Cyber Hype Versus Cyber Reality – How Severe Is The Threat That Chinese Cyber-Attacks Pose To United States' National Security?

July, 2019

2337200T

17116287

64451738

Presented in partial fulfilment of the requirements for the Degree of

International Master in Security, Intelligence and Strategic Studies

Word Count: 23526

Supervisor: Dr. Damien Van Puyvelde

Date of Submission: 26 July 2019

CHARLES UNIVERSITY

Abstract

Cyber threats regarding China's political espionage and intellectual property theft have featured prominently in United States (U.S.) government's public discourse in recent years. This thesis examines the threats that China's cyber-attacks pose to U.S. national security and critically assesses whether the government discourse surrounding China's cyber-attacks accurately reflects the actual threats. Overall, the study shows that China's cyber-attacks do not pose an existential threat to U.S. national security, contrasting U.S. government officials' claims which tend to exaggerate and depict Chinese cyber-attacks as an existential threat. Based on cyber-attack data between the U.S. and China from January 2013 to May 2019, this paper observes that China primarily conducts long-term espionage, exerting economic, diplomatic and social impacts, but does not conduct any degradative cyber-attacks. The study also observes from government statements surrounding two cyber-attacks – Office of Personnel Management (OPM) hack and Operation Cloudhopper – that U.S. government officials exaggerated China's cyber-attacks in imposing counterintelligence impacts of mortal danger, and inflated China as an unprecedented threat that unfairly benefits Chinese firms at the expense of U.S. firms. This paper concludes that Chinese cyber-enabled political espionage poses intelligence and counterintelligence effects that affect U.S. national security. However, these effects do not constitute an existential threat to U.S. national security, unlike what U.S. government officials have claimed. The U.S. understands and responds to China's cyber-attacks, and thus poses an equal, if not greater, threat to China. This paper also asserts that cyber-enabled commercial espionage impacts U.S. national security via economic consequences, but it forms a small part of the broader systemic threat underlying China's other forms of legal and covert transfer of technology. The Chinese government's direct involvement in commercial espionage against U.S. firms may be exaggerated given the personal commercial incentives of private firms to unilaterally conduct commercial espionage. Overall, U.S. government

officials' accusations of China are weakened by similar cyberespionage activities that U.S. intelligence agencies conduct, the refusal or inability of the U.S. government to provide the public with direct evidence, and the muddling of national security issues with trade goals.

Table of Contents

ABSTRACT ..... **I**

LIST OF TABLES ..... **II**

LIST OF FIGURES ..... **IV**

LIST OF APPENDICES ..... **V**

GLOSSARY **1**

I. INTRODUCTION **2**

1.1 Background 2

1.2 Research Questions and Research Aims and Objectives 5

2.1 Theoretical Framework 11

2.3 Cyber Conflict – International Relations Perspectives and Impact on Traditional Concepts of Deterrence and Power 16

2.4 Rise of China and U.S.-China Rivalry in Cyberspace 22

III. CYBER REALITY **28**

3.1 Research Methodology 28

3.2 Presentation of Findings 34

3.2.1 Chinese Cyber Operations *34*

3.2.2 U.S. Cyber Operations *43*

IV. CYBER HYPE **47**

4.1 Research Methodology 47

4.2 Presentation of Findings 51

4.2.1 Case Study 1 – The OPM Hack *51*

4.2.2 Case Study 2 – Operation Cloudhopper *61*

V. DISCUSSION **73**

5.1 Cyber-enabled theft of Commercial data 73

5.2 Destructive Cyber-attacks 79

5.3 CYBER-ENABLED POLITICAL ESPIONAGE 81
5.4 THE WIDER IMPLICATIONS ON U.S.-CHINA RELATIONS 86

VI. CONCLUSION 89

VII. APPENDICES 95

VII. BIBLIOGRAPHY 119

Acknowledgements

I would like to express my deep and sincere gratitude to my supervisor, Prof. Damien Van Puyvelde, for providing me with the best possible advice and prompt support throughout my dissertation work.

I am also extremely grateful to my family and friends near and far, especially, who have been a constant support in my academic journey.

To my family, thank you for your investment of love and patience.
To my friends, thank you for your support and encouragement, especially Mehwish Rani, who has always helped and inspired me in my academic journey.
And finally to my most favourite person in the world, thank you for your endless love and care.

List of Tables

Table 1: Non-State Actors – Capabilities, Targets and Motives …….21

Table 2: Sources for Responsibility Confirmation ……..32

Table 3: First-order impact of Chinese Cyberespionage……..39

Table 4: Details of U.S. Cyber Operations……..44

Table 5: Habermas' (1984) Theory of Communication Framework applied to Textual Analysis of CDA …….. 50

Table 6: OPM Hack: Assessing Truth Claims of Cyber Incident, Threat Actor and Referent Object ……55

Table 7: OPM Hack: Naming of the Threat Actor……... 56

Table 8: OPM Hack: Examples of Rhetorical Devices…… 58

Table 9: OPM Hack: Types of Government Officials ……60

Table 10: Operation Cloudhopper: Assessing Truth Claims of Cyber Incident and Threat Actor ……..65

Table 11: Operation Cloudhopper: Naming of the Threat Actor ……..66

Table 12: Operation Cloudhopper: Examples of Rhetorical Devices……...68

Table 13: Operation Cloudhopper: Types of Government Officials ……...70

List of Figures

Figure 1: Threat Framework ……12

Figure 2: Assessment of Hype: Threat Politics Framework ……14

Figure 3: Coding Categories ……31

Figure 4: Types of Chinese Cyber Operations on the U.S. from Jan 2013 to May 2019…….....35

Figure 5: Nature of Chinese Cyber Operations on the U.S. from Jan 2013 to May 2019……..35

Figure 6: Percentage of Strategic vs. Tactical Chinese Cyber Operations on the U.S. from Jan 2013 to May 2019 …… 36

Figure 7: Strategic Objectives of Chinese Cyber Operations on the U.S. from Jan 2013 to May 2019 ……. 38

Figure 8: Chinese Strategic Espionage: Types of Targets and Sources …….. 38

Figure 9: First-order Impact of Chinese Cyberespionage Operations from Jan 2013 to May 2019 ……40

Figure 10: Total ongoing Chinese cyber incidents from Jan 2013 to May 2019 ……41

Figure 11: Overall Analytical Framework for Cyber Hype Analysis…….. 51

List of Appendices

Appendix 1 – List of Technical Terms and Definitions……95

Appendix 2 – Coding Table…….....98

Appendix 3 – Description of Coding Factors…….101

Appendix 4 – Archive Permission Form…….105

Appendix 5 – Sources of Government Claims for the OPM hack……..108

Appendix 6 – Sources for Government Claims of Operation Cloudhopper...112

Appendix 7 – U.S.-China Cyber Incidents Database (from 1 Jan 2013 to 31 May 2019)……...115

Glossary

APT	Advanced Persistent Threat
CCP	Communist Party of China
DDoS	Distributed Denial of Service
FBI	Federal Bureau of Investigation
IP	Intellectual Property
IR	International Relations
LOAC	Law of Armed Conflict
MSP	Managed Service Providers
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OPM	Office of Personnel Management
PII	Personally Identifiable Information
PLA	People's Liberation Army
PwC	Pricewaterhouse Coopers
R&D	Research and Development
SOE	State-owned Enterprise
SSF	Strategic Support Force
S&T	Science and Technology
U.S.	United States
USTR	Office of United States Trade Representative

I. Introduction

1.1 Background

Cyberspace represents a new stage for international conflicts. Over the past decade, states increasingly leveraged cyberspace to conduct low-intensity operations below the threshold of an armed attack. In 2010, the United States (U.S.) government allegedly attempted to disrupt Iran's nuclear production by releasing the Stuxnet worm and causing physical damage to uranium centrifuges. Following Stuxnet, Iran purportedly developed the Shamoon malware to retaliate against the U.S. by attacking its ally, Saudi Arabia, in 2012. Shamoon crippled production capacity and drove up oil prices (Valeriano & Maness, 2015). More recently, the WannaCry and NotPetya ransomware campaigns inflicted organisations worldwide including banks, hospitals and nuclear facilities in 2017. Wannacry was attributed by U.S. intelligence agencies to North Korea. NotPetya was attributed to Russia by a consortium of Western intelligence agencies in the U.S., Canada, Australia and the United Kingdom (Kovacs, 2018). China was charged by the U.S. with conducting a 12-year cyberespionage campaign that stole trade secrets and intellectual property from companies worldwide at the end of 2018.

These cyber-attacks highlight a shift in states' preference from engaging in open conflicts in the physical realm to low-intensity competition in cyberspace to gain cumulative strategic advantage (Nakasone, 2018). States are investing more resources to develop cyber capabilities – Russia, the United Kingdom and India have increased research and development (R&D) of cyber weapons and invested in cyber forces (Xu, 2017). The U.S. raised its Cyber Command to combatant status in May 2018 and relaxed its protocols for conducting offensive cyber operations. The North Atlantic Treaty Organisation plans to establish an independent Cyber Command by 2023. These moves suggest that the new locus of the global power struggle for political, economic and socio-cultural influence among states is shifting to cyberspace.

The shift of global conflicts to cyberspace has been traced to the emergence of cyber hype (Valeriano & Maness, 2015). In this paper, the term 'cyber hype' borrows the concept of hype as understood in media and communication studies – cyber hype can be a utility for altering meaning and increasing the news' appeal to the audience (Powers, 2012). Similar to Powers' (2012) definition, the Oxford English Dictionary defines hype as the "extravagant or intensive publicity or promotion" of an issue. As a verb, hype means to "promote or publicise (a product or an idea) intensively, often exaggerating its benefits" (Oxford Dictionaries, 2019). Cyber hype emerged when Arquilla and Ronfeldt, (1993) from RAND Corporation theorised cyberspace's potential in revolutionising military affairs. They posit that the pre-eminence of cyber warfare is key to winning future wars through new military strategies such as targeting the adversary's command and control structure.

