describe the actors involved in the decision making process in each country, and how these countries have been interacting with the outside on this issue, asking whether the external world has or has not had an impact in shaping their decisions.

The fourth chapter describes the bilateral relation and how they address each other in this matter, beginning by describing how the International Organizations respond to this issues then, I describe directly the bilateral situation of the countries and how they have been dialoguing to reach certain joint agreements. To finish the chapter I highlight the challenges and opportunities for the US-China relations on cybersecurity.

The fifth chapter discusses the US-China talks on cyber issues, the role of Barack Obama and Xi Jinping towards agreeing to cooperate towards a single-goal: Setting up the rules of the internet. Then I talk about the process of negotiation and the minor agreements they achieved before the 2015 agreement. At the end of the chapter I will put this agreement in perspective: Has it had an impact? Has the number of attacks decreased or increased?

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

The sixth chapter, the conclusion, reviews the results obtained after the analysis of both countries. I will go back to the theoretical part to explain why they decide to cooperate in a realm such as cybersecurity, then the implications for the rest of the world and then the future of the issue with the new President of the United States Donald Trump.

國立政治大學
National Chengchi University

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Chapter 2 Literature Review

2.1 The current environment in IR and the transformation of the security concepts

It is a well-known fact that with the invention of the Internet and its accessibility to almost everyone in the world, the world changed drastically. The former Vice President of the United States, Al Gore (as cited in Molyneux, 1999) once stated that "This is a revolution in communication technology unsurpassed since the invention of the printing press" and his words are still valid nowadays. The invention of the printing press changed the way people could communicate and pass information from one generation to another. Now, the Internet makes this task even easier since information, as messages, sounds, or pictures, can be delivered within seconds all over the world. Besides that, the internet has become essential for a wide variety of sectors of the society such as banking, broadcasting platforms, online services, government etc. Steve Molyneux (1999) says that such changes represent the perfect example of a move towards a "Networked Economy" and an "Information Society". This move shows the potential to affect the lives of a lot of citizens and it also highlights a significant change in the range and diversity of traditional telecommunications and media services.

The new information and communication technologies are transforming the lives of everyone on earth and ergo it is transforming the context in which international relations are conducted. The information revolution is a fact, what is left to discuss is what has been the impact of the information revolution on diplomacy, foreign policymaking, and even the way countries, or maybe non-state actors conduct war?

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Elizabeth C. Hanson (2008) claims that the impact of the technologies is so profound and persuasive that it is accurate to call this an information revolution. There are several significant changes, which represent a breaking point with the past, the first one is the abundance of information available and the wide variety of sources from which it can be obtained. At the same time, the time and costs of communicating have significantly decreased. These changes affect not only the lives of people around the world, but also governments: "their ability to control the information, the speed of decision making, the transparency of their actions, and the way they conduct their relations with other countries" (Hanson, 2008)

The most notable and striking example of this information revolution is the Internet. For example, the World Bank (2017) measured the number of internet users who had used the internet in a period of three months via any electronic device such as computers, mobile phones, personal digital assistants, games machines etc., and found out that this percentage has increased exponentially. According to this dataset, in 1990 0% of the population were using the internet, ten years later in 2000 this number was 6.8% already, ten years after that the number increased 325% compared to 2000, being 28.9% of the population in 2010. The most recent number is from 2016 and it says that nowadays the percentage of the population using the internet is 45.9 being an increase of 575% compared to the year 2000.

"The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had." Erich Schmidt, the former CEO of Google, stated in 1997. The Internet is the technical infrastructure that makes the communications among people around the world possible. Basically, the internet is a way to connect computers

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

altogether, either physically or wirelessly. The nature of internet communication makes it hard to apply rules and laws to it. Some authors say that the internet is a place with no laws.

In the literature, there is a consensus about this facts, the problem and lack of it comes when agreeing on the implications of the information revolution in the security concepts. There are three main branches of this discussion: the first branch of researchers would argue that the state is still the principal actor in the International Arena, maintaining (although adapting) its role as the supreme provider of security, even in cyberspace. Another branch is the researchers that claim that the emergence of "virtual states" and network economies imply a decline of violence among states, and hence security plays a lesser role. The last approach acknowledges that this revolution has increased the significance of firms, interest organizations, social movements, transnational networks, and individuals. For them, these new non-state actors may challenge as well as provide security. (Eriksson & Giacomello, 2006)

2.2 Understanding the Cyber Space and Cyber Security

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes are now being perpetrated through cyberspace. This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences. (The United States Department of Homeland Security, Cyberspace Overview[1])

[1] See: https://www.dhs.gov/cybersecurity-overview

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

As mentioned before, the cyberspace is everywhere, from the supercomputers being used to communicate from the offices of the NASA to the outer space to the pockets of millions of people around the world via mobile phones. Cyberspace has created the perfect environment for people to communicate in a cheaper, faster and in general more efficient way. Likewise, it has fostered business and even has created the environment for decentralized digital currencies to flourish, Bitcoin for example. We can assume that we are more dependent than ever to these digital infrastructures, which has become at the same time a source of new threats for national and individual security. The United States Government states that: "The architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient (…) it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations" (United States National Security Council, 2010: 1). Likewise, the German government also agrees that the attacks against information infrastructures have become more frequent and complex, "Cyber attacks are launched both from Germany and abroad. Given the openness and extent of cyberspace, it is possible to conduct covert attacks and misuse vulnerable systems as tools for an attack" (German Federal Ministry of the Interior, 2011: 3). Roxana Radu (2012) argues that this growing dependence of individuals, groups, institutions, and organizations has transformed the types of security threats over the years.

Besides all these issues, cybersecurity events bring new challenges. For example, not all cyber threats are detected, sometimes affected institutions don't even realize they have been attacked. Furthermore, when detected chasing the source is another challenge, sometimes even more difficult to solve.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

From the literature reviewed so far for this thesis, there are some existing frameworks for understanding Cyber Security. Kremer and Müler (2014) recognize three different bodies of literature about cybersecurity. The first approach concentrates on the means and motivations of the actors involved, the second one focuses on the instruments used by the offenders in the context of the attack and this one does not really make a distinction between the different layers and dimension of threats for categorization. Nevertheless, he says that there is a problem with these approaches since none of them are neither distinctive nor conclusive.

2.2.1 Definitions of Key Concepts

Cybersecurity: Cybersecurity is about the involvement of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, and technologies that can be used to protect the cyber environment and organization and assets. Cybersecurity aims to ensure the attainment and maintenance of the security properties of specific entities such as governments or companies in the public sector. (ITU, 2008)**.** From the International Relations perspective, Cybersecurity is the "ability to protect itself and its institutions against cyber-threats"(Choucri, 2012)

Cyberpower: Kuehl's definition of cyberpower is described as "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power" (Kuehl, 2009) Also, Adam Segal says that there are a series of characteristics a country has to have in order to be considered a cyberpower: A cyberpower must posses economic and technological power, it must be able to work with the private sector, it must

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

have an "adventurous and inventive military and intelligence agencies"(Segal, 2016) and as the last characteristic is an attractive narrative of cyberspace. (Segal, 2016)

Cyberspace: Joseph Nye's definition of cyberspace says that: "the cyber domain includes the Internet of all networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications." (Nye, 2011). It is useful given the fact that he defines it as a physical structure that has layers: "Cyberspace has a physical infrastructure layer that follows the economic laws of rival resources and political laws of sovereign justification and control" (Nye, 2011)

Security incident: "An incident involving the compromise or disruption of corporate IT systems (computers or networks) or its intellectual property"(Romanosky, 2016)

In order to better understand the concepts of Cyber Space and Cyber Security, it is helpful to try to adapt the concepts and ideas of two of the main theoretical bodies in International Relations: realism and liberalism.

2.2.2 Neorealism

Realist theory has three core ideas:

1.-Power and security are the most important things for a state.

2.-State is the only actor and unit of analysis in the International arena.

3.-States act rationally in order to satisfy its national interests.

Realism assumes that world politics are merged in an international anarchic system, in which there is nothing above states, which are regarded as the most important and only actor. Ergo, International Relations are seen as a relation of anarchic states. These anarchical conditions lead,

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

most of the time to the "security dilemma." Their main goal is to project and defend their own interests in the system unilaterally, nevertheless, states are not equal and the system is hierarchical. (Jackson & Sørensen, 2007: 93)

When studying security in the digital age, it seems that realist scholars do not see a need to revise their theories for understanding it. In this context, the state is still seen as the main and almost the only actor. When describing security, they maintain a narrow definition related to the militia, thus they deny that non-state actors exercise any degree of military power. The way they tackle the challenge of cyber threats is that they see it as epiphenomena, which may vary well affect the policies and domestic structures of states, but that does not undermine the anarchic system of international politics, and ergo do not affect the primacy of the state as the supreme unit in the international system. (Eriksson & Giacomello, 2006)

Although realism considers non-state actors and other forces beyond states to play a role in the international arena, it considers that these forces do not challenge the primacy of states and state interest in international politics. Some authors say that realist tackle the challenge of the information revolution by seeing them as epiphenomena, which they've used before to explain challenges such as globalization. They also consider IT-related security threats as an economic issue, which does not affect the security of states.

Nevertheless, there is a branch of neorealist thinkers like Stephen M. Walt that still consider the state a more or less rational actor but they also accept that this rationality can be somehow affected by domestic politics. Walt also considers that states tend to balance against threats rather than against power alone. Stephen M. Walt has an interesting theory to analyze threats. The balance-of-threat theory incorporates power, along with other factors such as

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

geography, offensive capabilities, and intentions within the more general concept of threat. This theory predicts that states will tend to ally against the most threatening state in the system. With this theory, he tries to explain why one state may balance against another state which is not necessarily the strongest but which is seen as more threatening on account of its proximity, aggressive intentions, or acquisition of especially potent means of conquest.

Neorealism represents a modified version of realism, it focuses on the structure of the international system and its interdependence, this approach explains how states behave in the international system including how states seek relative or absolute power (Jørgensen, 2017) Fear and uncertainty are the key elements driving states goals in order to maximize their military capability, economic capability, and other powers (Dunne, Kurki, & Smith, 2013).

Kenneth Waltz, who is one of the most relevant authors for Neorealism, defines power capabilities as a mixer of various elements "size of population and territory, resource endowment, economic capability, military strength, political stability and competence" (Waltz, 1979: 131). All these elements are more on the tangible side of the variables mainly because they are easier to quantify. For this author power brings four main advantages: it provides the means of maintaining one's autonomy in the face of force that others wield, greater power permits wider ranges of action, the more powerful enjoy wider margins of safety in dealing with the less powerful and have more about to say which games will be played and how, and fourth great power gives its possessors a big stake in their system and the ability to act for its stake (Waltz, 1979: 194-195)

Neorealism depicts international politics as a competitive realm in which the fate of each state depends on its responses to what other states do. "The possibility that conflict will be

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

conducted by force leads to competition in the arts and the instruments of force. Competition produces a tendency towards the sameness of the competitors" (Waltz, 1979: 127)

The defensive neorealist offense-defense balance concept could be used to understand the logic behind some cyberattacks, "Offense-defense theory (…) [is] based on the argument that war can be prevented if defense gains an advantage over offense. It also argues that an effective arms control can reduce the risk of arms races and war"(Glaser & Kaufmann, 1998).

2.2.3 Liberalism

Liberalism is quite a broad way to look at the International Relations nowadays since it emphasizes on the plurality of actors involved, the importance of domestic policies in shaping the international behavior of states and the role of institutions in setting up rules of behavior for the international community. This theory represents an expansion of the realist approach where everything is seen as a constant struggle for power and survival since it focuses on a broader set of issues.

Nevertheless they acknowledge that states still have a huge impact in world politics, but in addition, they also consider other actors such as transitional corporations, social movements, migrants, terrorists etcetera. Most of the liberal thinkers argue that because of this variety of actors, the sovereignty of the nation-state it's being less clear by the development of transnational relations.

Liberals tend to have an idealistic perception of the international society, which can be traced back to the influence of the ideas of Kant and Wilson. For them, there is a possibility to

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

overcome conflicts by peaceful means through building norms and institutions at an international level. Modern things such as technological development, are seen as a "vehicle of enlightenment and peaceful change" (Eriksson & Giacomello, 2006)

Liberals think that war is most likely to occur when militaristic and undemocratic governments not attached to international norms or institutions pursue their interests. Ideologically, if two states share the same ideology they would not go to war, like the democratic peace theory that says that two democratic systems will not fight with each other. This would alight with the fact that most cyberattacks are made to countries with different ideology such as the US to China and vice versa. Cyberthreats are seen as a sovereignty and security weakener for states "Cyber-threats weaken the sovereignty and security of the state. Non-state actors are becoming even more numerous and powerful because of the information revolution" (Eriksson & Giacomello, 2006)

When discussing the effect of the Information Revolution there is still a gap in the literature since few of the liberals seem to have apprehended the challenge of this revolution. Besides that, those who have, have forgotten to discuss its implications for security. For example, Joseph Nye observes that security, seen as the absence of threat to major values, can be at stake but he does not mention anything about cybersecurity threats in his work. (Eriksson & Giacomello, 2006)

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

2.3 Development of the United States-China relations in the 21st century

The United States and China initiated formal diplomatic relations in 1979, when the US President Jimmy Carter granted China full diplomatic recognition, acknowledging China's One China principle. Since then the bilateral relation has had ups and downs in history, nevertheless ,for the purpose of this thesis I will just focus on the relations from the beginning of the 21st century.

In 2001 George W. Bush became president of the United States and its policy towards China was tougher than the policy of his predecessor. Relations went on a low level on April 2001, when a Chinese jet fighter crashed with a US reconnaissance plan. Nevertheless, both governments worked to resolve this kind of issues and worked together to establish a more economically oriented relationship.