However, optimism toward emerging information technologies experienced in the late 1990s gave way to pessimistic discourse about cyber war in a new millennium that began with worldwide panic over the anticipated failure of information technology systems (Cellan-Jones, 2018). In the aftermath of the Stuxnet cyber-attack, Clarke and Knake (2012) warned of the critical vulnerabilities that arise from an increasingly digitally interconnected world. Along with Greengard (2010) and Caplan (2013), they theorised that a single strike on a networked infrastructure by adversaries would create a domino effect on critical services such as transportation networks and power plants, resulting in a total collapse of society. Policy makers and intelligence officials in the U.S. reinforced the hype by referring to cyber war as akin to an "electronic Pearl Harbour" (Thomas, 1997). Barack Obama, the former President of the U.S. framed cyber-attacks as the "most serious economic and national security challenge" (BBC, 2012) while the U.S. Secretary of Defence Leon Panetta expounded on alarmist theories of terrorists using cyber means to carry out attacks (Panetta, 2012). By purposefully framing the increasing digitisation of the world as a threat, the academic and policy community in the U.S.

transformed the cyber war hype from fervent optimism in the 1990s to a doomsday discourse.

More recently, cyber threats from China have featured prominently in U.S. policy and intelligence circles. The 2019 Worldwide Threat Assessment by the U.S. Intelligence Community assessed China to present a "persistent cyber espionage threat" and a "growing attack threat" to U.S. critical infrastructure (Coats, 2019). Top officials from the Federal Bureau of Investigation (FBI) declared that China poses the "most severe" long-term threat to U.S. national security, exceeding that of longstanding U.S. adversary, Russia (Seldin, 2018). FBI Christopher Wray also described China's cyberespionage efforts as "the broadest" and the "most challenging threat" that the U.S. has faced (Lutz, 2018). U.S. foreign policy against China also adopted a more aggressive stance in denouncing Chinese cyber-attacks and indicting Chinese hackers. In October 2018, ten Chinese nationals, including two intelligence officers, were charged with stealing engine technology from U.S. and French aerospace firms over a 5-year period. Chinese company Huawei, the world's second largest mobile manufacturer and industry leader of the fifth-generation mobile network (5G) was brought into the spotlight after U.S. officials raised concerns about the firm's potential collusion with the Chinese government to covertly collect sensitive information via its telecommunication equipment. Despite the lack of publicly available evidence suggesting Huawei's ties with the Chinese government (Varghese, 2019), the U.S. government actively lobbied Japan, Italy, Germany and other key allies to ban China from participating in the 5G trials (Horwitz, 2018). The 5G trials are significant because 5G entails a much faster telecommunications network that paves the way for advanced technologies such as driverless cars. The U.S. also pursued legal actions by pressing criminal charges against Huawei for stealing technology and violating trade sanctions with Iran (Horowitz, 2019). Huawei has in turn alleged that the ban imposed on its products was unconstitutional according to U.S. laws (Yang, 2019). Amidst the brewing political conflict, China denied all allegations and

accused the U.S. of pushing Huawei out of the market based on political motives and of manipulating the market in favour of U.S. 5G technologies (Jiang & Westcott, 2019).

1.2 Research Questions and Research Aims and Objectives

In this context, the following research puzzle arises – Why did the U.S. express such severe concerns toward China's cyberespionage activities, using superlatives like "most severe" and "most challenging", given the long-standing nature of the threat of espionage (Laskai & Segal, 2018) and America's own spying capabilities? The U.S. National Security Agency's (NSA) PRISM surveillance programme has systematically monitored and collected global digital communications from foreign governments, companies and individuals (Amnesty International, 2018). Wikileaks also revealed in 2017 that the Central Intelligence Agency (CIA) hacks into smart phones, communication applications and other electronic devices (MacAskill, Thielman, & Oltermann, 2017). In the light of U.S. intelligence agencies' spy capabilities, Chinese cyber-enabled espionage activities do not seem as unique or threatening as suggested by U.S. government officials and media. This research seeks to ask the following question:

How severe is the threat that Chinese cyber-attacks pose to U.S. national security and how does the actual threat compare to the threat level intimated in U.S. government discourse?

This research question paves the way for the following sub-questions:

- What are the characteristics of Chinese cyber-attacks on the U.S.?
- How do Chinese cyber-attacks impact U.S. national security?
- How effective have U.S. efforts to mitigate the threat posed by Chinese cyber-attacks been?
- How do the U.S. media and government officials portray Chinese cyber-attacks and why do they do so?

This paper primarily aims to investigate whether the cyber hype surrounding Chinese cyber-attacks corroborates with reality, i.e. empirical data on cyber-attacks. To do so, it seeks to achieve the following objectives: (1) To understand the characteristics and impact of Chinese cyber-attacks on the U.S.; (2) To elucidate the effectiveness of U.S. efforts to mitigate Chinese cyber-attacks; (3) To examine how U.S. government officials portray Chinese cyber-attacks (4) To identify any social, political or economic reasons behind U.S. hype around Chinese cyber-attacks.

1.3 Definitions of Cyber related Terminologies

This research situates itself in the broader field of cybersecurity. The prefix 'cyber' means any "computer or digital interactions" (Valeriano & Maness, 2015). The complex corpus of cyber terminology warrants brief definitions of the following terms: cybersecurity, cyber-attack, cyber conflict, cyber war and cyberspace before a deeper discussion.

This paper defines national cybersecurity as a "state's ability to protect itself and its institutions against threats, espionage, sabotage, crime and fraud, identity theft, and other destructive e-interactions and e-transactions" (Choucri, 2012). Baldwin's (1997) concept of security is useful to understanding cybersecurity through the lens of "security for whom?", "security for which values?", "from what threats", "how much security?", "by what means?", "at what cost?" and "in what time period?". Since this study will provide a threat analysis, it answers the first three questions of security. The 2017 U.S. National Security Strategy addresses the first two questions. The document states that national security is constructed on four pillars of national interests: to protect the American people, territory and way of life, enhance U.S. economic prosperity, ensure a strong military to deter and win adversaries and advance U.S. global influence for assured security and prosperity (The White House, 2017). In other words, cybersecurity encompasses military, economic, social and political contexts in which the referent objects (Buzan et al., 1998, p. 36) of security refers to the

U.S. as a sovereign state, U.S. organisations including government departments and corporations and U.S. citizens.

The third question points to the threats from Chinese cyber-attacks. Due to the geopolitical nature of the research question, this paper defines cyber-attack as "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information" (Blank, 2013, pp. B6) (See Appendix 1 for an alternate technical definition).

The paper follows U.S. Joint Chiefs of Staff's (JCS) definition of cyberspace as "a global domain within the information environment consisting of the interdependent networks of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (JCS, 2018). Cyberspace consists of three interconnected layers – physical layer, logical network and cyber persona. The physical layer comprises physical hardware and infrastructure such as computing, storage and network equipment. The logical network consists of the programming code that enables the network components to interact by processing and transferring data. The cyber persona layer refers to data that describes the identity of a network or human entity such as IP addresses and email addresses (JCS, 2018).

This paper classifies cyber-attacks into three categories according to their effects – disruption, espionage and degradation (Valeriano, Jensen, & Maness, 2018). Cyber disruptions are low-cost and short-lived attacks such as Distributed Denial of Service (DDoS) attacks and defacement of government websites. These attacks are useful for signalling adversaries and preventing the escalation of a conflict. Cyberespionage operations are also low-cost operations which covertly collect short-term tactical information or long-term strategic information about the adversary's capabilities, intentions or trade secrets for

economic benefits. Cyber degradations are costly attacks that aim to degrade or destroy the target's cyberspace networks to create destabilising effects. By imposing high costs, degradation attacks change the target's cost-benefit calculations.

Cyber disruptions, cyberespionage and cyber degradation are typical cyberwarfare that states conduct in a cyber conflict**.** Building on Valeriano and Maness' (2015) work, this study defines cyber conflict as a foreign policy tool, in which states are guided by malicious intent to use computational technology to shape economic, diplomatic, military and social interactions to their advantage. In contrast, cyber war is an exacerbation of cyber conflict that involves death and physical destruction.

This paper focuses on cyberwarfare, which comprises offensive and defensive cyberspace operations, or simply, cyber-attacks. Offensive cyberspace operations "intend to project power in and through cyberspace" (JCS, 2018) while defensive cyber operations counter threat actors bearing malicious capability and intent via internal defensive measures and response actions. The former involves hunting threats on internal networks to eliminate or mitigate the effects, while the latter focuses on actions in foreign cyberspace to counter the initiator (JCS, 2018). Since response actions also involve operations that physically disrupt or destroy adversaries' systems, the line between offensive and defensive cyberspace is vague.

Unlike China, the U.S. distinguishes information operations from cyberspace operations. Information operations achieve the strategic objective of information warfare, i.e. to leverage information for competitive advantage and thus garner power (JCS, 2014). The U.S. Cyber Command conducts cyberspace operations while the U.S. Joint Information Operations Warfare Centre conducts information operations (Theohary, 2018). China does not have a published doctrine on information warfare (Iasiello, 2016, pp. 65). The recently established Chinese Strategic Support Force (SSF) oversees space, cyberspace

and electromagnetic operations and governs all aspects of information operations that includes cyber, kinetic, electromagnetic and psychological tools (Costello & McReynolds, 2018). While information and cyberspace operations are conducted by the U.S. military, China uses a whole-of-society approach for these operations.

1.4 Research Outline and Arguments

The rest of the paper is structured as follows: Section Two introduces the theoretical framework and reviews core themes in the literature. Section Three describes the methodology of collecting and analysing cyber-attack data and reports cyber reality findings. Section Four describes the methodology of collecting and analysing U.S. government officials' statements and presents the findings of cyber hype. Section Five synthesises findings from Section Three and Four. Section Six concludes the paper, explains the limitations and recommends future research areas.

This paper argues that Chinese cyber-attacks do not pose an existential threat to U.S. national security, contrasting U.S. government officials' claims which tend to exaggerate and depict Chinese cyber-attacks as an existential threat.

Specifically, Section Three shows that China primarily launches long-term cyberespionage in the absence of destructive operations, exerting economic, diplomatic and social impacts on the U.S. In response, the U.S. degrades Chinese cyber operations and conducts long-term espionage operations against China.

Section Four illustrates that U.S. government officials chose to exaggerate the mortality of counterintelligence impacts and depict China as an unprecedented threat that unfairly benefits its local industries by stealing commercial data from the U.S. and other countries. However, no publicly available evidence is present

to support such claims. Section Four also notes that the U.S. attributes blame more directly for industrial espionage compared to political espionage.