The first decade of the twenty-first century evolved to be a good and stable relationship. There has been growing economic interdependence and cooperation over key issues but there are some issues that still represent major obstacles to further cooperation between the two countries, issues such as Taiwan, Japan, North Korea keep policymakers busy.

Authors such as Sutter (2013) argue that Bush's Legacy to the relation is a positive equilibrium. During this period both countries converged and tried to broaden the common ground, neither one or the other sought trouble with the other, they were both preoccupied with other issues like the economic crisis of 2008.

The United States and Chinese administrations "worked hard to use multiple formal dialogues, high-level meetings and communications, and official rhetoric emphasizing the

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

positive in the relationship"(Sutter, 2013) The major differences were still there but they decided to avoid focusing too much on them, when this was impossible, there were tensions between them.

At the end of the Bush administration there were more and more tensions in four main categories: Opposition to the US support for Taiwan, opposition to US efforts to change China's political system, opposition to the fact that the US wanted to play a more dominant role along China's periphery and opposition to many aspects of the US leadership in world affairs.

It seems that during this period of time China went from being the reserved player who avoided conflict in order to keep gaining economic power to the player who started playing a bit more aggressively once he got the economic means and international recognition.

President Obama came to power in 2008 facing a great number of challenges domestically and internationally. In the case of China, the government of Obama was eager to build on what the previous government had achieved. Secretary of State Hilary Clinton noted that the administration would not let its traditional support of human rights "interfere with the global economic crisis, the global climate change crisis and the security crisis".

It was during Obama's administration that issues such as cyberespionage and the theft of information started to become a problem. Many American industrial secrets were stolen and outraged many US officials.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

2.4 Summary

This chapter analyzes the literature review regarding the transformation of the security concepts and how the new information and communication technologies are transforming the lives of every actor in the international system, people and states included. Given the challenges that cybersecurity brings, defining key concepts is a vital part for this chapter. Here the theoretical framework is constructed, using two of the main theoretical bodies in International Relations: Neorealism and liberalism. After the brief description of the brief description of the United States-China relations in the 21st century I concluded that cybersecurity issues such as cyberespionage and the theft of information were a great factor in creating instability in the bilateral relation. On the one hand, neorealism is a good theory that helps to explain cyberwar, while on the other hand, liberalism argue that there is a multiplicity of actors in the cyberwar. The control over cyberspace is viewed differently, liberals argue that cooperation through institutions is a key factor, neorealism has a different approach. According to the literature consulted, liberals lack to explain how norms and institutions can effectively tackle cyberwar while neorealist explain why war happens: states act offensively in order to seek their national security.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Chapter 3 The US and China on Cybersecurity: One issue, two different approaches

Is not a secret that the relationship between the United States and China is, if not the most, one of the most significant in the world nowadays, the economic power, the number of people involved and their military capabilities make them have such an important role in today's world. In this relationship, there is an issue that has changed the reality dramatically in such a short period of time: cyberspace.

Cybersecurity has generated a lot of uncertainty between the United States and China. Concerns over this domain have moved up to the list of issues in the bilateral agenda. Distrust is one of the key elements when discussing this issue given the nature of the cyberspace.

In this chapter I will discuss the experiences of the United States and China regarding cybersecurity, their individual experience regarding cybersecurity and how each country has used attacks against other entities, especially the United States against China and vice-versa. How they have adapted their agendas to include this new issues in it and the reasons behind doing so. It is really important to understand their perspectives and what the other can bring to the table. "Explanations by each side of how they came to a certain viewpoint can then move towards how the collective group can address some common problems" (Lieberthal & Singer, 2012) This is exactly why it is relevant to see what each country understands as an issue because even though its the same problem they see different solutions and approaches. Both sides can benefit enormously from the smooth functioning of the internet so it is an imperative issue to solve.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

3.1 The United States and China: Domestic experiences on cybersecurity

3.1.1 The United States

Fred Kaplan in his book *Dark Territory* published in 2016, give us some insights about the United State's "long" history of aggressions in cyberspace. In this book, Kaplan argues that the United States has been active in this kind of aggressions since the Gulf War when the American army was using "counter command-control warfare" to try to limit the enemy's ability to control its forces. Also during that time, allegedly the National Security Agency (NSA) was using technology to monitor the conversations of Saddam Hussein, president of Iraq at that time.

Also in the late 1990s, when Serbs in Bosnia and Herzegovina were out in the streets striking against the presence of NATO soldiers enforcing the 1995 Dayton peace agreement, the United States intervened transmission towers from local newscasters that were encouraging people to gather, telling them where and where. When the US officials learned about this, together with the NATO-led stabilization force installed those devices to control them and shut them off whenever the newscaster began urging people to go out to the streets and gather and even throw rocks at NATO soldiers.

Kaplan says that around a decade later, the US government installed a "mini-NSA" in Iraq, which aimed to intercept insurgent's e-mails and shut down many of their services with malware. Also, they were sending deceptive e-mails to those insurgents telling them to go to a certain place where US special forces would be waiting to kill them. "In 2007 alone, these sorts of operations, enabled and assisted by the NSA, killed nearly four thousand Iraqi insurgents" (Kaplan, 2016)

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

In 2006, the United States launched what Kaplan calls the US' most ambitious cyberattack. This cyberattack aimed to, together with Israel, sabotage the Iranian nuclear program. This offensive campaign was named Operation Olympic Games, and later known as Stuxnet. "For Olympic Games, they took some of their boldest inventions (…) and combined them into a single super-worm called Flame"(Kaplan, 2016) This worm could, once it infected a computer, swipe filer, monitor keystrokes and screens, even records conversations through the machine's microphones. It also allowed the NSA people to "remotely increase the flow of uranium gas into the centrifuges, which eventually burst[ed]. By early 2010, the operation had destroyed almost a quarter of Iran's 8,700 centrifuges"(Parker, 2017)

This intrusion "was a classic campaign of information warfare: the target wasn't just the Iranian's nuclear program but also the Iranian's confidence-in their sensors, their equipment, and themselves"(Kaplan, 2016) Another characteristic of this information warfare incident that makes it a good example is that for years the Iranians did not know that outsiders were attacking its systems, so they must have assumed that the malfunctions were their own fault. They realized only because the virus was accidentally spread to computers in other parts of the world, where the private sector researchers discovered it.

Cyberattacks have also often targeted the United States and since then, it has been a huge concern for the government of the United States and the private sector alike for more than a decade. The increased interdependence to the Information Technologies and to the E-commerce sector in the US has brought a huge rise to cyber crimes, causing a lot of damage to the economy of the government and the private sector. It has become an issue of more attention given the fact that it has reached key industries such as financial, healthcare and other important industries for

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

the US. The importance, volume, and cost of the data breaches have increased tremendously over the years. Figure 3.1 shows the number of data breaches from 2005 to 2017 in the United States. It also shows the number of records exposed during the same period of time.

As we can see in Figure 3.1, the number of data breaches has increased exponentially in the United States from 2005. The most common type of data breach incident online is identity theft, accounting for 59 percent of all global data breach incidents in 2016 according to the Identity Theft Resource Center. The most important data breach to date, given the amount of information that was stolen, was uncovered in 2016, when the web service provider Yahoo acknowledged that hackers stole information of all its 3 billion accounts in 2013.

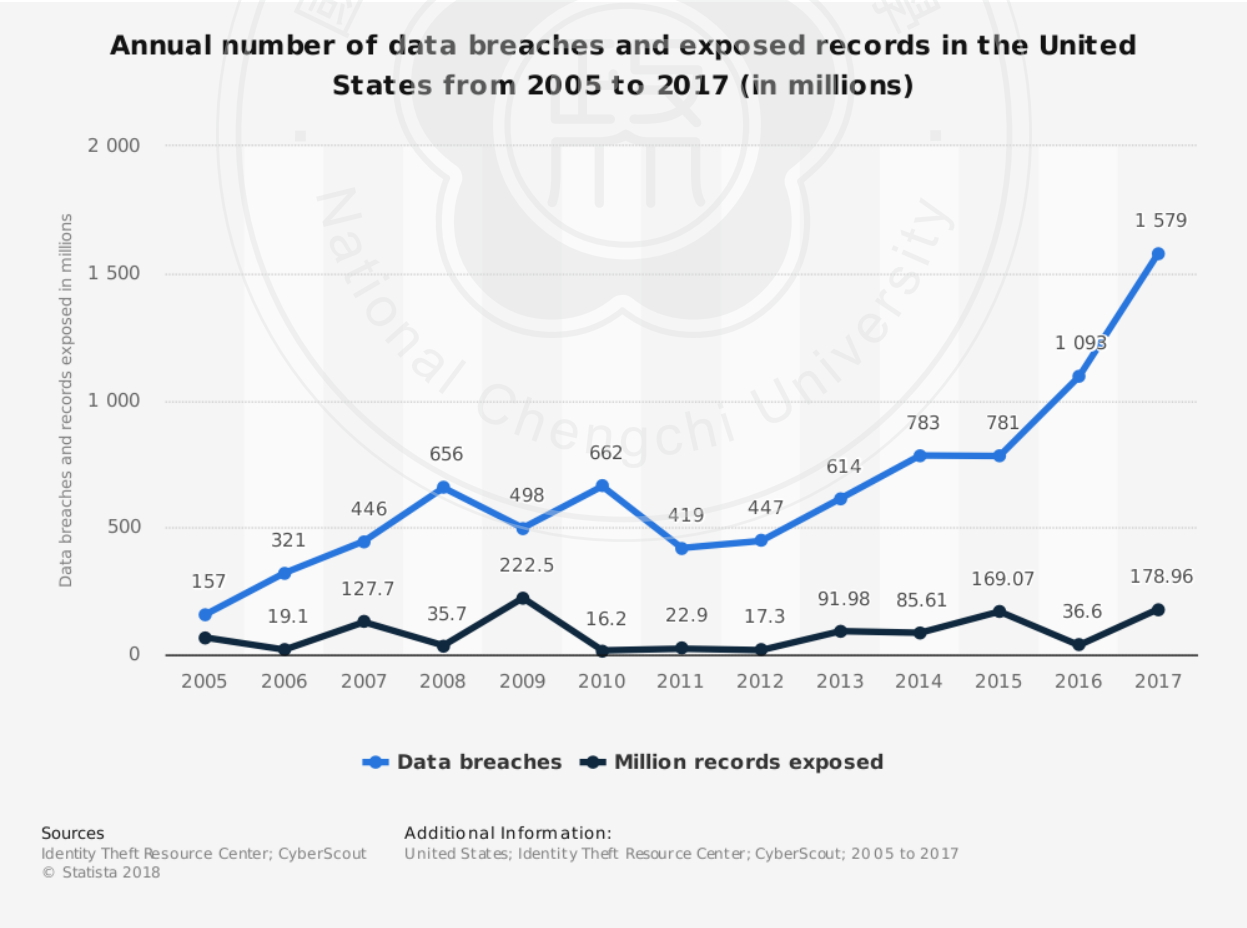

Figure 3.1. Annual number of data breaches and exposed records in the United States from 2005 to 2017

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

When these attacks were uncovered, Yahoo said that the date from more than 1 billion users was compromised, nevertheless on October 2017, they rectified and said that all of their more than 3 billion accounts were affected. According to Reuters "cyber thieves may have stolen names, email addresses, telephone numbers, dates of birth and encrypted passwords" (Volz, 2016)

This attack is not an isolated one, but it represent the largest in scale. Dan Kaminsky, an American security researcher says that these kind of attacks have affected almost everyone, "Five hundred of the Fortune 500[companies] have been hacked," he acknowledged in an interview carried by Reuters. The only problem is that we might not know about it, since most of these attacks have not been publicly disclosed and we still do not know if they ever will (Volz, 2016)

There might be many explanations behind these attacks, like economically driven but there is also the possibility, according to Reuters, that some intelligence officials from the United States said they believed some of these attacks were state-sponsored.

As a way to attack these attacks, in May of 2009, President Obama declared that the digital infrastructure of the United States was a strategic national asset and he also made protecting this infrastructure a national priority.

In 2013, President Barack Obama signed an Executive Order "to strengthen the cybersecurity of critical infrastructure by increasing information sharing and by jointly developing and implementing a framework of cybersecurity practices with our industry partners" (White House, 2013). This Executive Order expands the previously created Enhanced Cybersecurity Services program, they intended to strengthen the U.S. Government's partnership

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

with critical infrastructure owners and operators to address cybersecurity by creating new information sharing programs (producing unclassified reports of threats to U.S. companies and sharing them), also the Order directs The National Institute of Standards and Technology (NIST) to create the framework of cybersecurity practices relying on existing international standards, practices and procedures that were proven to be effective. The Executive Order likewise includes strong privacy and civil liberties protections based on the Fair Information Practice Principles, establishes a voluntary program to promote the adoption of the Cybersecurity Framework and calls for a review of existing cybersecurity regulation.

In 2015, the cyberthreats were noted as "among the gravest national security dangers to the United States" (White House, 2015) this because cyberattacks, privacy violations, data breaches, and cyberterrorism have become commonplace. In order to examine the risks and trends concerning these events, some authors such as Romanosky, Edwards, and Biener have conducted an analysis of cyber incidents in the United States with records form 2004 to 2015.

Sasha Romanosky (2016) distinguishes four types of cyber events: data breaches, security incidents, privacy violations and phishing/skimming incidents. Data breaches happen when personal information is disclosed by unauthorized users, security incidents are those malicious attacks targeting a company, the privacy violations are those violations to the privacy of the consumers and finally, the phishing/skimming incidents are those individual financial crimes.

Out of all these incidents, the most common one in the case of the United States are the data breaches which is exactly what happened in the previously discussed case of Yahoo. Besides basic information such as name and address, these cyberthreats steal credit card numbers and medical information.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

The question that remains in this equation is which sectors are these incidents attacking them most in the United States? In the figure 2, first, we can see the number of incidents across different industries and on the right panel shows the percentage of firms within an industry that suffer an incident.

Figure 3.2 examines the incidents and incident rates by industry based on the North American Industry Classification System. We can see based on the left graph in the Figure two how the Finance and Insurance Industry, is the one with a higher number of cyber incidents and Health Care, and Government entities are the second and thirds mostly affected by this issue. Nevertheless, when the incident rate is considered, Government agencies are affected at a much higher rate compared to other industries. While Health Care is above Government on the left side, when we consider the Incident Rate the Health Care sector falls considerably on the list, Government's rate goes to >1.5% while Health Care is <.5%.

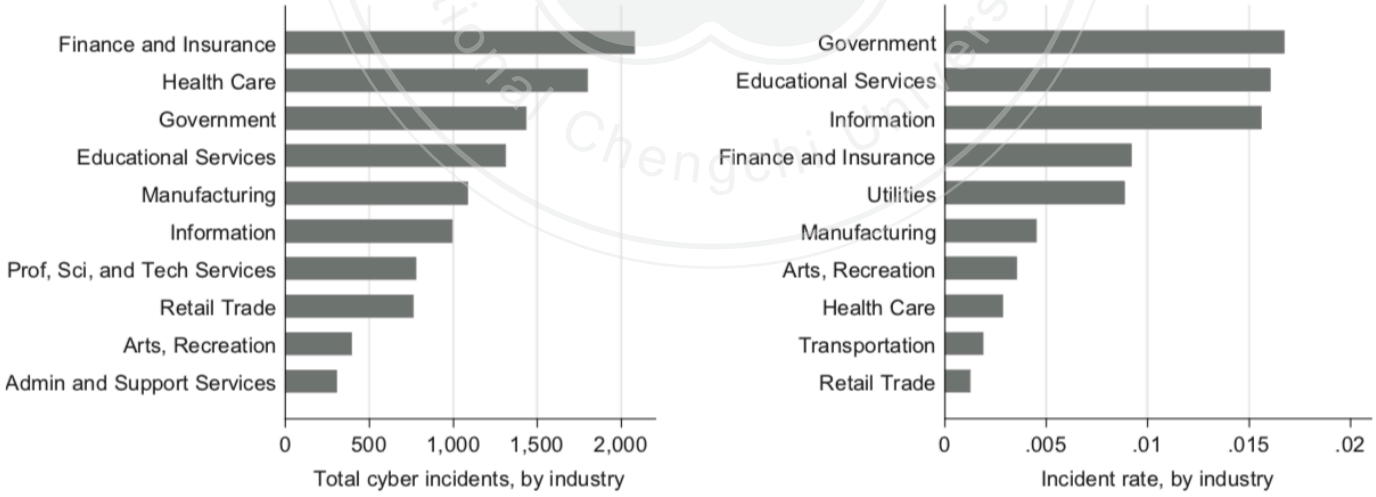

Figure 3.2. Cyber incidents, and rates, by industry.
Adapted from "Examining the costs and causes of cyber incidents" by Sasha Romanosky, 2016, *Journal of Cybersecurity, 2*(2), p.124.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

In the particular case of the United States, China and Russia have been the countries that keep US policymakers worried about, nevertheless China has traditionally "engaging not just in espionage and battlefield preparation, but also in the theft of trade secrets, intellectual property, and cash" (Kaplan, 2016) There are also other players like Iran and North Korea.

3.1.2 China

According to Statista China had, by the end of 2017, 771.98 million internet users making it "an attractive cybercrime target" (Nir Kshetri, 2013). According to data provided by The China Internet Network Information Center, in the first half of 2011 for example, 217 million Chinese people became malware victims, 121 million had online accounts hacked, and 8% were attacked by some scammers.

The development of the Internet in China is a really unique process, given the fact that the way their citizens use it is different from the American perspective. Nevertheless, "China [also] attaches great importance to Internet development (…) [however] China faces various challenges and has been one of the major victims of cyberattacks" (Longdi, 2014).

China started using the Internet relatively late, the first mail ever sent from China to the outside world happened on Sep 14, 1987, by some Chinese researchers sending it to their German counterparts (Wu, 2005). He Rulong, a Chinese spokesman from the Chinese Embassy in London explained to the *Financial Times* in April 2013 that this lateness in starting using the internet affects them, the spokesman acknowledged "As a late starter, China's internet is highly vulnerable and among the most victimized by cyberattacks"(He, 2013).

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

In order to be responsible for Internet affairs in the country, China founded in June 1997 a government department that would run under the Ministry of Information Industry called the China Internet Network Information Center (CNNIC or 中國互聯網絡信息中心). This information center constantly releases statistical reports in which they carry out an Internet development survey. Since its creation, the CNNIC has published 39 reports (last one on June 2017). They release two reports every year, at the beginning and the middle of each year.

According to the Report, cybersecurity incidents have also affected most of the internet users in China, they acknowledge that 70.5% of internet users encountered cybersecurity incidents. The report provides a table we can see in figure 3 that shows the types of cybersecurity incidents encountered by users in China.

As we can see from Figure 3.3 online fraud accounts for almost 40% of the incidents in China. The center considers that there are 6 main types of fraud incidents: bonus-winning information fraud, pretending to be a friend for cheating, online part-time job fraud, online shopping fraud, using fake employment information to cheat and pushing websites, there are others as well but the numbers are quite small so the report just puts them together and tags them as other frauds.

Until December 2016, 247 million PC's were infected by various virus such as Trojan viruses, attacking not only average internet users but also "more than 1.9 million mainframes in China"(Healey, 2013) According to Jason Healey the websites of 85 public institutions and companies were hacked between September 2012 and March 2013, with 39 of those attacks traced back to the United States "during a similar period, Chinese authorities noted that there

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

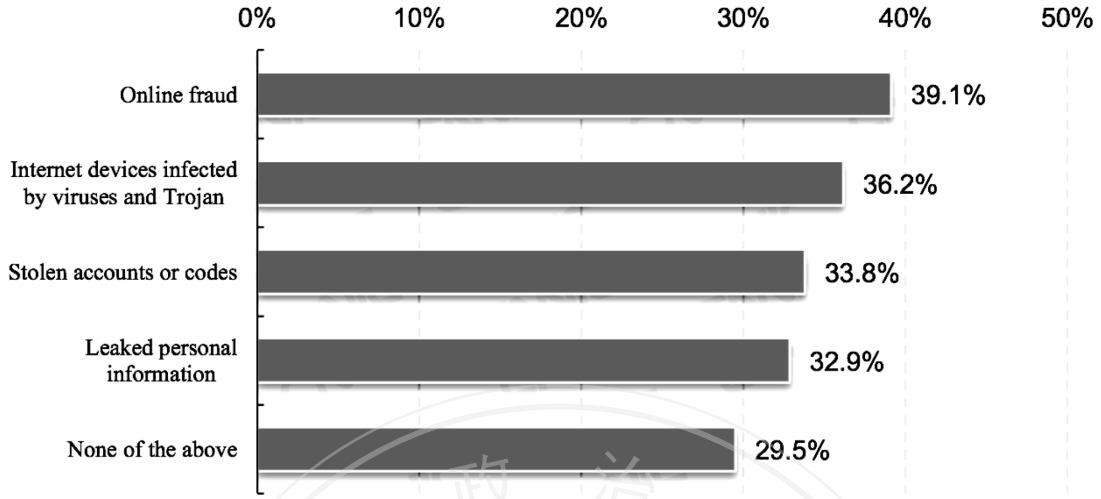

Figure 3.3. Types of Cybersecurity Incidents Encountered by users in China.
Adapted from the "Statistical report on Internet development in China" by CNNIC, 2017, p.106

have been some 5,800 hacking attempts from United States IP addresses and that U.S.-based servers had hosted 73 percent of the phishing attacks against Chinese customers"(Healey, 2013)

The deputy director of the Internet Society of China acknowledged in 2012 that Cybersecurity is also becoming an increasingly severe and complex issue in China. Mr. Gao Xinmin said "There are increasing attacks on China's Internet infrastructure as well as the information systems in key industries such as finance, transportation, energy, customs, taxation, and high technology. Financial sector websites have suffered frequent phishing attacks, becoming easy targets for online fraud and privacy theft".

Attacks originating from China to the outside world are a bit different from the ones coming from the United States which are mostly intended to gather information from governmental entities abroad. Chinese cyberattacks are usually targeting private sector companies trying to steal intellectual property, trade secrets, and other information that would be

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

profitable. Nevertheless, Chinese hackers have also targeted the negotiation strategies and financial information of energy, banking, law, pharmaceuticals, and other companies. " In 2013, the Commission on the Theft of American Intellectual Property (…) estimated that the theft of intellectual property totaled $300 billion annually, with 50 to 80 percent of that being from China"(Healey, 2013).

Likewise State-sponsored hackers have used cyberattacks to gather information on agencies, institutions, and individuals trying to influence international debates on topics that China considers of importance to either change the status quo or threaten the stability, "The embassies, foreign ministries, and other government offices of Germany, India, Indonesia, Romania, South Korea, Taiwan, and others have been targeted" (Healey, 2013)

Like Stuxnet for the United States, one of China's most high-profile cyberattacks happened in June 2015, these operations were tied to intelligence and counterintelligence operations. The US media reported that servers of the Office of Personnel Management (OPM) were attacked by Chinese hackers, granting them access to more than 22 million records that included security background checks and data on intelligence and military personnel. One of the goals according to Adam Segal was to use this stolen information to identify spies working undercover at US embassies around the world. Besides economic reasons, "Chinese hackers also break into US networks in preparation for a potential military conflict"(Segal, 2017)

Figure 3.4 shows thirty-seven cases of alleged Chinese intrusions from 2005 until 2013. The first known intrusion happened between September 2003 and August 2005, known as Titan Rain which aimed to affect the Department of Defense laboratories, NASA networks, and aerospace companies (Thornburgh, Forney, Bennett, Burger, & Shannon, 2005) This figure

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

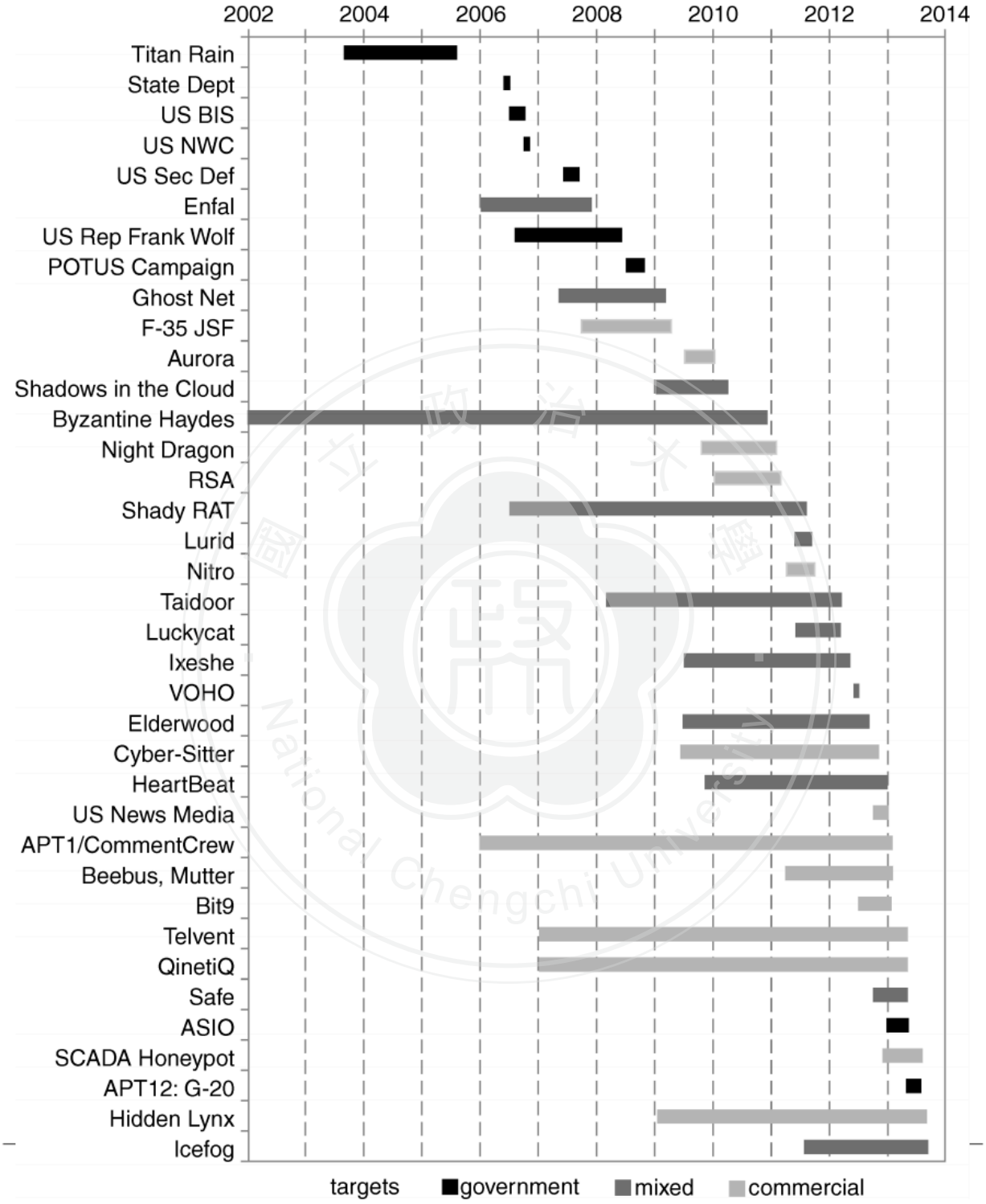

Figure 3.4. Alleged Chinese attacks on the United States, specifying duration and targeted institutions. Adapted from "From Exploitation to Innovation: Acquisition, Absorption, and Application." By Jon R. Lindsay and Tai Ming Cheung, 2005, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, 51-86.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

shows how originally most of the attacks were targeting the government, but around the year 2010 there was a shift and the attacks against the private sector were increasing in number.