Lastly, Section Five summarises the threats from cyber-enabled political espionage, industrial espionage and destructive attacks and explains any insincerities or exaggerations in U.S. government's discourse. Specifically, Section Five argues that cyber-enabled political espionage inflicts intelligence and counterintelligence consequences. However, unlike what U.S. government officials have portrayed, such threats are not existential to U.S. national security since U.S. intelligence capabilities also mirror an equal or greater degree of threat to China. Cyber-enabled industrial espionage poses economic implications regardless of intent. However, the extent of Chinese government's direct involvement in commercial espionage against U.S. firms and the degree of benefit in which Chinese firms reap from the state intelligence activities may be exaggerated. Moreover, Chinese cyber-attacks constitute a small part of industrial espionage. The broader systemic threat lies in the legal vectors of investment agreements, cybersecurity and investment laws and other covert forms of human espionage.

Overall, U.S. government claims are insincere given that U.S. intelligence agencies conduct similar cyberespionage activities, the U.S. refuses or fails to provide the public with incriminating evidence, and the U.S. muddles national security concerns of cyber-enabled political espionage with trade goals.

II. Literature Review

This section introduces the theoretical framework of threat analysis and threat perception. The second part outlines the debate about the likelihood and severity of cyber war based on traditional benchmarks of violence and international law of armed conflict (LOAC). The third part focuses on cyber conflicts by examining various international relations (IR) perspectives of the cyber threat and analysing how the unique features of cyberspace transform contemporary understanding of conflicts and traditional concepts of deterrence and power. Finally, the literature review presents contrasting interpretations of China's rise and the U.S.-China rivalry in cyberspace.

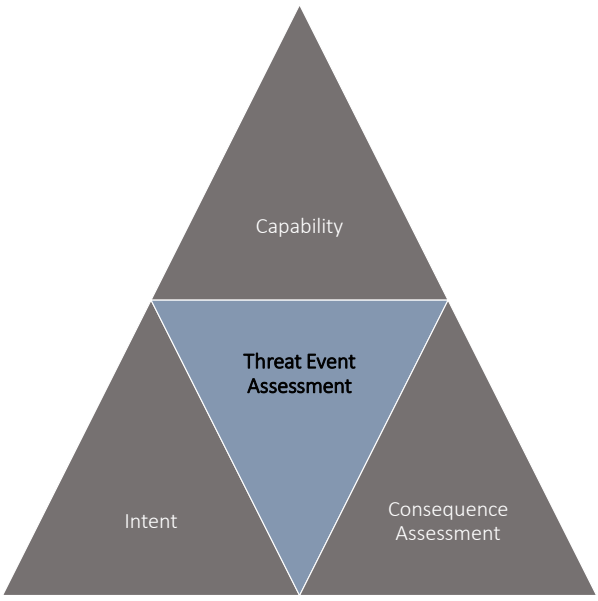
2.1 Theoretical Framework

Attendant with the increasing awareness of the cyber threat, governments, private firms, scholars and computer security firms have developed various cyber threat analysis frameworks. Most threat analysis frameworks focus on the technical process of cyber-attack life cycle (Lockheed Martin, 2019; Office of the Director of National Intelligence (ODNI), 2019) or the various parties involved in the cyber-attack (Pendergast, 2014; The MITRE Corporation, 2019). While these threat intelligence frameworks address the needs of corporations defending against cyber-attacks, they often lack analytical rigor from political and social perspectives. Hence, this paper draws on Steinberg's (2009) approach to assess the threat of Chinese cyber-attacks to U.S. national security. Steinberg outlines five functions of threat assessment: Threat Event Prediction, Indications and Warning, Threat Entity Detection and Characterisation, Threat Event Assessment and Consequence Assessment. Unlike others, his approach encapsulates the political and social contexts via analysis of the cyber incident and the ensuing consequences.

This paper does not predict future attacks but seeks to understand the specific threat posed by Chinese cyber-attacks. The paper focuses on Threat Event Assessment and Consequence Assessment using empirical data of cyber-attacks

between the U.S. and China. Threat is a function of capability, opportunity and intent (Little & Rogova, 2008). Capability refers to the attacker's ability to "design, develop and deploy" a weapon. Intent is inferred from the type of attack and the effects it generates. Opportunity relates to the attacker's assessment of the target's vulnerability and ease of access, and the perceived net pay-off of the attack (Steinberg, 2009). Though the vulnerability of U.S. entities increase the opportunities of cyber-attacks, this study focuses on 'capability' and 'intent' of China. It analyses U.S.-China cyber-attacks according to the capability and intent of the Chinese threat actors and assesses their effects to determine the severity of Chinese cyber-attacks to U.S. national security (see Figure 1 for an overview of the framework for threat assessment).

Figure 1: Threat Framework

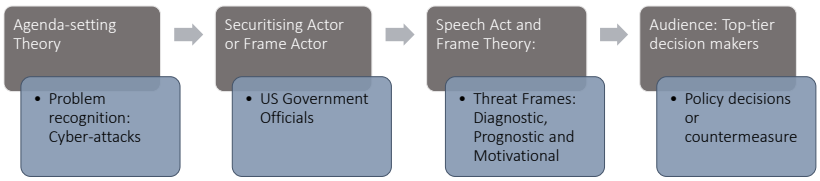


The examination of hype in this study is grounded in Dunn Cavelty's (2008a) threat politics framework, which integrates the securitisation theory, agenda-setting theory and framing theory. Copenhagen school's securitisation theory

focuses on the outcome, in which the audience accepts the "speech act" and "extraordinary measures" are implemented as a result (Buzan et al., 1998). Dunn Cavelty's (2008a) framework is apt for this study because it clarifies the process of securitisation by incorporating concepts from the agenda-setting theory and framing theory.

Agenda-setting theory augments the securitisation theory by explaining the process and conditions that result in particular issues gain political salience (Kingdon, 2003). According to Kingdon (2003), problems, policies and politics are three factors that influence the political salience of an issue. They intermingle with political context such as parliamentary majorities and pressure group campaigns to gain priority on key policymakers' agendas. In this study, problems are represented as cyber incidents initiated by the Chinese against the U.S. Selected cyber incidents function as starting points from which this study examines cyber hype. Framing theory describes how certain aspects of an issue are subtly emphasised to engineer a certain type of response (Snow & Benford, 1992). As frames define meaning through linguistics (Oliver & Johnston, 2000), government officials and experts often use frames to exaggerate the actual threat by leveraging specific phrases, words or stories (Dunn Cavelty, 2008a). Snow and Benford (1992) posit that a speech act in securitisation theory comprises three types of framing – diagnostic, prognostic and motivational. Diagnostic framing defines the problem and assigns blame; prognostic framing offers solutions while motivational framing calls for action to combat the problem. Frames are important because they impose practical consequences that direct the course of action.

Integrating elements from the three theories, Dunn Cavelty's (2008a) framework can be summarised into four key elements shown in Figure 2:



2.2 The Perceived Likelihood and Severity of Cyber War

U.S. scholars dominate most academic literature on the threat of cyber war. They view the U.S. as being extremely vulnerable to cyber-attacks due to its greater dependence on military and societal networks and thus deem cyber war as a real and existent threat. Clarke & Knake (2012), Caplan (2013) and Dudney (2011) hypothesised worst-case scenarios, in which a single strike on a networked infrastructure would result in a domino effect on other critical infrastructure such as energy grid and communications network. To support the existence of cyber war , these authors cite cyber-attacks in dyadic conflicts, such as the cyber-attacks between India and Pakistan during the Kashmir conflict in 1999, the DDoS attacks on Georgia by Russia in 2008 and Israel's successful attack against an Iranian nuclear facility in 2007. However, these claims are not substantiated with reference to legal standards that give credence to the 'cyber war' label and are vigorously challenged by others.

Rid's (2012) seminal work "Cyber War Will Not Take Place" notes that past cyber-attacks have neither resulted in human casualties nor widespread physical destruction, thus failing to meet the definition of war as conceptualised by Carl von Clausewitz (1940) – violence, instrumentality and political nature. His rebuttal sparked further debates about the likelihood and severity of cyber war. Arquilla (2012) insisted the non-violent cyber-attacks of "sabotage, espionage and subversion" which are described by Rid (2012) still constitute cyber war,

albeit in covert forms. However, he conceded that his primary concern still lies in the potential evolvement of past cyber-attacks into larger and more severe attacks, thus indirectly corroborating Rid's (2012) argument that wars should be non-routine and exclusive in its violent character. Stone (2013) provided a stronger critique of Rid's (2012) argument by disputing lethality as an inevitable outcome of violence. He argued that even though all wars involve the use of force, it is not necessarily lethal. For instance, a cyber-attack causing widespread damage to physical infrastructure in the absence of human casualties would still be considered an act of war.

Scholars also debate the likelihood and severity of cyber war using international law. Article 2(4) states that "All Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations.". Article 51 stipulates that "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." (United Nations, 1945). The "use of force" in Article 2(4) distinguishes from an "armed attack" because the latter triggers the right of self-defence, fulfilling the standards of war by retaliation through conventional military means, while the "use of force" only justifies retaliatory measures short of war such as economic sanctions. However, the threshold of an armed attack is ambiguous under the UN Charter, forming a source of contention among scholars.

The 'effect and scale' criterion is a common benchmark that scholars use to judge whether a cyber-attack constitutes an armed attack. Similar to Clausewitz's (1940) definition, they argue that a cyber-attack must result in significant physical damage or deaths that are analogous to the effects of a conventional armed attack to warrant a kinetic retaliation (Hathaway & Crootof,

2012; Lin, 2010; Roscini, 2010). This perspective was first formalised in the authoritative but non-binding Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn 1.0), which states that any use of force that "injures or kills persons or damages or destroys property" would unequivocally be considered an armed attack (Schmitt, 2013). However, the International Group of Experts (IGE) who created the manual were split regarding whether attacks resulting in severe consequences other than death or damage to infrastructure constitute an armed attack. One example is a cyber-attack on New York Stock Exchange, in which some experts contended that the resulting devastating economic impact constitutes a threat to national security, while others in the IGE disagreed. The U.S. government concurred with the former's broader view and posited that there should be no standard threshold for retaliatory self-defence but the context of the attack and intent of the attacker should be points of consideration (Koh, 2012).