3.2 The evolution of the concept of Cybersecurity

3.2.1 The United States approach to Cybersecurity

According to the United States Department of Homeland Security and its cybersecurity strategy released on May 2018, cybersecurity is nowadays a matter of homeland security and one of the core missions of the same Department. For them, the term cyberspace refers to "the interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computers, information and communications systems, and embedded processors and controllers" (U.S. Department of Homeland Security, 2018).

The department has seven main cybersecurity goals, in order to manage national cybersecurity risks:

Goal 1: Assess Evolving Cybersecurity Risks

Goal 2: Protect Federal Government Information Systems

Goal 3: Protect critical infrastructure

Goal 4: Prevent and Disrupt Criminal Use of Cyberspace

Goal 5: Respond effectively to Cyber Incidents

Goal 6: Strengthen the Security and Reliability of the Cyber Ecosystem

Goal 7: Improve Management of the Department of Homeland Security Cybersecurity Activities

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

These seven goals are at the same time grouped in different pillars, the first one, involving the first goal is about identifying the risk: in order to act consequently, DHS must understand the global cybersecurity landscape. The Second pillar involves the second and third goal which aims to reduce the vulnerability: by providing technical capabilities, cybersecurity information and other assistance they aim to reduce the vulnerabilities across the federal enterprise. The third pillar is about threat reduction and it includes Goal 4: by conducting research and use this knowledge to prevent cyber crimes. The fourth pillar involves the fifth Goal and is about the Consequence Mitigation: they know that some cyber incidents will happen but still, they will try to limit its impact. The last pillar encloses the last two Goals, and it aims to enable Cybersecurity outcomes: they wanna improve cybersecurity risk management outcomes by supporting policy and operational efforts in order to create a more secure and reliable cyber ecosystem.

There are several key events in the history of Cybersecurity in the United States in response to these issues. In 2003, the National Strategy for Securing Cyberspace (NSSC) was issued. Then in 2006, the National Infrastructure Protection Plan (NIPP) was released. After in 2008, a Comprehensive National Cybersecurity Initiative (CNCI) was released. In 2009 the Obama administration released Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. In 2009 the Pentagon established the US Cyber Command.

But according to Nir Ksherti, the United States still lacks a comprehensive security law or a Cybersecurity legislation. “Compared to the European Union, the United States provides

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

more autonomy to business regarding the way they disclose and store personal information" (N. Kshetri, 2016).

Henry Farrell and Charles L. Glaser argue in his article The role of effects, saliencies, and norms in US Cyberwar doctrine published in the *Journal of Cybersecurity* by the University of Oxford that the US approach to cybersecurity "implicitly rests on an effects-based logic"(Farrell & Glaser, 2017)

For the Obama administration authors such as Susan Hennessey claim that its administration's cyberstrategy "presented ambiguity as a deterrent tactic, claiming that a lack of specificity would discourage states from simply tailoring their malicious activities to avoid crossing lines"(Hennessey, 2017)

Cybersecurity regulations in the United Staes tend to rely on the voluntary self-regulation of sensitive data while encouraging marketing and innovations. This has created some degree of fear among users and customers that the US government can require Organizations to disclose user's data without the data owner's consent of knowledge.

3.2.2 China's approach to Cybersecurity

"Without cybersecurity, there is no national security; without informatization, there is no modernization" (没有网络安全就没有国家安全，没有信息化就没有现代化) stated President Xi Jinping to the news agency Xinhua. The Chinese government perceives software from the western countries as a threat to the national security of China, therefore its use domestically is highly regulated, proof of this is the expulsion of Google and other US made technologies from China.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

In the case of China, the ministries responsible for cyber-security policies are those that are already dealing with more general security issues, such as Ministry for Public Security (中 华人民共和国公安部) responsible for the areas of cybercrime and infrastructure security. The Ministry for Industry and Informatization (中华 人民共和国工业和信息化部) which coordinates cooperation with the private sector. The General Staff Division of the People's Liberation Army (中国人民解放军总参谋部) that mainly provides information about cyber attacks. Figure 3.5 shows more in-depth the key actors in cybersecurity policies in China.

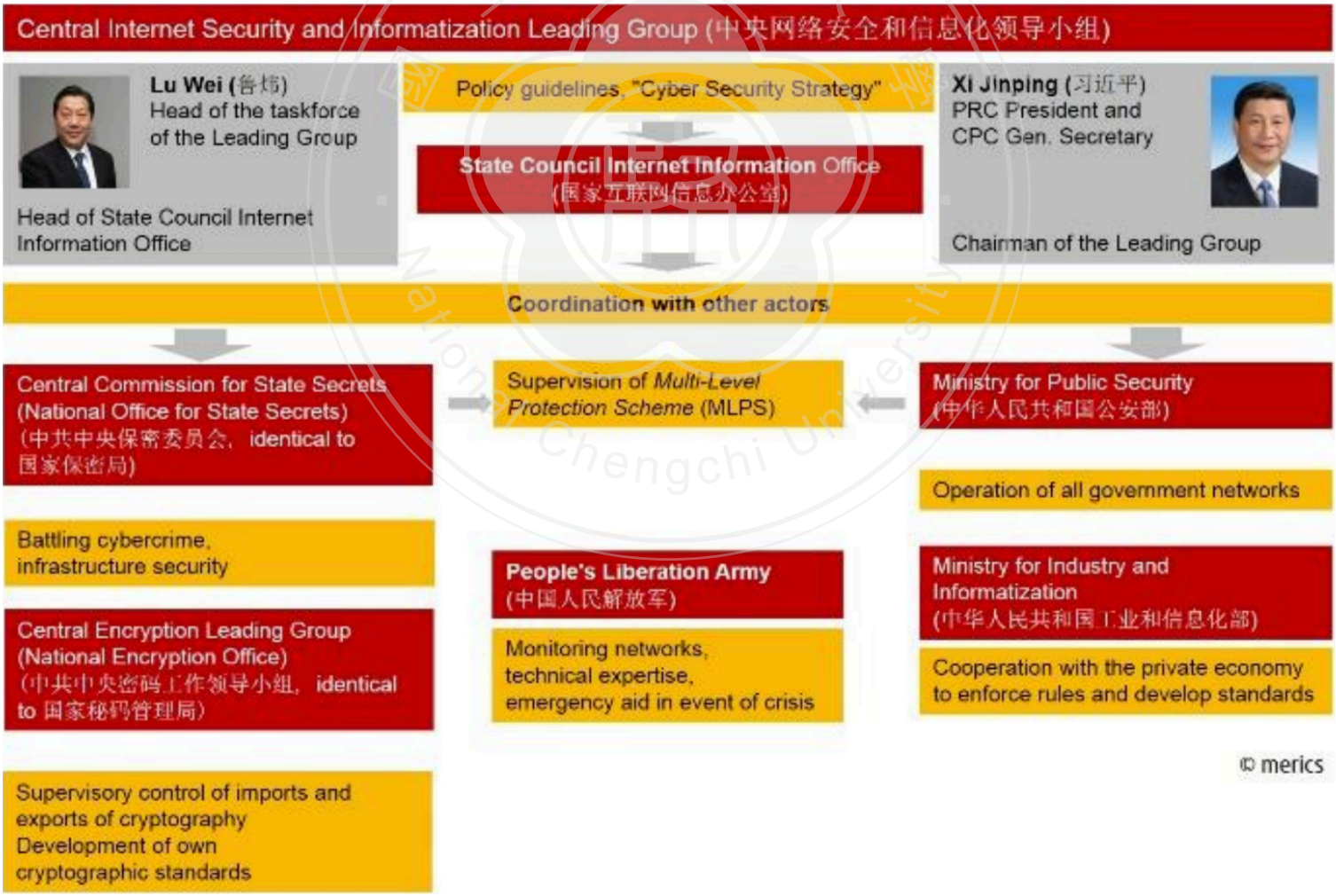

Figure 3.5. Key Actors in Cybersecurity Policies in China.
Adapted from "Cyber security in China: New political leadership focuses on boosting national security.." By Hauke Gierow and Leah Shih, 2014, *China Monitor*, (20), 1-9.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

The Chinese government has taken concrete efforts to enhance its cybersecurity, in order to create a more centralized body to control the cyber related issues, in 2014, founded the Central Cyber Security and Informatization Leading Group (中央网络安全和信息 化领导小组), in which the head of the Organization is Xi Jinping himself. This group focuses on cyber issues in almost all its aspects, from economic, political, cultural and even military issues. It is a breaking point in Chinese history regarding cybersecurity, the news agency Xinhua categorized it as "an important step" in the Chinese efforts to create a national strategy regarding cybersecurity and informatization. President Xi pursues this strategy by focusing on two main aspects: Developing technology and ensuring cybersecurity

This Group brings high ranking officials together with representatives of ministries such as the Ministry of Finance, Education, and Culture as well as the National Development and Reform Commission. This Group is not an executive entity but develops the guidelines for China's cybersecurity policies and works close to the State Council Internet Information Office.

The Leading Group, according to Xinhua acknowledges that China is a major victim of cyberattacks, saying that for example in the case of 2013, nearly 900,000 individual IP addresses suffered attacks from foreign viruses.

Until the creation of the Leading Group, the responsibility regarding cybersecurity in China was divided among many departments within the Government, so one of the goals in creating the Leading Group was to unify efforts by top-level guidance. It aimed to "establish a strong and authoritative mechanism at the central level" to deal with China's cybersecurity. The Leading Group, besides of taking care of external threats, also regulates the domestic content of

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

China's Internet in order to create what President Xi described as "an essential prerequisite for overall security"

The issue of cybersecurity has been present in the Chinese legislation for more than fifteen years, the first Chinese cybersecurity strategy was developed in 2013 by the National Coordination Small Group for Cyber and Information Security (全国网 络与信息安全协调小组).

Historically, we can trace China's current cybersecurity strategy back to 2012 and its "Opinion of the State Council Concerning Forcefully Moving Informatization Development Forward and Realistically Guaranteeing Information Security" (国务院关于大力 推进信息化发展和切实保障信息安全的若干意见) (中华人民共和国国务院, 2012).

The strategy defines some objectives such as boos broadband expansion in China, develop Chinese security technology, tighten the control of the internet to "uphold good morals in the Net", research new generation mobile networks, and expand e-government services in China (Gierow, 2014a)

Cybersecurity in China is a national priority, proof of that is that President Xi Jinping has recently headed the newly formed Central Internet Security and Informatization Leading Group. Xi Jinping has made cybersecurity a focal point in government work. (Gierow, 2014b).

The key feature of the Chinese cybersecurity policy is to develop a high-powered domestic Information Technology industry in order to protect China form "potential threats from foreign software"(Gierow, 2014a). The problem with China is that it has not pursued a coherent

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

strategy regarding cybersecurity. This is a really interesting fact given the nature of the Government in China that it's so centralized.

Cybersecurity regulations in China encourage purely the economic use of Information and Communications Technologies characterized by a strict governmental control. This with the objective of balancing economic modernization and the stability through political control. Notwithstanding, the policies are vague and create uncertainty most of the time. Also the fact that some western services such as Google or facebook in China has been a concern for some foreign firms.

3.3 Summary

In this chapter, the contrasting approaches of both countries on cybersecurity are analyzed. The United States has become the pioneer in adapting and trying to regulate the cyberspace. When tackling the problem, the involvement that the United States has with International Organizations is clearly seen while China seems a bit less worried about this. Even though they have differences, both agree in saying that cybersecurity is one of their national priorities.

Neorealism's idea of competition would help us explain why even though they have differences, the competition in cyberspace has created a tendency towards the sameness of the competitors. China, even though came relatively late to join the Internet Age, is slowly reaching the level of the United States. The liberal idea that cyberattacks are seen as a sovereignty and security weakener for states would explain why China, in a relatively short period of time, has taken so many efforts in having a more organized rule of law regarding cyberspace, all this with the goal of protecting its sovereignty.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Chapter 4 Thinking bilaterally: How does the US and China address each other?

4.1 The International response: Do they listen to what some International Organizations say?

The United Nations International Telecommunications Union launched in 2017 its Global Cybersecurity Index (GCI) in which they measure the status of cybersecurity worldwide. It measures the commitment of Member States to cybersecurity in order to raise awareness. The 2017 index includes the surveys made to 134 States in 2016.

Member States were classified into three different categories depending on their GCI score: Initiating stage, groups 96 countries which have just started to make commitments in cybersecurity. The Maturing stage refers to 77 countries that have developed complex commitments, and have engaged in cybersecurity programs and initiatives. And the last category is the Leading stage in which 21 countries are grouped, these countries have demonstrated high commitment in the five pillars of the index.

The five pillars of the index are legal, technical, organizational, capacity building and cooperation. The legal pillar is measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime, the more developed the cyber laws in the country the better ranking it has. The technical pillar refers to the existence of technical institutions and frameworks dealing with this issue. The Organizational pillar is measured based on the existence of policy coordination institutions and strategies at the national level. The capacity building pillar is measured by the existence of research and development, education and

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

training programmes. The Cooperation pillar is calculated based on the existence of partnerships, cooperative frameworks, and information sharing networks.

In the case of the United States, the Index considers that they are one of the 21 leader countries because of its high scores and legal capacity building the previously explained pillars. For the United Nations International Telecommunications Union a notable aspect of both capacity building and cooperation in the country is the initiatives to coordinate cybersecurity among all states. It is considered as the top one country in the Americas region, with Canada and Mexico as the top second and third.