2.3 Cyber Conflict – International Relations Perspectives and Impact on Traditional Concepts of Deterrence and Power

The cyber war debate gradually shifted away from contending the probability of its occurrence to analysing the implications of vast majority of cyber-attacks below the conventional legal threshold for war. In tandem with the linguistic shift from "war" to "conflict", scholarly attention on cyber conflict became more prominent. Moderate scholars like Richards (2014) contend that past cyber-attacks do not fit the binary thesis and anti-thesis of war. Demchak (2012) proposed the term "cybered conflict" to underscore the critical role that information and technology plays in state conflicts, characterising such conflicts as unofficial, persistent and imposing a spectrum of effects. Notions of cyberspace as a "substrate" of in hybrid and asymmetric conflicts replace the pre-dominant concept of cyberspace as a warfighting domain (Dombrowski & Demchak, 2014). Similarly, Blank (2017) highlights how cyber conflict should be viewed in conjunction with information operations and political warfare. The

scholarly attention on "cyber conflict" or "cybered conflict" is useful for overcoming the conceptual limitations of a traditional armed conflict by drawing more attention to the insidious effects of cyber-attacks on the political and social levels.

Other scholars employed IR theories to explain cyber threats. Deibert (2003) was one of the first scholars who noted the stealthy development of offensive cyber warfare capabilities by international actors such as China, Russia, U.S., United Kingdom, and Australia. Choucri (2012) portrays such development of cyber capabilities as part of a state's "natural" extension of defence policies into the cyber domain. While both scholars present the realist perspective of a zero-sum arms race in cyberspace, Manjikian (2010) compares liberal and realist interpretations. Unlike liberals, realists view cyberspace a strategic extension of the physical space that in need of defence (Manjikian, 2010). Eriksson and Giacomello (2006) aver that interdependence and perception of symbols and language in liberal and constructivist theories respectively, construct a better understanding of the cyber threat compared to the realist theory.

Scholars also applied securitisation theory to cybersecurity. Securitisation theory posits that a securitising actor highlights an existential threat to an audience through the illocutionary "speech act" (i.e. the securitising act of uttering the word "security" or another term to express the urgency of the matter) to implement exceptional measures in response to the threat (Buzan et al., 1998). Dunn Cavelty (2008b) builds on previous work done (Bendrath, Eriksson, & Giacomello, 2007; Eriksson, 2001) on frame theory and securitisation theory to analyse how the three types of framing in defining the problem (diagnostic), proposing solutions (prognostic) and calling for action (motivational) contribute to the securitisation of the cyber-terror issue. Hansen and Nissenbaum (2009) propose cybersecurity to be a new sector of security due to its distinct set of threats and referent objects. Similarly, Lawson (2013) refines the framing and securitisation theories by providing a constructivist analysis of how

motivational frames stimulate social action and suggests ways to "desecuritise" the issue by altering the frames.

In line with the realist perspective, Buchanan (2017) examines the security dilemma in cyberspace. He agrees with Kello (2017) that states are more prone to escalatory and destabilising measures in cyberspace because certain unique features of the domain favour the offensive rather than the defensive. The features include ambiguity between offence and defence, the dearth of credible information which enables covert stockpiling of weapons and the lack of international norms to govern cyberspace. Other moderate scholars analyse how the unique features of cyber threats impact deterrence in cyberspace. Libicki (2009) states that deterrence is difficult to apply in cyberspace due to the offensive advantage in cyberspace, uncertainty, anonymity and the problem of attribution – which are discussed below respectively.

First, a surprise attack in an operational cyber war can momentarily throw the adversary off-guard, allowing the attacker to gain a temporary military edge (Libicki, 2009, p.139). Cyber offense is also relatively cheaper and easier to deploy than cyber defence. The compressed time horizon of cyber-attacks decreases the likelihood of detecting and countering an impending attack (Liff, 2012). However, many scholars note that cyber-attacks can only achieve tactical but not strategic outcomes since their impacts are short-term and reversible (Gartzke, 2013; Libicki, 2009; Liff, 2012; Saltzman, 2013). Demchak (2012) and Blank (2017) echo the view that cyber-attacks can only impose a lasting and substantial impact when combined with conventional warfare.

Second, uncertainty in cyberspace arises from the paucity of information about states' cyber capabilities, vulnerabilities and intentions. States are unable to use cyber-attacks to signal their intentions without risking conflict and escalation due to uncertainty of the adversary's response (Libicki, 2009; Kello, 2017). However, Liff (2012) argues that the uncertainty can impose deterrence effect

when states hesitate to launch cyber-attacks for fear of accidentally inflicting self-harm.

Third, anonymity in cyberspace and the accompanying attribution problem weaken deterrence among states. From the defender's perspective, retaliation requires proper attribution but the lack of transparency in capabilities creates challenges in doing so. Anonymity also reduces the utility of the attack since knowledge of the perpetrator is required to coerce and elicit concessions from the target (Liff, 2012). However, anonymity is a powerful tool for the attacker because stealth is required for operational effectiveness of a cyber-attack (Gartzke, 2013). Apart from anonymity of the attacker's identity, Brantly (2016) posits other aspects of anonymity, involving the inability to detect an ongoing attack and the inability deduce the objective of the attack.

Responding to the conceptual limitations of deterrence in cyberspace, Valeriano and Maness (2015) introduced the idea of 'restraint' i.e. states abstain from total offensive operations, i.e. "direct and malicious" attacks that destroy critical infrastructure (Valeriano & Maness, 2015, p. 62). Although Lin (2012) and Austin (2015) analysed the concept of restraint, Valeriano and Maness (2015) confirmed the theory with empirical evidence of cyber-attacks between dyadic rival states. Their findings demonstrate that most cyber-attacks between states are based on territorial considerations rather than random and power projection motivation. Most cyber interactions yield no impact on overall state relations apart from negative foreign policy responses (Valeriano & Maness, 2015, p. 127). States also practise restraint for fear of collateral damage and retaliation by conventional methods (Valeriano & Maness, 2015, p. 63).

Another aspect of IR studies relates to the concept of power. Like in traditional domains, cyber power is integral to understanding how states interact and shape conflicts. According to Kuehl (2009), cyber power is defined as "the ability to use cyberspace to create advantages and influence events in other operational environment and across the instruments of power". Betz and Stevens (2011)

also discuss other dimensions of power: structural, institutional, and productive power. Structural power describes how the nature of cyberspace constrains, maintains or alters the actions of all actors within while institutional and productive power stem from the actions of the states. Productive power refers to the ability of the state to designate certain actors as legitimate threats to national security and implement policies against them. States demonstrate institutional power when they engage formal and informal institutions to construct international norms. A prime example is the U.S., who led the effort in developing the Tallinn Manual for applying current laws of armed conflict to cyberspace. China also exercises institutional power through organisations like the International Telecommunication Union and the Shanghai Cooperation Organisation (Betz & Stevens, 2011).

Okomentoval(a): [KLT(1]: How U.S. set the rules of what is considered commercial espionge. Diffeence between U.S.' institutional power/productive power and China's non-state power

States possess little structural power over the unique features of cyberspace Being low cost, anonymous and asymmetric, cyberspace allows an unprecedented ease of operations by small states and non-state adversaries (Nye, 2011). Betz (2012) notes cyber power also decreases non-state actors' power differential with state actors. Similarly, Kello (2017) posits that non-state actors challenge the existing international order as threat actors, as providers of national security and as interferers of state conflict to accelerate existing crises. Indeed, there has been a power shift to non-state actors of varying capabilities and motivations, including lone opportunists, organised crime groups, hacktivists, terrorists and cyber militias (Ranger, 2018) (see Table 1 for list of non-state actors and intentions).

According to Klimburg (2011), another aspect of cyber power lies in states' ability to command the cooperation of non-state actors. In China, cyber militias are crucial to the government's effort in information warfare such as conducting cyberespionage on military plans and industrial secrets (Maurer, 2018, p. 181). The Chinese government exercises great cyber power with over eight million cyber militias, comprising military, commercial and academic professionals who conduct plausibly deniable cyber-attacks (Williams, 2018).

Table 1: Non-State Actors – Capabilities, Targets and Motives

Non-state actors	Motives
Lone wolf criminals	- Armed with basic technical skills - Target individuals to commit petty crimes e.g. cryptocurrency mining - Motivated by financial gains
Organised crime groups	- Sophisticated actors with the ability to develop hacking tools and vulnerabilities - Target big corporations via cyber extortion e.g. credential fraud, ransomware - Motivated by financial gains
Hacktivists	- Operate as individuals with no technical expertise or loose organisations engaging in cyber espionage - Target government institutions or corporations to release embarrassing information - Motivated by political agendas
Terrorist groups	- Known cybercrimes committed by terrorists are currently rare - Usually involves unsophisticated disruptive attacks e.g. DDoS and website defacements - Motivated by political or financial gains

Despite the ascent of non-state actors into the international political arena, states still remain the most powerful actor in international politics (Nye, 2010). States are more likely than cyber criminals or terrorist to conduct massive destructive attacks (Lewis, 2018). Moreover, instead of upsetting the current balance of power, Betz (2012) argues that cyber power reinforces the extant distribution of military power.

The literature review on the perceived threat of cyber war illustrates that scholarly consensus on the impact and scale of cyber threats is non-existent. However, a distinct shift from cyber war toward examining the impact and nature of cyber conflict can be observed. Traditional LOAC is adapted to apply to cyber-attacks. The follow-up publication of Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations in 2017 reflects such efforts. The IGE agrees that states bear international legal responsibility for an attributed cyber-attack, regardless of geography and consequence of physical damage or injury. However, the IGE stipulated a high threshold for attribution, stating that evidence such as the origin of malware and place of receipt of hacked information, is insufficient evidence for attribution (Jensen, 2017).

At the same time, the proliferation of IoT raises awareness of the vulnerability of critical infrastructure. The present concern revolves around "multi-vector" and "multi-wave" destructive cyber-attacks on all civil and military infrastructure of the adversary i.e. "cyber blitzkrieg" (Austin, 2019). Awareness of state vulnerability is reflected in many national security strategies, where critical information and infrastructure protection has been accorded high priority (Austin, 2019, p. 10).

2.4 Rise of China and U.S.-China Rivalry in Cyberspace

Having examined the main debates regarding cyber war and cyber conflict, this section analyses contemporary geopolitical issues between China and the U.S. After outlining issues regarding U.S.-China relations amidst China's ascent to the world's second largest economy, this section explores U.S.-China. relations specifically in cyberspace.

Contrasting interpretations of China's meteoric growth have dominated the academic community. Several scholars including Mearsheimer (2001), Kirshner (2012) and Goldstein (2013) support realist perspectives that the state of world anarchy and the attendant security dilemma will trigger a power struggle and increase the likelihood of conflict or opportunistic aggression between the two global powers. Similarly, Allison (2017) warns about the "Thucydides Trap", describing the inevitability of a conflict when a rising power threatens to displace the incumbent power.

Besides structural reasons, the expanded interests of the growing power and differences in strategic cultures increase the likelihood of conflict. China's recent re-assertiveness in the disputed waters of the South China Sea demonstrates its desire to expand its sphere of influence to better secure its long-term security (Le, 2018). It also seeks to reshape global alliances and the global economy by playing a larger role in global institutions (Maher, 2018). In addition, both countries bear a low tolerance for vulnerability. China seeks to restore its country's pride from a century of humiliation through reclamation of

territory while the U.S. possesses a self-imbued responsibility of providing for global security (Steinberg & O'Hanlon, 2014). Chinese authoritarian values and U.S. liberal democratic value also compounds suspicion and distrust, escalating the chances of conflicts. China often views U.S. opposition to its foreign policies in Asia as a form of containment (Friedberg, 2005).

Okomentoval(a): [KLT(2]: To be linked to contaiment of China using ban of Huawei

Liberal scholars believe that economic interdependence and participation in global institutions mitigate the chances for aggressive confrontation between the global powers (Ikenberry, 2013; Twomey, 2013). Similarly, the constructivist perspective posits that China's involvement in global institutions may lead to a fundamental change in mindsets and beliefs to become more open toward Western liberal norms. Economic development is also believed to be a driver for democracy through increasing people's desire for political freedom and the institutionalisation of democratic processes such as courts and rule of law (Friedberg, 2005). While such optimistic views are theoretically sound, they take years to materialise and are gradual in effect.

A more balanced view lies between the extreme ends of inevitable conflict and peaceful cooperation. Sutter (2010) observes that China still lags the U.S. in the military domain so any power transition will be gradual. Friedberg (2005) and Maher (2018) consider China and the U.S. constitute a bipolar international order despite China's lack of military power. The opposing forces of cooperation and conflict i.e. "competitive co-existence", breed stability in a bipolar system (Shambaugh, 2013). Moreover, China struggles to redefine the international order because Western values are deeply entrenched in the rule-based global system (Ikenberry, 2008).

However, some authors note that disparity in U.S.-China military power does not immunise the U.S. from a military confrontation with China if red button issues like the independence of Taiwan threatens its foreign and domestic position and worsens from inaction (Chan, 2018; Goldstein, 2013). Ultimately, a peaceful transition of power is contingent on a shared positive perception of

the U.S.-China relations. A strongly skewed threat perception will lead to unnecessary escalation even in the absence of a power transition (Zhu, 2006).

Realists in the U.S. often justify their animosity toward China by referring to *Unrestricted Warfare*, a 1999 publication by two senior People's Liberation Army (PLA) colonels, which describe how China can leverage cyber-attacks to target the most digitally connected states on both civilian and militant fronts (Liang & Wang, 1999). Despite being a relatively weaker military power, China can gain asymmetric advantage by launching pre-emptive attacks on U.S. information systems to cripple its strategic decision-making apparatus. China's latest Military White Paper names cyberspace and outer space as "new commanding heights in strategic competition" and in winning "informatised local wars" (The Information Office of the State Council, 2015). In December 2015, China restructured its cyber force from an independent branch to become subsumed under the SSF as part of integrated multi-domain operations.

China's cybersecurity objectives seek to attain military knowledge via military-technological espionage, to gain economic advantage via industrial espionage and to deter adversaries by infiltrating critical infrastructure (Hjortdal, 2011). The first two goals are linked to China's "Made in China 2025" (MIC2025) plan, an ambitious vision by Chinese President Xi Jinping to transform its economy from a low-end manufacturer to a leader in high-technology products in ten years (Cyrill, 2018). Ensuring prosperity through continued technological progress is crucial for China's internal stability. However, experts deem MIC to be impossible without stealing IP (Bluestone, 2018). Indeed, China's history of espionage activities is copious. A few noteworthy cases include Titan Rain in 2003, in which multiple U.S. government and contractor networks were intruded, Operation Aurora was a series of intrusions into various American corporations via retrieving a source code from Google's networks in 2010, Shady Rat consisted of a global intrusion into multiple governments, corporations and international bodies over a five-year period (Inkster, 2015). More recently, China targeted sectors central to its MIC2025 strategy, which

includes cloud computing, artificial intelligence, biotechnology, among others (Crowdstrike, 2019). It also targeted U.S. academic institutions to obtain the latest commercial and military technologies and U.S. research organisations to garner information about policy engagement process (Harrell, 2018). Cybersecurity scholars have also expressed concerns that China's frequent intrusions into U.S. critical and supply chains would lead to future disruptive or destructive attacks (Fazzini, 2019; Lieberthal & Singer, 2012; Lindsay, 2015).

While such concerns are perturbing, they do not warrant hyperbolic predictions of an impending China-U.S. war or a destabilising power struggle (Barrett, 2005; Thomas, 2012). Valeriano et al. (2018) observe from empirical data that that U.S.-China interactions in cyberspace depict a predictable and stable relationship. China typically launches cyberespionage operations to gain valuable information, triggering a complex degradation but targeted attack from the U.S. Both states usually cease cyber operations before commencing on another cycle of espionage and counterattack.

China's core priority is to alter the long-term balance of power through engaging in economic and military espionage rather than launching short-term disruptive attacks on the stronger adversary (Carlin & Graff, 2019; Laskai & Segal, 2018; Lindsay, Cheung, & Reveron, 2015; Valeriano et al., 2018). Though its espionage efforts are persistent and aggressive, they reflect predictable actions which are not wholly driven by the desire to maintain control in Asia and achieve a balance of power with the U.S, but are strongly motivated by domestic concerns of regime stability and population control to sustain its economic prosperity via technological progress (Valeriano et al., 2018). Furthermore, cyberespionage serves an ambiguous signalling function for China to demonstrate resolve or dissatisfaction and deter adversaries from taking escalatory measure (Chang, 2014; Valeriano et al., 2018). Bluestone (2018) corroborates the finding that cyber-attacks are used for signalling political intent with evidence that Chinese cyber-attacks from 2011 to 2015 correlate with trade tensions with the U.S. during the same period.

Other scholars debated the viability of technology transfer via cyberespionage. Lindsay (2015) highlights the complexity of technology transfer, which involves multiple steps of "introduce, digest, assimilate and re-innovate". Assimilation and re-innovation of stolen technology is especially challenging for China given its complex web of stove-piped bureaucracy and lack of capacity in high-end manufacturing. Lindsay (2015) buttresses his argument with an example of Russian fighter jet engines, a technology which China still cannot produce despite assistance and access to technical information.

Yet, structural and organisational limitations are not permanent and can be overcome. As Brenner and Lindsay (2015) contended, China has been successful in the stealing solar-power technology and entering the Western market. Interestingly, Lindsay's (2015) also noted U.S.' culpability in exploiting Chinese networks and China's weak cyber defences. U.S.' extensive surveillance and espionage efforts were revealed after classified intelligence was leaked by former U.S. government contractor Edward Snowden in mid-2013. Although the U.S. asserted that its espionage was for legitimate national security purposes, as opposed to industrial espionage for economic advantages, such a distinction is ambiguous and difficult to ascertain (Lindsay, 2015).

Austin (2019) also notes that China's cyber defences are weak relative to the U.S. due to vulnerabilities in technologies and a delayed start in implementing policy solutions. A recent report revealed that China's attack breakout time, i.e. the period of time from initial compromise of a system to the point when lateral movement within the enterprise becomes possible, is unexpectedly slow at four hours and 26 seconds, behind North Korea and Russia (Crowdstrike, 2019). China's shortcomings in defence and attack thus allow leeway for the U.S. to both exploit its networks and defend against its intrusions.

In sum, as long as the perceived benefits of economic or industrial espionage remains high compared to the potential costs of political retaliation or trade sanctions, and that a military retaliation remains unlikely, China is likely to

continue to rely on plausible deniability to exploit the grey area of conflict for economic, political and military advantage (Hjortdal, 2011).

This study contributes to the extant literature in three ways. First, it updates Valeriano et al.'s (2018) analysis of actual U.S.-China cyber interaction by collecting data from 2015 to 2018. Although non-state actors are a crucial component of cyber conflicts and they constitute interesting topics worth exploring, this paper adopts a nuanced approach to analyse cyber conflict between the most powerful and sophisticated threat actors in cyberspace. Considering the role played by state-backed hackers such as cyber militias and political hackers (Applegate, 2011), attacks by these parties are included to the extent that there is evidence suggesting they are proxies of the state or their actions are sanctioned by the state. Second, the study uses Valeriano, Maness, and Jensen's (2017) codebook as a basis for empirical analysis of cyber-attack data between the U.S. and China. However, Valeriano et al. (2018) did not investigate the extent of hype and political motivations behind the U.S. portrayal of Chinese cyber-attacks, and most literature on securitisation and threat framing on hype, do not go beyond theoretical analyses. My research resolves this gap by augmenting the analysis of empirical data with critical discourse analysis of the hype manifest in U.S. media reports and government statements. Third, this study contributes to the debate regarding the political and economic future of China as a rising power by analysing China's intentions behind its cyber-attacks on the U.S.

The following sections will a) examine cyber reality by analysing the nature and impact of cyber-attacks between the U.S. and China, b) examine whether cyber hype is present by comparing government statements selected cyber incidents with the known facts, c) synthesise the cyber hype and cyber reality findings from the latter two sections, and d) conclude and suggest paths for further research.

Okomentoval(a): [KLT(3]: Insert citation from Nye (2011) about classification of government, organisation, and individuals?

III. Cyber Reality

This section finds that Chinese cyber-attacks on the U.S. consist of short-term and long-term espionage incidents that impose economic, social and diplomatic impacts, while U.S. cyber-attacks on China involve degrading Chinese cyber operations coupled with long-term espionage. This section will explain the methodology of collecting and analysing cyber-attacks, followed by a detailed analysis of the findings on Chinese cyber-attacks and U.S. cyber-attacks.