China, on the other hand, is not considered in the top three ranked countries in Asia, it is stagnated behind Singapore, Malaysia and Australia, countries which have developed its pillars to such an extent to be considered the top in Asia and the Pacific. This might be related to the fact that China purposefully distances itself from existing international agreements. It is creating parallel IT standards to work with them domestically, not really following the International standards and practices. The United States ranks as number two in the score, just behind Singapore, while China ranks as 32 in the list of 165 countries.

The United States actions in the cyberspace are bounded by its constitution, supposedly aiming at the right of freedom of speech, and by its international commitments with International Organizations such as the United Nations. On the other side, China has traditionally argued for the recognition of sovereignty as a basic principle also in the cyberspace and the need to avoid and prevent actions that could destabilize the relations.

In the case of China, together with Russia and other members of the Shanghai Cooperation Organization, they have been trying to promote for more than a decade its ideas for

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

internet governance in the world. The principle of internet sovereignty that the Chinese people are trying to promote includes two main things "first, to abstain from uninvited influence of any kind within any state's information space and, second, to regulate the internet through an international forum, such as the United Nations' International Telecommunication Union"(Lindsay, 2015). The first of this ideas opposes the American idea of openness and the second aims to give a more equal treatment to the issue by an independent and strong organ such as the United Nations rather than "the constellation of multi-stakeholder institutions that has historically governed internet protocols and global network management"(Lindsay, 2015).

It is clear that both, United States and China, face many similar problems, regarding cybersecurity; however, they have different views. China has more openly used its idea of sovereignty by censoring the web and strongly surveilling its citizens. For the Chinese, adapting the international openness idea on the internet represents a threat "Full freedom can bear not only a terrorist threat but also a danger to the life and freedom of citizens (…) we must pay serious attention to check and filter incoming information" (Lu, 2016).

The main difference between United States and China's views on cybersecurity mainly concern freedom of information in cyberspace. Also, each government's decision-making process vary; while in the case of United States, many branches are involved, the CCP basically controls every decision in the process.

4.2 United States and China Cybersecurity Dialogue

The cybersecurity dialogue between the United States and China is not different from other kinds of dialogues between these countries, it "reflects the thoroughly ambiguous relationship between

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

China and the United States, distinguished by deep economic interdependence as well as rivalry and mistrust in the security arena"(Lindsay, 2015)

The United States and China have significant differences in almost every aspect, and cybersecurity and cyberspace are not the exception. The definitions and objectives differ which makes the approach sometimes a tricky and not so easy one. For example, in the 2011 White House International Strategy for Cyberspace the US clearly argues that it will work towards creating a more open, secure and reliable information and communications infrastructure, while China traditionally argues to create the norms of what could be called the cyber sovereignty, in which states have the right to control and regulate their own cyberspace freely.

As exposed in the previous chapter, China's rhetoric is more about how the cyberspace should be governed, making emphasis in the sovereignty of the cyberspace while it has not really offered a lot of justifications or explanations on how and why a state may conduct cyberattacks. (Segal, 2017) China's rhetoric is not a new one and the dialogue with the United Staes has happened accordingly.

In 2009, US President Barack Obama and Chinese President Hu Jintao established the US-China Strategic and Economic Dialogue (S&ED or 中美戰略與經濟對話 in Chinese) which is an upgraded mechanism that replaced the former Senior Dialogue and Strategic Economic Dialogue started under the George W. Bush administration[2]. This is a high-level dialogue for the United States and China to discuss a wide range of regional and global strategic and economic issues between both countries.

[2] Since April 2017, the Dialogue is renamed to Comprehensive Economic Dialogue by President Trump and President Xi Jinping.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

This Dialogue is important given that it has created "new habits of cooperation (…) providing more senior, more direct, and more comprehensive communication (…) [on] critical domestic and global challenges"(Kuo, 2016). This dialogue is relevant because cyber issues were part of it and is one of the precedents of the 2015 Agreement. The S&ED "will meet once per year in alternate capitals" (U.S. Department of the Treasury, 2009). It was on the seventh round of the S&ED, on June 2015, where cyber issues were featured prominently on the security side of the Dialogue for the first time. After the 2015 Agreement reached by President Obama and President Xi, the S&ED, on June 2016, welcomed the results of the first US-China High-Level Dialogue on cybercrime.

There have been other more specific and concise communication strategies between both sides, such as the one organized by the think thanks: The Center for Strategic Studies and International Studies (CSIS) and the China Institute of Contemporary International Relations (CICIR) who have held talks, where officials and experts from both the United States and China gather. The main objectives of the discussions are to reduce misperceptions and to increase transparency of both countries' authorities and understanding on how each country approaches cybersecurity, and to identify areas of potential cooperation, including confidence-building measures and agreement on norms and rules for cybersecurity. This kind of dialogues might not represent, even though there are participation of officials coming from both governments, the real views of both governments, nevertheless, it is relevant because it is a source to see how the bilateral relation in terms of cybersecurity developed during this period of time.

The importance of these dialogues falls in the fact that even though they are not formal official communication channels between governments, they serve as a trustful source of

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

information to track down the development of the cybersecurity related issues from 2009 until 2017 given the importance and relevance of both think tanks and also the fact that it includes not only expert on cybersecurity but also government officials from both sides. Also, due to the limited open resources, this mechanism presented by these think thanks serves as a platform that has lasted for several years and the information is consistent.

The first dialogue event took place on December 17, 2009, in Washington DC. On this day, officials and experts worked together in two different sessions, the first one called Cyberspace and International Security and the second one called Multilateral and National Activities to Promote Cybersecurity.

In the first session, they both agree on saying that no nation by itself can adequately secure cyberspace. But also, there is neither an adequate policy framework to manage cooperation and conflict in cyberspace, nor a coherent lexicon to describe it. The main topics discussed in that session were three: National perspectives on cybersecurity, Principles, norms and lexicon for international security for cyberspace, and Multilateral approaches to future Estonia-like incidents.

In the case of the second session, they acknowledged that every nation faces the same problem of making cyberspace a secure environment for innovation and economic growth. Besides that, nations face the problem of how to best build trust and assurance in key national networks. The topics discussed in that session were four: Cooperative approaches to cybercrime, Securing the global cyberinfrastructure, Confidence-building in cyberspace, and Next steps in CICIR-CSIS dialogue.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

It was in May 2010 when the second Sino-US Cybersecurity Dialogue happened in Beijing. During this event, there were six different panels: 1.-How should we define responsible state behavior in cyberspace? 2.-How does national sovereignty apply in cyberspace? 3.-What sort of international governance structure or rules would best serve the international community? 4.-What rules are appropriate for military conflict in cyberspace? How should existing laws of war be applied? 5.-What roles do technology and trade play in cybersecurity (e.g. techno-nationalism, technological hegemony)? 6.-What is the basis for cooperation on combating cybercrime? And as we see the topics discussed are still super similar to the discussed in the previous meeting.

In the case of the third meeting, there is no information listed on the Web page of the Center for Strategic and International Studies, but I can assume it happened in the United States probably at the end of the year 2010, it is quite interesting that it jumps from the second to the fourth meeting in their official page online (consulted on June 3, 2018).

The fourth dialogue took place in Beijing and for that, the only information available is the Agenda of the day, without going deep in providing more information. They discussed the Use of force in cyberspace (like basic principles, basic concepts, criteria, and processes), Law enforcement cooperation, Supply chain and Trade issues, Governance in Cyberspace (like Institutions, Sovereignty and Responsibility, Norms), and to conclude they discussed the State-to-State trust in cyberspace.

The fifth CICIR-CSIS talks on cybersecurity happened from November 30 to December 1, 2011. This time it took place in the office of the Center for Strategic and International Studies in Washington DC. There were two sessions this time, the first one concerning the US and

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Chinese perspectives on development in cybersecurity, their National Practices and policies for cybersecurity and the Military and Security issues in Bilateral Cybersecurity. The second session was about the Framework for International Security in Cyberspace and Building Strategic Trust in Cyberspace.

In the case of the sixth Dialogue, it happened in Beijing on the 13-14 of June 2012. This Dialogue was quite interesting, during the first day they had normal sessions discussing four different things, first the China-US Confidence building in the Cyberspace, where they were trying to identify the main causes preventing the two sides from building trust, second the International Norms and Cooperation over the Cyberspace, third the Law Enforcement Cooperation, and fourth the New Risks, New Threats then New Concepts, where it was all about defining the concepts and considering if old definitions were still adequate.

The second day was a bit different, they created two scenarios in which they had to theoretically react. In the first simulation a really powerful virus breaks out somewhere, it has a lot of power since its sophisticated and devastating. They wanted to see first, how would China and the United States immediately communicate with each other in order to prevent infections? Second, how would China and the United States send out convincing signals in order to avoid misperception and escalation of tension? Third, would it be possible for both countries either jointly or in collaboration with other States or players, conduct effective investigations? Fourth, what would they do if after the investigations they find out that the responsibility points at non-state actors such as terrorist or if it turns out to be originated from a State? What should they do in each case?

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

In the second scenario, an accidental incident between naval vessels causes damage and leads to heightened tensions in both countries. Hackers start issuing threatening statements, and both countries detect cyber exploits against government and military networks that appear to originate in the other country, nevertheless, they are unable to determine if they come from either private or governmental hackers. In this case, hey wanted to see first, what sort of cyber incidents would be considered destabilizing or would lead to an escalation of tensions? Second, how would China and the United Staes immediately communicate with each other in order to prevent misinterpretation or escalation? Third, are there implicit signals that could be used to indicate discomfort over a particular malicious cyber activity? Fourth, how do they indicate what actions are unacceptable and would trigger a damaging response? Fifth, what understandings should be put in place between the two countries in advance of any incident to better manage a future crisis and to avoid conflict?

These kind of simulation are really fruitful in my point of view, and it would be incredibly beneficial for my thesis to have access to the results and the way they dealt with the issue, but since those documents are not available I can only assume what could have happened. What I could find is a Joint Statement released after the sixth meeting by both the CSIS and CICIR. In this joint statement, they point out three main things: the areas of agreement, the unresolved areas and the next steps both states need to go.

Both countries have a shared interest in avoiding the misperceptions and miscalculations that could lead to conflict, they also share the same interest in finding measures that can be suggested to the two governments to reduce tensions in the cyber arena. They also found out after the simulations that both Staes have formal processes for dealing with cyber crises, but

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

there is no identified channel of communication, reason why they agree that creating a formal approach to communicating in a crisis would be useful and necessary. Both the CICIR and CSIS have similar views on the risk posed by non-state actors and the need to limit their capabilities in the cyberspace.

One of the issues that remain unsolved is the question regarding what sort of behaviors could be regarded as an attack or war in cyberspace, there are also areas of ambiguity involving the scope, duration, and effect of cyber actions and those issues also need to be clarified not only by the United States and China but internationally. The treatment of proxy forces also remains an outstanding issue affecting the discussion of norms and codes of conduct.

After the first six meetings both institutions form both countries acknowledge that the dialogue has already provided a place for informal discussion among the respective governments but it is not enough, it should be broadened. That's why they propose that in order to carry out official discussions over this issue, additional channels at high levels should be set up between the two governments. Government to government discussions would create a better environment to create better and effective bilateral crisis communication channels, also if both governments have high official meetings it would help increase the public awareness.

On December 4-5, 2012 the seventh Dialogue took place in Washington DC. This Dialogue copied the same style as the previous one, leaving the first day for discussion and the second for the Scenarios-based Discussions. On the first day, they US representatives explained their perceptions on China's cybersecurity policy while the Chinese representatives also provided their perceptions of the US cybersecurity policy. After that, they both provided their own perceptions of the international cyber environment.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

During the second session, they discussed the future of interdependence between the United States and China: the implications of cybersecurity, the boundaries of acceptable behavior in cyberspace and at the end each side provided a description of the requirements for stability in the cyberspace and also measures that could enhance it.

The fact that they replicated the model form of the previous session makes me believe that they saw it as a good exercise to see and measure how the states would react under certain circumstances. This time there were 4 scenarios: In the first one, Iran experiences a range of cyberattacks and suspects Israel and the United States are behind them. Iran asks China for technical assistance while Israel asks the United States for assistance. The main question is can the US and China cooperate in managing this situation and defusing this cyber battle kind of situations? In the second scenario, each country discovered that its energy pipelines have been probed and mapped for possible cyber attacks, each suspect the other is responsible. In the third scenario authorities from both countries found a serious vulnerability with a widely used IT product. In the fourth scenario, the United Kingdom announces that cyber espionage has reached intolerable levels and calls for a global conference of leading nations since the current institutions such as the WTO are ineffective, would both countries agree that a new approach is necessary?

The eight Dialogue was held in Beijing and it had four sessions plus two discussions. Sessions were about Chinese and US Expectations for Responsible State Behavior, Mechanisms for avoiding Miscalculation, Cooperative Measures to Increase Stability and Chinese and American Views on the Link between Security and Governance. The two extra discussions were

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

about how would China and the US cope with common threats? And what are the next steps of Track Two Cybersecurity Dialogue after the establishment of an official working group?

The last meeting's agenda published in the official webpage of the CSIS happened on February 2015. There were more meetings during 2017, one in January and one in November but there is no official information about them yet. During the 2015 meeting, experts from each country discussed The Use of Force in cyberspace, given the fact that at that time there was no international agreement that would define when cyber incidents qualify as an armed attack or the use of force. They also discussed Fundamental principles for sovereignty, stability, and state responsibility, in which Chinese and American experts provided their views on how sovereignty applies in cyberspace. The Norms for Cyberspace were also discussed, mainly the principles and criteria and the applicability of norms to non-state actors, and their relation to existing International commitments, with a goal of identifying useful norms for cyberspace.