3.1 Research Methodology

Cybersecurity literature mostly examines how cyber conflicts shape conventional warfare and impact international security. Existing studies develop qualitative analysis based on IR theories, securitisation theory and the legality of cyber operations (Deibert, 2003; Dunn Cavelty, 2008a; Koh, 2012; Kuehl, 2009). Other literature perform historical analysis of the evolution of cyber conflicts and the key developments and trends in cyberspace (Healey, 2013; Segal, 2017; Tikk-Ringas, 2015). Herzog (2011) and Langner (2011) examined individual case studies while Goldman and Arquilla (2014) use cross-domain analogies to assess the nature of cyber-attacks. While these studies add value to the understanding of cybersecurity, most of them constitute unstructured methods that may lack analytical rigour compared to structured or quantitative methods. Axelrod and Iliev (2014) apply a mathematical model to analyse the optimal timing for using cyber resources. Other structured analyses use empirical datasets to analyse political cyber-attacks from 2000 to 2014 (Valeriano et al., 2018; Valeriano & Maness, 2015).

My research adopts a case study design to analyse the severity of Chinese cyber-attacks on U.S. national security. According to Yin (2003), a case study design best serves the research when the question answered is of ‘how’ and ‘why’, when the phenomenon is contemporary and when the research concerns behavioural events that are uncontrollable. The case study design is appropriate

for the purpose of this research to explore cyber-attacks by state actors, specifically U.S. and China, which constitute novel threats in the international arena. This study uses a descriptive case study methodology to explicate and compare the threat that Chinese cyber-attacks pose to the U.S. with the actual threat level intimated in the U.S. government discourse. The paper seeks to present an objective picture of cyber-attacks between the U.S. and China by testing theoretical constructs surrounding cyber war, cyber conflict and U.S.-China relationship in cyberspace explicated in the literature.

The use of China and the U.S. as a case study for the tension between cyber hype and cyber reality is meaningful on several fronts. First, cyber hype has mostly been generated by U.S. academics and pundits. From technological optimism to cyber doom, the U.S. policy and academic circles have been instrumental in shaping the cyber discourse in the West. Hence, the U.S. is a relevant case for analysing cyber hype. Second, China's unique position as the U.S.' strongest competitor and current challenger to the U.S.' hegemonic status provides a strong basis to analyse how socio-political and economic dynamic intertwine with threat representation. Third, an objective assessment of Chinese cyber-attacks on the U.S. is critical in informing policymakers on both sides to prevent miscalculation or unnecessary escalation amidst an increasingly complicated cyber landscape with the burgeoning number of networked devices – the Internet of Things (IoT) and the imminent arrival of 5G. Lastly, China and U.S.' cyber interactions warrant a detailed study because they will heavily shape global norms and international relations in cyberspace and beyond.

Although China's cyber-attacks against the U.S. have a long history, this study collects and analyses ongoing cyber-attacks between the U.S. and China from 1 January 2013 to 31 May 2019. While time constraint is a practical consideration, the chosen timeframe of data collection captures critical events. In 2013, President Xi assumed power and implemented military and domestic reforms to centralise its cyber operations. 2014 also marks a temporary decline in Chinese cyber-attacks and the first U.S.' indictments against PLA officials (Fireeye,

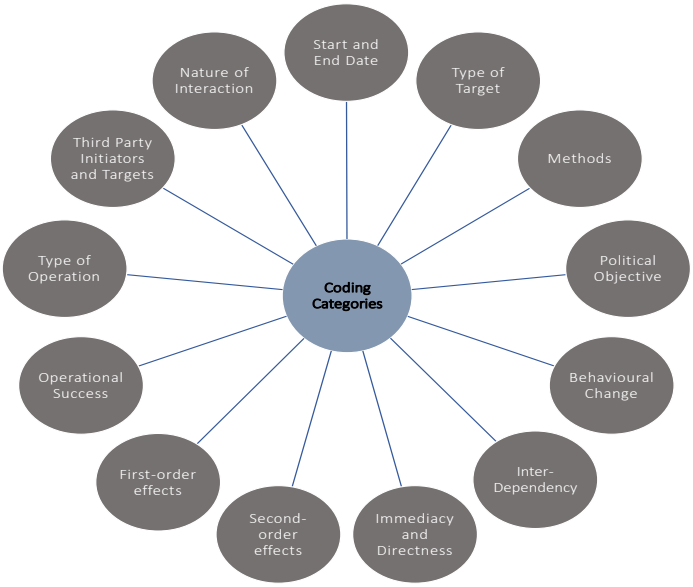
2016). By capturing the latest evolutions of cyber-attacks, this study provides a comprehensive and up-to-date picture of the threat.

This study employs framework analysis by Ritchie and Spencer (2002) to collect and analyse cyber incidents. Framework analysis involves familiarisation of data, identification of coding categories and sub-categories, coding and summarising key findings into tables to draw relevant conclusions. According to Happa and Fairclough (2017), three types of cyber-attack evaluation models exist: technology-centric, social-centric and cyber-situational awareness and understanding models. This study focuses on the third type to provide a holistic evaluation of the impacts of cyber-attacks. While cyber-situational awareness models are available (Gandhi et al., 2011; Klimburg, 2012; NIS Cooperation Group, 2018) , they are either too simplistic (NIS Cooperation Group, 2018) or overly detailed, which extends beyond the scope of this study (Gandhi et al., 2011).

Valeriano et al.'s (2017) Codebook for Dyadic Cyber Incident and Dispute Dataset (DCIDD) Version 1.1 (2017) heavily influenced this study's data collection and coding procedures (see Figure 3 for coding categories and **Chyba! Nenalezen zdroj odkazů.** for the complete coding template). This study follows a longitudinal approach by collecting observable cases of cyber incidents between China and the U.S. from 2013 to 31 May 2019. It considers "cyber incident" as a set of individual cyber-attacks belonging the same reported event, e.g. revelations from courts indictments or reports by computer security firms. Accounting for different cyber-attacks relating to the same incident according to different objectives is impractical and unwieldly since it unnecessarily expands the dataset due to repeated coding of other details. Cyber incidents involve the manipulation of computer code with malicious intent and exclude electronic warfare methods such as electromagnetic attacks. Although cyberspace includes the physical layer, this study excludes cyber-attacks that involve only insider access or physical access to computers without the manipulation of computer code. Some common types of cyber-attack

techniques include phishing, man-in-the-middle attacks (MIMA), DDoS, Structured Query Language (SQL) injection, zero-day exploits, cross-site scripting and password attacks (See **Chyba! Nenalezen zdroj odkazů.** for definitions). Nevertheless, since this study does not require a large extent of technical details, it classifies methods employed in the cyber incidents into broad methods of Vandalism, Denial of Service, Intrude and Infiltrate and Hijacking (See Appendix 3 for detailed explanation of each category).

Figure 3: Coding Categories



The incidents under study must also be state-initiated, either by China or the U.S. Non-state initiators like cyber mercenaries are included to the extent that their actions are state-sanctioned or state-sponsored. This study excludes non-state initiators, such as hacktivists, because their intentions do not overlap with the state and including cyber-incidents initiated by them will obscure the focus and undermine the feasibility of this study. State-initiated cyber incidents are verified through responsibility confirmation or political attribution as opposed

to technical attribution (Goodman, 2010; Steiger, Harnisch, Zettl, & Lohmann, 2018). Responsibility confirmation follows Valeriano et al.'s (2017) approach, whereby responsibility is assigned based on consideration of intent and history of relations together with verification from government statements of different departments and computer security firms (see Table 2 for the examples of the sources for responsibility confirmation). State and non-state targets in the private sector are scoped in if they are direct targets that qualify under critical infrastructure sectors in the U.S. Presidential Policy Directive 21 (see Appendix 1 – List of Technical Terms and Definitions

Cyber-attack Process: Comprises pre-attack, attack and post-attack phases. The pre-attack phase consists of reconnaissance and scanning activities to identify potential targets and scan for vulnerabilities in people, processes and technologies. The attack phase occurs when the identified vulnerabilities are exploited. The attacker gains access and escalates privileges for complete control to ex-filtrate data or spread malware to degrade, disrupt or destroy the system. After the attack, malware is installed to maintain future access to the system. The attacker would also obfuscate the attack to make attribution and forensic examination difficult.

Phishing: Technique used in a cyber-attack that deceives the target into installing malware or accessing malicious websites through sending fraudulent emails from a seemingly legitimate source. Targets large numbers of people simultaneously.

Spear-phishing: Technique is the same as phishing, except that spear-phishing personalises attacks to specific targets

Worms and Viruses: Malware that compromise regular functionalities by corrupting or deleting data. However, unlike worms, viruses attach themselves to programs and self-replicate.

Trojans: Malware that masquerade as legitimate programmes which contains malicious code

Ransomware: Malware that encrypts data until a ransom has been paid off

Rootkits: Malware that grants the attackers total control of the system while evading detection

Bots: Malware that assemble a large malicious network through compromising individual clients

Logic Bomb: Malware that causes a network or system to cease operations, involving elimination of all data

Keystroke Logging: Malware that tracks keys being inputted into the computer and replicate them for infiltration into the network.

Sniffers or beacons: Monitoring techniques that search for specific information and usually inflict no malicious harm.

Man-in-the-Middle Attack: Technique used in a cyber-attack that intercepts cyberspace communication to between two parties to steal or modify data.

Distributed Denial of Service: Technique used in a cyber-attack that compromises the system through loading it with excessive information such that it is unable to perform regular functions.

Structured Query Language (SQL) injection: Technique used in a cyber-attack that targets websites and the accompanying databases to reveal sensitive information including usernames, passwords, personal, and banking information.

Zero-day exploits: Technique used in a cyber-attack that leverage on discovered vulnerabilities with no developed solutions

Cross-site scripting: Technique used in a cyber-attack that attacks legitimate website or web application by running malicious scripts in order to infect targets who visit the compromised website.

Watering Hole: Technique used in a cyber-attack in which attackers target websites that are frequently visited or are trusted by the targets to increase operational success.

Password attacks: Technique used in a cyber-attack that leverages common weak passwords and previously hacked passwords to gain access to targets' systems.

Confidentiality: One of the information goals to maintain the privacy of data.

Integrity: One of the information goals to maintain the non-alteration of data without proper authorisation.

Availability: One of the information goals to maintain the ability to access the system.

Information Operations: Comprises of four tenets – a) psychological operations, b) electronic warfare, c) operations security and d) military deception. (Definition according to US DoD Joint Publication 3-13)

- *Psychological Operations* – Using planned information to influence foreign target audiences, including friendly and adversarial governments, individuals and organisations into subscribing to an agenda by manipulating their emotions, motives, objective reasoning. (Definition according to US DoD Joint Publication 3-13)
- *Electronic Warfare* – Involves attacking the electromagnetic spectrum such as jamming radio communication systems.
- *Operations Security* **–** Involves identifying and analysing critical information to ensure the functioning of military operations
- *Military Deception* **–** Related to psychological operations, but focuses on disinformation, but only applies to adversarial military, paramilitary or violent organisations.

Cyberspace Operations: Achieve objectives in or through cyberspace by executing cyberspace capabilities.

- Offensive Cyberspace Operations – Intent is to project power in and through cyberspace.
- Defensive Cyberspace Operations – Intent is to defend DoD information networks and other key cyber terrains from malicious cyberspace activity to preserve the freedom of manoeuvre in cyberspace.

US Presidential Policy Directive 21: Critical infrastructure sectors comprise of the chemical sector, commercial facilities sector, communications sector, critical manufacturing sector, dams sector, defense industrial base sector, emergency services sector, energy sector, financial services sector, food and agriculture sector, government facilities sector, healthcare and public health sector, information technology sector; nuclear reactors, materials and waste sector, transportation systems sector, water and wastewater systems sector.

Advanced Persistent Threat: Actors that use sophisticated techniques to intrude a computer system and maintain a persistent presence for a prolonged period of time to create potentially destructive consequences

Living-off-the-land: Technique used in a cyber-attack which leverages pre-existing software in the target systems or run attacks in the memory to evade detection

). Cyber incidents that involve multiple targets are also included if entities in the U.S. or China are direct targets.

Table 2: Sources for Responsibility Confirmation

Types of source	Examples
US government statements	Federal Bureau Investigation, Department of Homeland Security, Department of State, Department of Defence, US Cybersecurity and Infrastructure Security Agency,
Chinese government statements	China's Ministry of National Defence of the State Council, Ministry of Foreign Affairs, Cyberspace Administration of China
Computer security firms	Kaspersky, McAfee, Symantec, Crowdstrike, Fire Eye, Infosys

This study collects data from a variety of databases such as the DCIDD, CSIS Significant Cyber Incidents Database, Hackmageddon, Council of Foreign Relations Cyber Operations Tracker, RISI Online Incident Database and the National Security Archive. As some databases may not be up-to-date, additional Google search of cyber incidents was conducted, focusing on search terms of "China" AND "U.S." AND "cyber" OR "attack" OR "cyber-attack" OR "network breach" OR "hack", and a customised date range from 1/1/2013

onward. While Valeriano et al. (2017) rely on English-language and Western sources, this study will conduct the same search terms (in Chinese) on Baidu, a popular Chinese language search engine, to avoid the risk of underreporting of cyber incidents inflicted on China due to publisher constraints or lack of Western media correspondence. To ensure the reliability of data, the cyber incidents will be triangulated with other sources including government statements, policy reports and white papers from computer security firms. The underlying objective of each state will be assessed with government publications such as military doctrines, national security strategies, policy papers and the wider academic literature from cyber security journals and magazines such as *Foreign Affairs* and *Journal of Cybersecurity*. Since this study relies on open-source data, there is no major ethical considerations. Cyber incidents that involving sensitive government targets are recorded only after ensuring that the incident has been publicly disclosed. Care is taken to ensure that the work of existing researchers are fairly represented.

Valeriano et al.'s (2017) codebook is the most appropriate for the purpose of this study. It not only captures the relevant details for understanding cyber incidents (e.g. start and end date of attack, third parties, nature of interaction, type of target, type of operation, methods used, operational success, political objective and behavioural change) but also incorporates factors linked to international law including severity, directness and immediacy (Pipyros, Thraskias, Mitrou, Gritzalis, & Apostolopoulos, 2018). However, Valeriano et. al.'s (2017) codebook has three limitations. The severity scale does not differentiate online and offline effects clearly, fails to include second-order impacts such as public confidence and diplomatic relations, and lacks a rigorous assessment of the scope and intensity of each type of impact.

Following Steiger et al. (2018), this study collects first-order effects of espionage and disruption with varying levels of severity. For second-order effects, this study adapts Theoharidou, Kotzanikolaou, and Gritzalis' (2009) list of impact criteria which consists of a set of vigorous and transparent severity

scales for impacts concerning economic, policy implementation and provision of public service, safety, defence, public order, public confidence and international relations (see Appendix 3 for definitions). In addition, the study considers the target's "Interdependency with other critical infrastructure" (see Appendix 3 for definition) and the resulting cascading, escalating or common cause failure on other cross-border and/or cross-sector infrastructure or service (European Union Agency For Network and Information Security, 2018). This coding framework distinguishes from traditional risk analysis methodologies by integrating internal impacts i.e. effects on the affected organisation, commonly found in the traditional methodologies, with external social impacts on the society such as public confidence and public order.

Despite best efforts to code cyber incidents between the U.S. and China, this study will be limited in a few ways. First, the collection of data relies on open sources, thus not all cyber incidents between the U.S. and China are captured since not all incidents are reported due to lack of resources or reputation concerns (Phneah, 2012). Second, information about the effects of cyber incidents may not be easily available. Investigations or litigations processes may be ongoing hence details like information stolen may be unknown. Finally, the blurring distinction between state and non-state actors due to dual military and civil roles has made responsibility confirmation difficult since state actors may be motivated to hack for personal reasons while in their official positions.

3.2 Presentation of Findings

3.2.1 Chinese Cyber Operations

A. Analysing Intent through Nature of Attacks

Most Chinese cyber operations on the U.S. are offensive, three are nuisance operations and none is of defensive nature (see Figure 5). Nuisance attacks aim to disrupt daily operations or scan for information but are usually reversible and easily removable by the target. Cyber operations are classified as defensive if the initiator is responding to a cyber incident in which it was a target, while

offensive cyber operations are conducted to disrupt a specific national strategy or policy, or steal critical information (Valeriano et al., 2017). Of 47 Chinese cyber-attacks coded, only two constitute disruptive events. These disruptions consist of temporary, low-cost and low-intensity DDoS attacks to counter political dissidents and maintain strong censorship of political sensitive

Figure 4: Types of Chinese Cyber Operations on the U.S. from Jan 2013 to May 2019

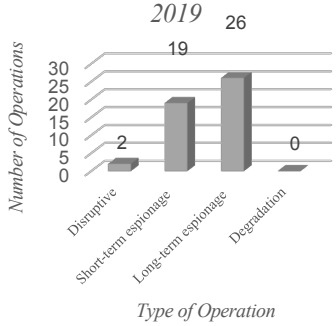
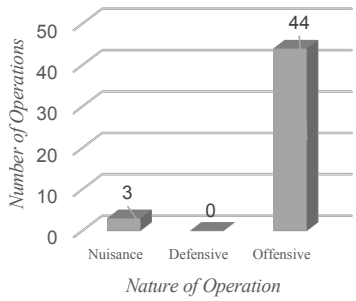


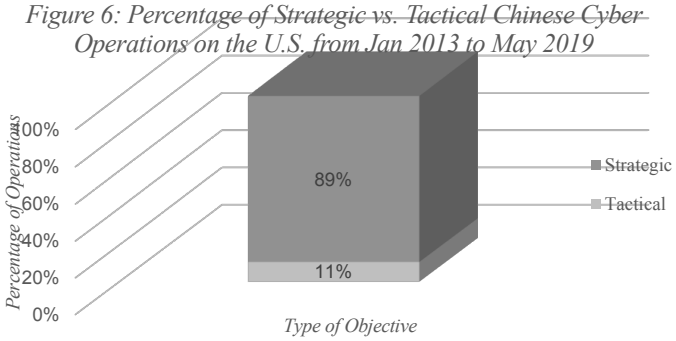
Figure 5: Nature of Chinese Cyber Operations on the U.S. from Jan 2013 to May 2019



materials that are detrimental to the Communist Party of China (CCP). Notably, degradations i.e. attacks that cause irreversible physical damage to the target's capabilities, are absent. China conducts cyber-attacks mostly for offensive espionage purposes. Of the 47 instances, 19 are short-term espionage incidents that last no longer than six months while 26 are long-term espionage incidents (see Figure 4). Espionage incidents seek to steal critical information for an immediate or a future advantage. The range of targets spans from private entities in healthcare, media companies, technological industries and non-government organisations to government military and non-military agencies.

China conducts cyber operations for tactical and strategic reasons, of which 11% (5 out of 47) of the cyber incident are short-term tactical events while a vast majority of 89% (42 out of 47) are conducted for strategic purposes (see Figure 6). Tactical cyber-attacks typically respond to external events deemed detrimental to the initiating state's national security interests. China launches tactical cyber-attacks to clamp down on external sensitive information that challenges the CCP's political legitimacy. The short-term espionage on *The New York Times* and the DDoS attack on Github exemplify China's attempts to

Figure 6: Percentage of Strategic vs. Tactical Chinese Cyber Operations on the U.S. from Jan 2013 to May 2019

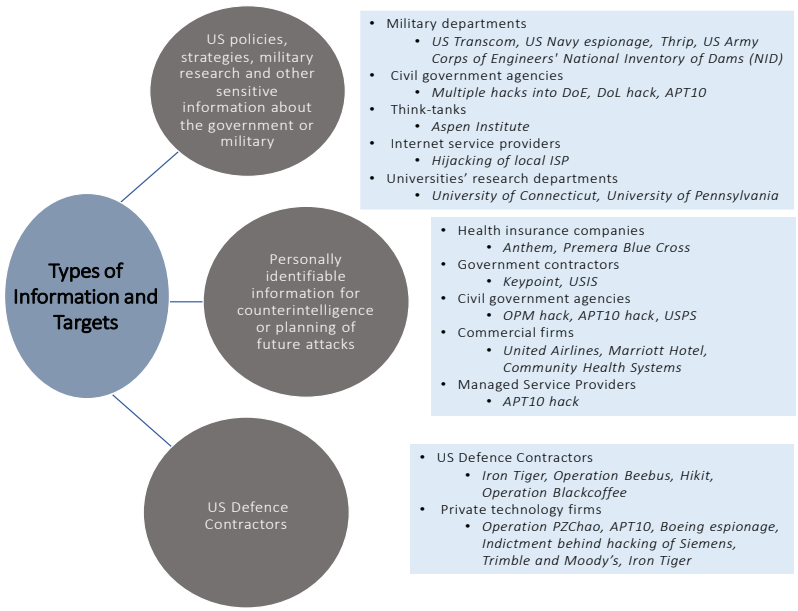


control external information that runs counter to its censorship efforts. They also serve as signalling functions for expressing resolve and risk of escalation against the continuation of the adversary's plans (Valeriano et, al., 2018). China also launches tactical cyber-attacks in response to political events that potentially endanger its core interests. Territorial issues over Taiwan and the South China Sea are evidenced to intertwine with China's cyber operations. Both incidents feature spear-phishing attempts (see Appendix 1 for technical definition) – the former targeted at officials visiting the U.S. aircraft vessel just one day before the international court ruling on the territorial claims of the South China Sea, while the latter targeted attendees of the U.S.-Taiwan security conference. Although both attacks were thwarted upon discovery, cyber operations are potentially a convenient tactic to gain intelligence on perceived external threats.