Now that I have discussed the specifics of all the information available for these talks, I can assert that mistrust is a word that would define the talks since they started dialoguing back in 2009. Although there is one obvious thing that remains constant in all the talks "for the United States, China should stop stealing so much intellectual property; and for China, the US should stop trying to maintain its hegemony in cyberspace, contain Beijing, and militarize cyberspace"(Segal, 2012). It is hard to make more assumptions without knowing exactly what happens behind closed-door meetings.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

4.3 Challenges and Opportunities for the US and China regarding Cybersecurity

There are four main dimensions for the US and China relations that in my opinion contain the main challenges for the bilateral relations and they also apply in cyberspace particularly. These dimensions are: The Political dimension, The Military dimension, The Economic dimension and the Institutional dimension. There is another dimension that some authors would argue has a huge impact in the better development of the bilateral relation, which is the cultural dimension, but I think that for the case of cybersecurity this dimension can be omitted, given that the cyberspace does not really recognize these type of boundaries.

On the political dimension, cybersecurity reflects the reality of the relationship between the United States and China, "Harassment in cyberspace (…) both exploits and amplifies the ambiguity in the political relationship"(Lindsay, 2015) As we have seen before the field of cybersecurity represents a lot of questions because getting the information is really hard. Nevertheless, in recent years, China has started to be more assertive in terms of their policies and goals in the world, taking more firm steps with its neighbor countries and in International Organizations, which can create better opportunities for the better understanding of both countries' policies.

Political openness is a challenge in the eyes of China since its a threat to its legitimacy and to the party and the whole status quo. The notion of cybersecurity is different, the United States emphasizes the technical threats while China poses greater weight on ideological threats. Politically, for China, the control of information content is a main component of their notion of information security.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Another challenge for China in this matter is its fragmented Cyber defenses, as Lindsay (2015) calls it. The law enforcement concerning cyberspace in China is "Lax and uneven (…) cyber policy coordination among defense, law enforcement, and regulatory agencies is a challenge in any state, but China's lack of governmental transparency makes a hard problem worse"(Lindsay, 2015)

Theoretically, this political dimension, from the realist perspective in which they believe that in a world of unipolarity other powers will rise to challenge the predominant position of the strongest state this unipolar world may not last a long time. (R. Li, 2004) From this realist point of view, the cybersecurity supremacy of the United States could be challenged by a more and more economically and technologically prepared China, which will bring instability to the system. And politically both countries would try to impose their systems, the United States arguing for the openness and freedom while China advocating for the respect of the sovereignty.

Borrowing some insights from the liberalism, who believe in institutions and norms as a way to avoid conflict and bring countries together, the differences between the United States and China represent an opportunity. This opportunity to create norms and institutions to rule the cybersecurity could create the perfect environment for both countries to have high official meetings to reach agreements and instead of creating discussion, encourage dialogue.

In the military dimension in the US-China relations regarding cybersecurity, there is always the question behind, in the event of military conflict how would both countries react in the cyberspace? Traditionally, cyberwarfare attacks aim mainly at the adversary's means of fighting, like its technological systems and institutions. In this context, given the development of the US capabilities in the cyberspace "the United States brings a much better foundation to the

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

battle than China does" (Heginbotham et al., 2015) in this case, this might pose a challenge for China who will need to improve its cyberwarfare capabilities even faster. The opportunity, in this case, is for the United States that could take advantage of its current advantage and keep the distance from China, by developing new and more sophisticated technologies.

For the Economic dimension, there are more opportunities than challenges and both countries have already taken advantage of these opportunities. In the recent years, the two countries are each other's largest trading partner already, growing bilateral trade to more than $650 billion in 2016. Even though both countries profess different economic models, they have overcome most of the disputes and created a better ground for new opportunities. Nevertheless, in this dimension on of the problems concerns cybersecurity. Most of the cyber intrusions from China to the United States have, as I have discussed earlier in this thesis, targeted private institutions with the goal of stealing intellectual property, this creates a challenge for the bilateral relation but in this specific case, "China and the United States seem to cooperate more after an attack; this is probably because the issues at stake in cyber actions are of such low salience that they do not provoke antagonistic reactions"(Valeriano & Maness, 2018). It is a well-known fact that money is a key variable in the development of both countries so it makes sense to think that they would do all it takes to try to keep this variable running as smooth as it can be.

The institutional dimension brings more challenges than opportunities given the Chinese rejection to the Western strengths in this international normative model. Simply put, China and the United States do not agree on how to set up the norms of the internet. The United States multistakeholder model versus China's internet sovereignty model "involves not only technical

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

standards and protocols, but also alternative visions of global political order, one based on authoritarian states and the other on liberal globalization"(Lindsay, 2015)

The Obama administration released its International Strategy for Cyberspace in which their goal is to create "an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation"(White House, 2011) While China, together with Russia proposed the International Code of Conduct for Information Security at the United Nations in 2011 as well. This aims to promote constructive and responsible behavior and enhance their cooperation in addressing common threats and challenges while asks the countries to voluntarily cooperate with one another to fight against the so-called three evils: terrorism, secessionism, and extremism.

These opposite views on the internet bring challenges to China, which are mentioned throughout the document, for example, internet censorship is illegitimate, and the US will work against it, intellectual property theft is unacceptable, and all the countries must enforce laws protecting ideas. (Lindsay, 2015) So we can see that a major reform in the current regime of the internet is highly unlikely and will remain as a challenge for the bilateral relationship.

4.4 Summary

This fourth chapter serves as the description of the way both countries have approached each other in dealing with the cyberspace. Here I found that internationally, China is seen as an important country in Cybersecurity index but it falls way behind the US when they measure their scores. This is in accordance to the Chinese rhetoric of the state sovereignty principle. I

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

described as well the official mechanisms of dialogue such as the one established by President Obama and President Hu, in which the cyberspace talks were not really relevant until both presidents reached the agreement in 2015. Because of this reason, I described other non-official dialogue mechanism organized by an American and a Chinese think-thank in which officials and experts from both governments exchange ideas. This dialogue might not represent the official views of the governments nevertheless, following their meetings helps me picture the cybersecurity problem throughout the years, their ups and downs. I also described the challenges and opportunities for the US and China regarding Cybersecurity and I grouped them in four different dimensions: The political, the military, the economic and the institutional dimension.

From the realist point of view, the cybersecurity supremacy of the United States could be challenged by a more and more economically and technologically prepared China, which will bring instability to the system. From the liberal point of view, the differences between the United States and China represent an opportunity. This opportunity to build norms and institutions to rule the cybersecurity could create the perfect environment for both countries to have high official meetings to reach agreements and instead of creating discussion, encourage dialogue.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Chapter 5 Walking towards the same goal: finding ways to avoid further conflict

5.1 The United States and China: how to arm the cyber puzzle

On September 22, 2015, Xi Jinping arrived to the United States for his first state visit. President Obama and President Xi held two rounds of talks over two days in which they agreed to build bilateral ties featuring no conflict, no confrontation, mutual respect and win-win cooperation, according to the Xinhua News Agency.

This State Visit came in difficult times for both countries. Washington accused China of very damaging cyberattacks, China at the time devaluated its currency which made the trade deficit with the United States even worst, it also accelerated its military buildup in the South China Sea over the objections of Washington and its allies.

As soon as President Xi arrived to the United States, he said in a speech in Seattle that "The Chinese government will not in whatever form engage in commercial theft, and hacking against government networks are crimes that must be punished in accordance with the law and relevant international treaties". According to the New York Times, President Xi told an audience of American and Chinese business leaders "China is ready to set up a high-level joint dialogue mechanism with the United States on fighting cybercrimes (…) We are ready to strengthen cooperation with the US side on this issue"

During this Visit, both presidents exchanged views on global, regional, and bilateral subjects. Concerning the Global and Regional Challenges, they discussed the case of Afghanistan, their commitment towards Peacekeeping, their engagement to deepen their

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

cooperation on nuclear security, Wildlife Trafficking, and Ocean Conservation. They also signed a Memorandum of Understanding that established a framework for development cooperation to guide their future collaborative efforts. This Memorandum focuses on five things: the 2030 Agenda for Sustainable Development, Food Security, Public Health and Global Health Security, Humanitarian Assistance and Disaster Response, and Multilateral Institutions.

One of the most important parts of the visit was about Strengthening Bilateral Relations in four key elements: Military Relations, Cybersecurity, Law Enforcement and Counterterrorism and People-to-People Exchange. It is a really important step forward that cybersecurity is treated as a single issue, and it has not adhered to another category such as military relations, economic relations, or law enforcement.

The agreement regarding cybersecurity is regarded as a huge improvement in this field, since its the first time both governments reach some sort of consensus. The agreement has four main points, The White House (2015) published a fact sheet in which they detailed the specifics, the first point being:

> The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory. Both sides also agree to provide updates on the status and results of those investigations to the other side, as appropriate.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

As we can see from the agreement, the way they see that the cyber puzzle can be armed is through exchanges of information. The agreement acknowledges that both sides have different national laws nevertheless they agreed "to cooperate, in a manner consistent with their respective national laws and relevant international obligations"(The White House, 2015). This approach is really interesting, especially for the first formal agreement of its type since it's not focusing in shaping the system but adapting each others system and try to work together without paying attention to their differences. The results investigations as well should be shared, "as appropriate" which is a really appropriate way to say that they will do so just whenever they think it's appropriate. The second element in the agreement according to the White House(2015) is:

> The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors

Issues regarding cyber-enabled theft of intellectual property were and its still are a longstanding issue. In 2011, the US International Trade Commission estimated American Intellectual Property intensive firms lost $48 billion in 2009 because of hackings coming from China. The United States has even brought this case to the World Trade Organization to try to overcome it with the help of an independent Institution. Intellectual Property refers to creations of the mind, such as inventions, literary and artistic works, and designs, symbols, names, and

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

images used in commerce, according to the definition provided by the World Intellectual Property Organization. The third element in the agreement according to the Fact Sheet (The White House, 2015) says:

> Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. The United States and China welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International security, which addresses norms of behavior and other crucial issues for international security in cyberspace. The two sides also agree to create a senior experts group for further discussions on this topic.

The apparent will to engage with the norms os state behavior within the international community is also a factor. It seems so far away from the traditional rhetoric that China has traditionally advocated for: the respect of sovereignty even in cyberspace. The last part of the agreement according to The White House(2015) is:

> The United States and China agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. China will designate an official at the ministerial level to be the lead and the Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State Internet and Information Office will participate in the dialogue. The US Secretary of Homeland Security and the US Attorney General will co-chair the dialogue, with participation from representatives from the Federal Bureau

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

of Investigation, the US Intelligence Community and other agencies, for the United States. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. As part of this mechanism, both sides agree to establish a hotline for the escalation of issues that may arise in the course of responding to such requests. Finally, both sides agree that the first meeting of this dialogue will be held by the end of 2015, and will occur twice per year thereafter.

It is the first time that both countries agree on establishing a high-level joint dialogue mechanism on fighting cybercrime and related issues. This was one of the main recommendations from the multiple dialogue events carried before by both the Center for Strategic Studies and International Studies (CSIS) and the China Institute of Contemporary International Relations (CICIR). Even though this agreement is mostly meant to prevent the economically driven cyber espionage, particularly the theft of intellectual property and trade secrets, it is considered as a positive step forward in a very sensitive area. (Renard, 2015)

5.2 The role of leaders in reaching agreement in trying to set up some rules for the cyberspace.

President Obama assumed office in 2009 for the first time, and since then having positive relations with China was a priority for the US. Obama himself said: “The relationship between the United States and China is the most important bilateral relationship of the 21st century”. President Obama became in 2009 the first American president to visit China during the first year in office. Authors such as Cheng Li (2016) say that during Obama’s presidency, the President

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

“stressed the need for the United Staes to integrate itself into a changing world rather than stomp around arrogantly and blindly”(C. Li, 2016) Furthermore he, expressed that “the United States welcomes the rise of China”.

This principle might be consistent to Obama’s decisions with China given the fact that as we reviewed before they found a way, even though kind of abstract, to get together and try to integrate themselves rather than just attacking them directly with more tariffs.

Traditionally China’s conceptions were revolutionary but weak internationally. Nevertheless, when President Xi Jinping, assumed its position in 2012 China’s reality was a bit different, the reality of China had changed dramatically from the China his predecessors ruled. At the time, China was already the second largest economy in the world and the world’s largest trading country. It was the biggest destiny of foreign direct investment after the United States and fastest source of outward direct investment. It was the largest scale manufacturing country in the world, the largest trading partner of every country in South Asia. Also, China’s military capabilities were being revitalized and modernized slowly.

It is important to note this new reality for China when Xi Jinping assumed the leadership to understand Xi Jinping’s actions in the world. During the era of Deng Xiaoping, China’s Foreign Policy was characterized by its interdependence with the outside world and adherence to International Institutions and norms. This new era of success has allowed President Xi to act more confidently internationally, “allowing China to selectively stand outside of the established international order or to establish new competing institutions” (Bader, 2016)

During Xi’s period, China has strengthened its political, economic, and military position in the world and especially in East and Central Asia. In the economic arena, China consolidated

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

his position as the dominant actor in the region by establishing the Asia Infrastructure Investment Bank (AIIB), an institution that challenges the role played by the World Bank and the Asian Development Bank in Asia.

5.3 The Process of Negotiation: Why did they decide to agree in such a conflictive matter?

If I had to choose a word to describe US and China I would certainly pick deficit. It's hard to describe them either as friends or enemies because the relationship does not really fit in any of those fully. Their political and security interest and conceptions of the world are not always similar. Yet they are not really adversaries, either. They do not really see each other as a security or ideological threat, and the fact that their economies are so dependent on each other makes both countries try to diminish those differences to avoid conflict (Pei, 2014).

Deficit nevertheless is present in most of the areas of the bilateral relation. US-China Trade deficit, for example, was $375 billion in 2017 according to the United States Census Bureau. This simply because the United States is buying more from China than China is buying from the United States. US exports to China were $130 billion while imports were $506 billion in the same year.

Most importantly, the bilateral relation suffers from a "trust deficit" and in the case of the cyberspace, the lack of trust can be highlighted. As I discussed in previous chapters, cyber espionage issues have strained the bilateral relations since early 2000. This created uncertainty and since 2010 Chinese cyber activities in the US started to become a vividly discussed topic by the US Government, press and people. Since then the United States and China have accused and counter-accused each other. The US complaining about cyber attacks coming from China aiming

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

to steal IP, while China has criticized the US "for using its commanding position in cyberspace to secure advantages for its own intelligence gathering"(Brown & Yung, 2017a)

The year before they reached the agreement, the US Department of Justice (DoJ) accused five Chinese Army officers of stealing trade secrets and other information from US firms in order to give it to Chinese firms and benefit them economically. The Chinese Army officers were accused of using malicious code to access the computers and infiltrate the networks of Westinghouse Electric, the United States Steel Corporation, and other companies. The stolen information was delicate, including both technical data and information about trade negotiations. This event was called by the New York Times as the most direct confrontation in the Obama administration with China. The direct involvement of the Department and the public condemnation of the issue by the US government was a completely new approach "The indictment was seen as a shot across the bow to China, signaling that the United States was growing more serious about taking action against China for its commercial espionage" (Brown & Yung, 2017a)

Even though the US government knew that there was no chance that the Chinese would turn over the five officers named in the indictment, the move can be seen as highly symbolic. This happened two years later Edward Snowden disclosed information about United States' efforts in spying China. Nevertheless, The US decided to ignore this and focus in their most favorable "treasure" to fight for: intellectual property. The US focused the cybersecurity in this intellectual property theft, Attorney General Eric H. Holder Jr even said that "When a foreign nation uses military or intelligence resources and tools against an American executive or

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

corporation to obtain trade secrets or sensitive business information for the benefit of its state-owned companies, we must say, 'Enough is enough',"

China, on the other hand does not make a distention between economic and national security and they have used Snowden's disclosures about the NSA to point out that the position of the United States is hypocritical because they are also launching attacks directer to China, trying to steal information from the Government, Universities, and even Chinese military systems. Right after the accusations were publicly made, China reacted saying that this issue "grossly violates the basic norms governing international relations and jeopardizes China-US cooperation" and it protested against the US accusations.

Authors such as Gary Brown and Christopher D. Yung argue that the anger expressed by the Americans convinced Chinese officials that the United States was ready to do something else, like economic sanctions against China, so it "set the stage for talks between the two nations" (Brown & Yung, 2017a).

And as I discussed before, those talks happened a year after in 2015, resulting in the first cybersecurity agreement, in which both presidents stated that there was a need to increase the communication and cooperation between the two countries to investigate and prevent cybercrimes coming from their respective territories, and neither the US nor China would purposely conduct or support any cyber theft of intellectual property. They also committed to identifying, developing, and promoting appropriate norms of state behavior in cyberspace and establishing high-level joint dialogue mechanisms on fighting against cybercrimes.

Both countries, especially China decided to immediately have presidential talks in order to avoid hurting their economic exchanges through economic sanctions. It seems that this is

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

exactly the key element that moved them towards having executive talks. Analyzing this through the lenses of the Realist theorist we could assume that both the United States and China just decided to cooperate in order to prevent advances in the relative power of each other. According to the theory as well, States might even let go of some opportunities to increase their absolute capabilities if doing so contributes to a more stable distribution of power. So it can be possible that even though the United States had the technical opportunity, given its supremacy in technology, it let the opportunity go just to avoid further conflict with China. Because as Waltz says "the first concern of states is not to maximize power but to maintain their positions in the system" (Waltz, 1979) In this view, The United States would be just looking to maintain their superior position in the cyberspace and they are trying to avoid war by effectively (or at least try to effectively) control the use of cyberattacks.

The Liberal idea that says that peace can be achieved through cooperation and consensus could be easier to portrait in this agreement. The only part that this theory lacks to explain is why two countries with different ideologies and almost opposite views on cybersecurity get together and discuss ways to avoid conflict. Some liberal authors might say that cyberwar is like any other war so the democracies do not attack democracies would also apply here, but it seems that it's not the case for The US and China. Since there was a deficit of mutual trust in this bilateral relation it was hard for both countries to imagine the future of the agreement, and about this Liberalism does not provide enough information on how liberal norms and institutions would effectively work.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

5.4 The 2015 agreement in perspective

Now that I can see and analyze the agreement in perspective, I have found among the sources that I consulted divided opinions, some are pointing out at the uniqueness of the agreement, given that it is one of the first of its kind, while others are tremendously skeptical about it "The entire process is been seen by some as an elaborate way of saying that the two sides agreed to nothing"(Brown & Yung, 2017b).

After the agreement was made, President Xi continued denying China's involvement in the theft of commercial secrets, which made a lot of people skeptical about the willingness of China to do something about the issue. Internally, China referred to the agreement as a consensus making it even more difficult to know what that really means. "China believes each party has the right to exercise the discretion in how to proceed. By contrast, the United Staes believes the two sides have agreed to specific measures"(Brown & Yung, 2017b) The US-China agreement served as a way for China to express its willingness to get closer with western countries and was the predecessor for a United Kingdom-China agreement. In the case of the United States, days after the visit, President Obama noted that: "the question now is, are words followed by actions?" according to *The Atlantic* (Kelly & Foran, 2015).

A few days after the agreement, according to *The Diplomat* (2017b), the FBI reported that hackers based in China had hacked into companies contracted with the Navy and Marine Corps, stealing military information. Given that the agreement mostly is about protecting Intellectual Property theft, these actions do not necessarily violate the agreement, as the agreement doesn't state that countries can't collect classified information useful for their national security interests.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Weeks in, a company called CrowdStrike Inc. said that it detected at least seven cyberattacks against US technology and pharmaceutical companies targeting Intellectual Property. These incidents could be an indicator of how successful or unsuccessful the agreement was at the moment. “I haven’t seen any evidence of increased arrests in China for ‘cyber-enabled theft of intellectual property’ outlined in the agreement, even though the idea was for more cooperation on investigating crimes. The number of incidents reported in recent months looks to be similar to those before the agreement, so we have no real evidence of any changes yet” said Sarah Granger, form the Truman National Security Project.

On the other hand, there are also entities such as NBC News that report that after the agreement was set up, Chinese hacking thefts of American corporate secrets plummeted in the months after. The co-founder of the same company that reported the cyberattacks right after the agreement, Dmitri Alperovitch, also said to NBC that they observed a 90 percent drop in commercial hacking against the United States attributable to Chinese Government actors. But he also acknowledged that Chinese intelligence agencies are still hacking to steal national US security secrets, but his company doesn’t consider them as a big problem given the fact that he said it is exactly what the NSA is also doing to China and other US adversaries.

Adam Segal also says that the agreement has been relatively working, he argues that The Chinese hackers may have shifted activity to Southeast Asia. Also, China has seen an increase in domestic intrusions against companies in China.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

5.5 Summary

In this chapter, I described President Xi's first state visit to the United States, and how it became a breaking point in terms of cybersecurity given the fact that because of it, both Presidents officially agreed to enhance security in the cyberspace. This agreement consists of four main points: provide timely responses to requests for information and assistance concerning malicious cyber activities, refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property, pursue efforts to further identify and promote appropriate norms of state behavior in cyberspace within the international community, and establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. I also analyzed the role of both presidents in reaching this agreement and some ideas in which by using the theoretical framework described in the first chapters try to detail why they decided to cooperate in a conflictive matter such as cyberspace. Finally, I show the official reactions both governments had after the state visit and I analyzed what experts say about the number of the attacks after the agreement, to see if they actually decreased or increased.

By using the neorealist theoretical framework I assume that both the United States and China just decided to cooperate in order to prevent advances in the relative power of each other. According to the theory as well, States might even let go of some opportunities to increase their absolute capabilities if doing so contributes to a more stable distribution of power. So it can be possible that even though the United States had the technical opportunity, given its supremacy in technology, it let the opportunity go just to avoid further conflict with China. Because as Waltz says "the first concern of states is not to maximize power but to maintain their positions in the

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

system" (Waltz, 1979) In this view, the United States would be just looking to maintain their superior position in the cyberspace and they are trying to avoid war by effectively (or at least try to effectively) control the use of cyberattacks.

On the other hand, the agreement was easier to portrait by using the Liberal framework, since they say that peace can be achieved through cooperation and consensus, so in order to maintain the status quo, and avoid the sanctions they must cooperate.

國立政治大學
National Chengchi University

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Chapter 6 Conclusions

With the aim of assessing cybersecurity and United States-China relations, the transformation of the security concepts, their views on cybersecurity, the way they address each other, and the ways they dialogue, this thesis was conducted. The results and views of the individual assessments are to be summed up and written as a final result of this research in the following last chapter.

The rapid development in technology and the rise of new ways to interconnect people, governments and companies have led to dramatic changes in the interaction between them. These new ways to interact have had enormous implications for security, given that it can be seen as an opportunity or a threat for states and organizations.

Cybersecurity has been in this matter, an issue of greater importance in International Relations, nevertheless because of its novelty there is a lot of speculation. Cyberwar and cyberconflict have become dominating issues of concern in International Relations. And as Henry Kissinger stated, "Cyberspace challenges all historical experience (…) the definition of the state authority might be ambiguous" (Kissinger, 2015) when he is referring to the multiplicity of actors in the cyberspace.

The central questions of this thesis were why such a new issue like cybersecurity has become a national security priority for states such as the United States and China? How they view cybersecurity? Why do they decide to cooperate and officially agree in a cybersecurity agreement? And what are the future challenges and opportunities for the bilateral relations?

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

These questions were guiding the research from the first chapter, which helped to give insightful background information on the issue. Here we learned that there are only a few countries that can be considered superpowers and also, that security as a concept it's traditionally entailed with threats. And in the case of cybersecurity, it is no different since it is creating new types of threats for almost every country, especially when they're strong and dependent on computer networks.

The second chapter reviews the existing literature and gives the conceptual framework to better understand relevant concepts in this thesis. In this chapter, we concluded why Realism and Liberalism are relevant to analyze cybersecurity and why the United States-China relations in the 21st century is so important and in this context cybersecurity issues such as cyberespionage and information theft were a great factor in creating instability in the bilateral relation.

The third chapter analyzed each country's approach on cybersecurity, the conclusion is that both approaches have contrasting features. In this matter, we notice that the United States and China have both different approaches to protect their cybersecurity. After all the research done, it is safe to say that China pursues cyber policy goals that are sometimes seen as highly conflictive with the cyber policy goals the United States or even the broader international community are pursuing. On the one hand, the United States' vision of the cyberspace is one characterized by its openness, its multiplicity, and its multistakeholder governance, on the other hand, China's vision is for a system more regulated by the government in which all the content available needs to be regulated and approved in advance. China's goals are to maintain its stability and its sovereignty over its domestic cyberspace. The United States cybersecurity policies focus on attacking threats to networks, cyberinfrastructure, China also adds the threats

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

posed by online content. For them, its online structure domestically is intended to work like that to defend themselves against not only domestic but also foreign influences, that is the case of the explosion of western internet companies such as Google and Facebook from China.

The fourth chapter started by describing how each country is regarded and scored internationally when they measure their status of cybersecurity. Then it described the dialogue between the United States and China regarding cyberspace, first the US-China Strategic and Economic Dialogue (S&ED or 中美戰略與經濟對話 in Chinese), in which the issue of cybersecurity was not really present until President Obama and President Xi signed the agreement in 2015, and other dialogue channels such as the one organized by the think thanks The Center for Strategic Studies and International Studies (CSIS) and the China Institute of Contemporary International Relations (CICIR) which invite officials from both governments and experts. The conclusion is that there are still challenges and opportunities for these countries regarding cybersecurity, and I detailed them in four different dimensions: The political, the military, the economic and the institutional dimension.

The fifth chapter detailed President Xi's first state visit to the United States which in my conclusion represents a breaking point in terms of cybersecurity. The role of both leaders was a key element in reaching this agreement since both showed their will to do something in this matter. This chapter is of vital importance because is in this one where I answer one of the main questions of the thesis: why did they decide to cooperate? I answered them by using both theoretical bodies to arm a more complete answer. The end of the chapter described the official reactions both governments had after the state visit and I analyzed what experts say about the number of the attacks after the agreement, to see if they actually decreased or increased.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

After the research on the United States and China we observe that they have significant differences in almost every aspect, and cybersecurity and cyberspace are not the exceptions. The definitions and objectives differ which makes the approach sometimes a tricky and not so easy one. Both countries have a shared interest in avoiding the misperceptions and miscalculations that could lead to conflict, they also share the same interest in finding measures that can be suggested to the two governments to reduce tensions in the cyber arena. They also found out after the simulations that both Staes have formal processes for dealing with cyber crimes, but there is no identified channel of communication, reason why they agree that creating a formal approach to communicating in a crisis would be useful and necessary.

Mistrust is a word that would define the talks since they started dialoguing back in 2009. Although there is one obvious thing that remains constant in all the talks "for the United States, China should stop stealing so much intellectual property; and for China, the US should stop trying to maintain its hegemony in cyberspace, contain Beijing, and militarize cyberspace"(Segal, 2012). It is hard to make more assumptions without knowing exactly what happens behind closed-door meetings.

A way to tackle this lack of trust is through exchanges of information and the 2015 agreement marks a new era since it was the first time that both countries agree on establishing a high-level joint dialogue mechanism on fighting cybercrime and related issues. In my opinion, China in relatively few days decided to sign up to a list of norms the United States was pushing and China was not looking for at all, because at that time China just wanted to calm the agitated situation, trying to avoid the sanctions Obama's administration was pushing, signing this agreement was a way to show the United States their will to cooperate. The conclusion is that

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

there are at least three ways to explain this: First, the Chinese government did not have any intention of applying any of these aspects in the agreement. Second China would apply the norms but only partially, respecting its own sovereignty at all cost. Third, China would do everything as agreed. At the time of the agreement scholars agreed that it was too soon to tell, but now, 3 years after we can see what has happened.

The agreement was a step forward nevertheless, it still falls short because, even though its a fact known from the beginning, it won't stop all hacks or espionage coming from either country, that is virtually impossible to do. Also, the agreement is too specific, it targets state-sponsored cyberattacks targeting intellectual property, and ignores other cyberattacks such as attacks on governments infrastructures or election processes.

Finally, after all the research and analysis we can say that the hypothesis mentioned in the earlier chapters of the thesis can be proved right, since the Foreign Policy Decisions on cyber superpowers such as the United States and China have resulted in a digitalization because the cybersecurity talks are never left behind in almost any of the official dialogues since 2015. Before the 7th round of the S&ED (中美戰略與經濟對話) in June 2015cybersecurity issues were never addressed officially, but since then, and especially after the high-level agreement, they have been present almost every time, which will prove right the idea of "digitalization" of the practices of foreign policy mentioned in my hypothesis.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

6.1 Future of the cyber world and IR: the case of the United States and China

On October 2017, the Attorney General Jefferson B. Sessions III and Acting Secretary of Homeland Security Elaine Duke, together with Chinese State Councilor and Minister of Public Security Guo Shengkin, co-chaired the first US-China Law Enforcement and Cybersecurity Dialogue (LECD). This is one of four dialogues agreed to by President Trump and President Xi during their first meeting in April 2017. They discussed repatriation, counter-narcotics, cybercrime and cybersecurity and fugitives.

Even though differences still remain, it seems that both sides try to make some progress, at least officially on issues such as cybercrime. In the specific topic regarding Cybersecurity they both said that they will continue their implementation of the consensus reached by President Obama and President Xi on 2015, regarding US-China cybersecurity cooperation. They will continue implementing five main points: first, that timely responses should be provided to requests for information and assistance concerning malicious cyber activities; second, that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors; third, to make common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community; fourth, to maintain a high-level joint dialogue mechanism on fighting cybercrime and related issues; and fifth, to enhance law enforcement communication on cyber security incidents and to mutually provide timely responses.

The US-China is one of the most relevant relationships in the world, they both require a stable environment to benefit from the smooth functioning of the economic system. It seems that

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

the Cybersecurity issues won't be resolved anytime soon. The process of understanding each other and overcome the "trust deficit" won't be an easy one in the short term. It will require more willingness to approach, and the role of the leaders is a key element in this realm. Donald Trump seems a bit more reluctant than his predecessor, so it will be a really interesting time not only for cybersecurity and United States and China but for the whole bilateral relations.

國立政治大學
National Chengchi University

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Bibliography

Adler, E. (2002). Handbook of International Relations. in London: SAGE Publications Ltd. Retrieved from http://sk.sagepub.com/reference/hdbk_intlrelations. doi: 10.4135/9781848608290

Bader, J. A. (2016). How Xi Jinping Sees The World & And Why. *Order From Chaos: Foreign Policy in a Troubled World*.

Baldwin, D. (1997). The Concept Of Security. *Review Of International Studies, 23*(1), (pp. 5-26). doi:10.1017/S0260210597000053

Baylis, J. (2008). The Concept of Security in International Relations. In H. G. Brauch, Ú. O. Spring, C. Mesjasz, J. Grin, P. Dunay, N. C. Behera, B. Chourou, P. Kameri-Mbote, & P. H. Liotta (Eds.), *Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century* (pp. 495-502). Berlin, Heidelberg: Springer Berlin Heidelberg.

Brauch, H. G. (2008). Introduction: Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century. In H. G. Brauch, Ú. O. Spring, C. Mesjasz, J. Grin, P. Dunay, N. C. Behera, B. Chourou, P. Kameri-Mbote, & P. H. Liotta (Eds.), *Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century* (pp. 27-43). Berlin, Heidelberg: Springer Berlin Heidelberg.

Brown, G., & Yung, C. D. (2017). Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace. *The Diplomat*.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Brown, G., & Yung, C. D. (2017). Evaluating the US-China Cybersecurity Agreement, Part 3: Over a Year Later, What Impact has the 2015 Cyber Agreement had on U.S.-China Relations? *The Diplomat*.

Bull, H. (1977). The Anarchical Society: A Study of Order in World Politics. *New York*.

Buzan, B. (1983). People, States, and Fear: The National Security Problem in International Relations: Wheatsheaf Books.

Buzan, B. (2008). The Changing Agenda of Military Security. *Globalization and Environmental Challenges*, (pp. 553-560).

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*: Lynne Rienner Pub.

China Internet Network Information Center. (2017). Statistical Report on Internet Development in China. In: CNNIC Beijing.

Choucri, N. (2012). *Cyberpolitics in International Relations*: MIT press.

Coats, D. R. (2017). *Worldwide Threat Assessment of the US Intelligence Community*. Retrieved from https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf.

Dunne, T., Kurki, M., & Smith, S. (2013). *International Relations Theories*: Oxford University Press.

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) Relevant Theory? *International Political Science Review / Revue internationale de science politique, 27*(3), (pp. 221-244).

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Farrell, H., & Glaser, C. L. (2017). The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine. *Journal of Cybersecurity, 3*(1), (pp 7-17). doi:10.1093/cybsec/tyw015

Fountain, J. (2004). Building the Virtual State: Information Technology and Institutional Change: *Brookings Institution Press*.

German Federal Ministry of the Interior. (2011). *Cyber Security Strategy for Germany*. Federal Ministry of the Interior Retrieved from https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile.

Gierow, H. J. (2014). Cyber Security in China: New Political Leadership Focuses on Boosting National Security Restructuring Internet Regulation. Placing Restrictions on Foreign Software. Developing the PRC's own IT Standards. *China Monitor*.

Glaser, C. L., & Kaufmann, C. (1998). What is the Offense-Defense Balance and how can we Measure it? *International Security, 22*(4), (pp. 44-82).

Hanson, E. C. (2008). *The Information Revolution and World Politics*: Rowman & Littlefield Publishers.

He, R. (2013) China Opposes and Combats Cyber Attacks. Financial Times.

Healey, J. (2013). China is a Cyber Victim, too. *Foreign Policy*(April 16).

Heginbotham, E., Nixon, M., Morgan, F. E., Hagen, J., Heim, J. L., Engstrom, J., . . . Libicki, M. C. (2015). *The US-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017*: Rand Corporation.

Hennessey, S. (2017). Deterring Cyberattacks: How to Reduce Vulnerability. *Foreign Affairs, 96(6),* (pp. 39-46).

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Jackson, R. H., & Sørensen, G. (2007). *Introduction to International Relations: Theories and Approaches*: Oxford University Press.

Jørgensen, K. E. (2017). *International relations theory: A new introduction*: Macmillan International Higher Education.

Kaplan, F. (2016). *Dark Territory: The Secret History of Cyber War*: Simon & Schuster.

Kelly, N., & Foran, C. (2015). President Obama and Chinese President Xi Jinping Announce Cybersecurity Agreement. *The Atlantic*.

Kissinger, H. (2015). *World order*: Penguin Books.

Koselleck, R., & Presner, T. S. (2002). *The Practice of Conceptual History: Timing history, spacing concepts*: Stanford University Press.

Kremer, J.-F., & Müller, B. (2014). SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World. In *Cyberspace and International Relations* (pp. 41-58): Springer.

Kshetri, N. (2013). Cyber-Victimization and Cybersecurity in China. *Commun. ACM, 56*(4), (pp 35-37). doi:10.1145/2436256.2436267

Kshetri, N. (2016). Cybersecurity in China. In *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies* (pp. 123-143). Cham: Springer International Publishing.

Kshetri, N. (2016). *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*: Springer International Publishing.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. *Cyberpower and national security*, (pp. 24-42).

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Li, C. (2016). Assessing US-China Relations Under the Obama Administration. *Brookings Institution, 5*.

Li, R. (2004). Security Challenge of an Ascendant China: Great Power Emergence and International Stability. *Chinese Foreign Policy: Pragmatism and Strategic Behaviour, East Gate, New York*, (pp. 23-58).

Lieberthal, K., & Singer, P. W. (2012). *Cybersecurity and US-China relations*: Brookings.

Lindsay, J. R. (2015). The impact of China on Cybersecurity: Fiction and friction. *International Security, 39*(3), (pp. 7-47).

Longdi, X. (2014). China's Internet Development and Cybersecurity–Policies and Practices. *Chinese Cybersecurity and Defense*, (pp. 1-54).

Molyneux, S. (1999). Broadband Internet: Future Applications and Challenges. In J. Vince & R. Earnshaw (Eds.), *Digital Convergence: The Information Revolution* (pp. 3-12). London: Springer London.

Nye, J. S. (2011). *Nuclear Lessons for Cyber Security?* (Vol. 5): Strategic Studies Quarterly.

OECD. (2011). *Cybersecurity Policy Making at a Turning Point*: OECD Publishing.

Parker, E. (2017). Hack Job: How America Invented Cyberwar. *Foreign Affairs, 96(3)*, (pp. 133-138).

Pei, M. (2014). How China and America See Each Other. *Foreign Affairs, 93*(2), (pp. 31-32).

Petallides, C. J. (2012). Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat. *Inquiries Journal/Student Pulse, 4*(03). Retrieved from http://www.inquiriesjournal.com/a?id=627

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

Radu, R. G. (2012). The Monopoly of Violence in the Cyber Space: Challenges of Cyber Security. In E. Fels, J.-F. Kremer, & K. Kronenberg (Eds.), *Power in the 21st Century: International Security and International Political Economy in a Changing World* (pp. 137-150). Berlin, Heidelberg: Springer Berlin Heidelberg.

Renard, T. (2015). US-China Cybersecurity Agreement: A Good Case of Cyber Diplomacy. Egmont Commentary, 1 October 2015.

Romanosky, S. (2016). Examining the Costs and Causes of Cyber Incidents. *Journal of Cybersecurity, 2*(2), (pp. 121-135). doi:10.1093/cybsec/tyw001

Rulog, H. (2013) *China Opposes and Combats Cyber Attacks*. Financial Times.

Segal, A. (2012). U.S. and China in Cyberspace: Uneasy Next Steps. In: Council on Foreign Relations.

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*: Hachette UK.

Segal, A. (2017). How China is Preparing for Cyberwar. *The Christian Science Monitor*.

Sutter, R. G. (2013). *US-Chinese Relations: Perilous Past, Pragmatic Present*: Rowman & Littlefield Publishers.

The International Telecommunication Union (ITU). (2008). *Overview of Cybersecurity, Recommendation ITU–T X.1205*. Paper presented at the The ITU Plenipotentiary Conference 2010, Guadalajara, Jalisco, Mexico. http://tinyurl.com/boys7dj

The International Telecommunication Union (ITU). (2017). Global Cybersecurity Index 2017. In: ITU.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

The White House. (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington D.C.: White House.

The White House. (2013). Executive Order on Improving Critical Infrastructure Cybersecurity [Press release]. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0

The White House. (2015). *FACT SHEET: Cyber Threat Intelligence Integration Center. The White House, Office of the Press Secretary Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.*

The White House. (2015). Fact Sheet: President Xi Jinping's State Visit to the United States. *Press Release, 25*.

The World Bank. (2017). Individuals Using the Internet (% of population) [Table]. In (pp. Internet users are individuals who have used the Internet (from any location) in the last 3 months. The Internet can be used via a computer, mobile phone, personal digital assistant, games machine, digital TV etc.).

Thornburgh, N., Forney, M., Bennett, B., Burger, T. J., & Shannon, E. (2005). The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them). *Time Magazine, 29*, 1098961-1098961.

U.S. Department of Homeland Security. (2018). *Cybersecurity Strategy*. Retrieved from https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06

U.S. Department of the Treasury. (2009). Fact Sheet: U.S.−China Strategic and Economic Dialogue. Retrieved from https://www.treasury.gov/initiatives/Documents/SEDfactsheet09.pdf.

United States National Security Council. (2010). *Cyberspace Policy Review: Securing America's Digital Future*: Cosimo, Incorporated.

Valeriano, B., & Maness, R. C. (2018). International Relations Theory and Cyber Security. *The Oxford Handbook of International Political Theory*, (pp. 259).

Ventre, D. (2014). *Chinese cybersecurity and defense*: John Wiley & Sons.

Vince, J., & Earnshaw, R. (2012). *Digital Convergence: The Information Revolution*: Springer London.

Volz, D. (2016). Yahoo Says Hackers Stole Data From 500 Million Accounts in 2014. *Reuters*. Retrieved from https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-hackers-stole-data-from-500-million-accounts-in-2014-idUSKCN11S16P

Waltz, K. N. (1979). *Theory of International Politics*: Waveland Press.

Weibin, Z. (2017). The Four Stages of Sino-American Cyber Relations. In: China-United States Exchange Foundation.

Wu, X. (2005). *Chinese Cyber Nationalism: How China's Online Public Sphere Affected its Social and Political Transitions.* University of Florida,

中华人民共和国国务院. (2012). 国务院出台意见推进信息化发展切实保障信息安全.

DOI:10.6814/THE.NCCU.IMPIS.007.2018.A06