Most Chinese cyber-espionage operations are conducted by actors with strategic intent. These actors, known as Advanced Persistent Threats (APT), use sophisticated techniques to intrude a computer system and maintain a persistent presence for a prolonged period of time to create potentially destructive consequences (Kaspersky, 2019). Strategic cyber-espionage can: a) to gain intelligence regarding the target's military and civil departments, including the number of weapons and forces, available resources and finances, identities and background of government personnel and internal workings of the U.S. government, b) to loot commercial trade secrets and IP from private U.S. firms, which may be used to advance national security objectives or benefit selected Chinese firms.

Among strategic cyber-espionage incidents, 81% (34 of 42) of the cases gathers intelligence from traditional targets including military or civil departments constitute (see Figure 7). Chinese hackers commonly pilfer intelligence directly linked to U.S. policies, strategies or other sensitive military data from U.S. military departments, civil departments and influential think-tanks. The digitisation of information allows Chinese hackers to siphon large troves of personally identifiable information (PII) from public and private entities such as health insurance companies, civil government agencies and government contractors. PII is valuable for counterintelligence purposes or planning of future attacks. 36% (15 of 42) of Chinese strategic cyber-incidents involve looting of intellectual property (IP) such as trade secrets or other sensitive business information (see Figure 7). The common targets are universities with defence technology research, private firms in key defence and technology-related fields such as aerospace, energy and maritime. Managed Services Providers (MSPs), i.e. entities that remotely manage a customer's IT infrastructure, are a relatively novel target (see Figure 8 for an overview of targets and sources).

Figure 8: Chinese Strategic Espionage: Types of Targets and Sources



B. Analysing Capabilities through Online Effects and Methods

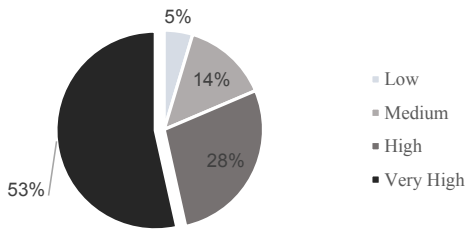
Nearly all of Chinese cyber incidents (45 of 47) are operationally successful, with only two attacks on the U.S. aircraft carrier and U.S.-Taiwan Security

Conference being thwarted at an early stage. 81% (35 of 43) of success cyberespionage operations scored 'Very High' or 'High' first-order impacts in espionage (see Figure 9). First-order impacts are rated according to the type of data and its quantity. 'Very high' and 'high' scores are credited to cyber operations concerning critical information with direct tactical or strategic applications e.g. military intelligence, weapon system designs, IP or PII. Sensitive information such as policy documents that have little tactical or strategic applications are deemed to have a lower impact. Cyberespionage incidents are deemed to impose 'Very High' first-order impact when more than five million records are stolen, or the length of operation exceeds a year (see **Chyba! Nenalezen zdroj odkazů.** and Table 3).

Table 3: First-order impact of Chinese Cyberespionage

First order impact	Examples of Cyber Operations (not the full list)	Year Ended
Very High	Operation Beebus, US Transcom hack	2013
	Indictment of 5 in China army, Multiple hacks into Department of Energy, Anthem Breach	2014
	Premera Blue Cross breach, Office of Personnel Management (OPM) hack, Iron Tiger	2015
	US government and contractor networks hacked	2016
	Indiction of 3 Chinese nationals behind hacking of Siemens, Trimble, Moody's, Hijacking of Local Internet Service Provider	2017
	Operation PZChao , Operation Cloudhopper, Thrip	2018
High	Department of Labour hack, US Army Corps of Engineers' National Inventory of Dams (NID)	2013
	Operation Snowman, USIS hack, Keypoint hack	2014
	University of Connecticut Engineering hack, United Airlines, University of Pennsylvania state engineering hack	2015
Medium	Aspen Institute, NY Times attack, Operation Ephemeral Hydra	2013
	US government agency hack, University of Virginia	2015
Low	Overseas Chinese language new websites	2017
	Operation Tradesecret	2017
	Opportunity Alaska	2018

Figure 9: First-order Impact of Chinese Cyberespionage Operations from Jan 2013 to May 2019



The most common method of Chinese cyberespionage is via intrusion and infiltration of networks, with one exception being the hijacking of the Border Gateway Protocol of local Internet Service Providers. Chinese hackers compromise systems through watering hole attacks or spear-phishing emails (see Appendix 1 for technical definitions). They exploit vulnerabilities in popular applications such as Microsoft Internet Explorer, Microsoft Office, Adobe and Java to deliver malware to targets. APT actors are usually identifiable by custom malware they use (see Appendix 1 for technical definition of APT). For instance, the Hikit is a malware highly skilled at obfuscation within legitimate computer processes and has enabled APT17 to pilfer data from defence and technology industries for over six years (Scott & Spaniel, 2016). APT19 commonly uses Sakula, a Remote Access Trojan in several campaigns such as the Anthem and United Airlines hacks. APT groups share a common pool of human and technological resources hence their tactics, techniques and procedures are often not exclusive (Hegel, 2018).

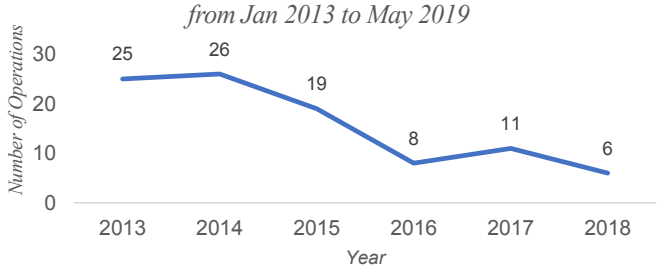
Chinese hackers are also use increasingly sophisticated methods to increase stealth (Segal, Hoffman, Hanson, & Uren, 2018). In June 2018, Thrip hackers used living-off-the-land tactics, which leverage pre-existing software in the target systems or run attacks in the memory to evade detection (Wueest, 2017).

Similarly, APT10 hackers fashioned malware out of open-sourced tools and used legitimately signed software such as Windows Defender to launch cyber-attacks. The hackers' ability to adapt to network defenders by combining open-sourced tools with in-house malware development proves their increasing sophistication and intention to avoid getting caught.

C. Trends in Chinese Cyber-attacks

Overall, publicly known Chinese cyber activity on U.S. entities dropped significantly by 75% from 2013 to 2018, with the first 27% decrease in 2015 and a 58% decrease in 2016 (see Figure 10). The decrease in 2015 is possibly correlated to the unprecedented indictment of five members of the Chinese military in May 2014 (Fireeye, 2016). The second major decrease in 2016 possibly relates to the 2015 U.S.-China agreement to forbid commercial hacking or the restructuring of Chinese military, in which espionage responsibilities were shifted from the PLA to the Ministry of State Security (MSS) (Fireeye, 2016). China's targets also shifted from the U.S. to regional targets such as Japan, Tibet and Hong Kong in 2016 (Bennett, 2017). The sustained low number of cyber-attacks after 2016 suggests China's hackers have become more sophisticated under the MSS to launch attacks that to evade detection.

Figure 10: Total ongoing Chinese cyber incidents from Jan 2013 to May 2019



Operation Cloudhopper reflects novel targeting on IT service providers that was previously not observed. This targeting strategy of attacking supply chains or

third-party providers to access ultimate targets such as defence and technology firms is efficient and effective. By hacking supply-chain infrastructures which comes with invested trust by its clients, Chinese hackers can obtain access to the vast troves of clients easily for future attacks (Fisher, 2019).

D. Analysing Consequences – Second-order Impacts

Second-order impacts of Chinese cyber operations are typically economic loss, weakening of public confidence and impact on diplomatic relations. No Chinese cyber-attacks thus far engendered degradation effects on public safety, state defences, public order or government operations. Economic loss is associated with attacks involving the theft of IP or PII (see Figure 8). Direct costs arise from increased competition and lost business (Center for Strategic and International Studies (CSIS), 2013), while indirect costs include detection and forensic investigation activities, notification costs, post-breach remediation costs and lost business stemming from system disruption and reputation loss. A stolen record of PII is estimated to cost an average of U.S.$148 in 2018 (Ponemon Institute, 2018). Massive loss of PII from private and governmental entities weakens in public confidence since individuals are personally affected and made aware through mandatory breach notifications (Skeath & Kahn, 2018). Diplomatic relations are usually adversely affected when there is theft of IP or the targets involve governmental entities. However, no single cyber incident between China and the U.S. has caused material damage and diplomatic reactions are limited to verbal condemnations.

In addition, targets with high (inter)dependencies such as telecommunications, satellites and MSPs typically results in more severe impacts. The material outputs of infrastructure with high (inter)dependencies are usually depended upon by other cross-border or cross-sector infrastructures (Petit et al., 2015). For instance, a destructive cyber-attack on dams will create public safety concerns and impairment of other infrastructure such as roads, bridges and water systems. The espionage incident on the National Inventory of Dams creates a greater loss of public confidence since it can enable a destructive attack that

threatens the loss of lives. Overall, 98% (46 of 47) of China' targets enjoy medium to high dependence by other critical infrastructure (see **Chyba! Nenalezen zdroj odkazů.** for definition), demonstrating its ability to inflict widespread impacts.

In summary, Chinese cyber operations against the U.S. have advanced in sophistication and stealth, resulting in an overall decline in the quantity of cyber-attacks observed. However, the observed decline does not imply a reduced threat on the U.S., but publicly reflect Chinese ability to evade detection. Furthermore, increased targeting on supply-chain entities suggests that China is able to inflict widespread yet targeted attacks on selected entities. However, China's broad strategy of conducting long-term and short-term cyberespionage for political, economic and military gains remains consistent throughout the years.

3.2.2 U.S. Cyber Operations

A. Analysing Intent Through Nature Of U.S. Attacks

Open source data regarding U.S. cyber-attacks on China is sparse aside from revelations of U.S. intelligence activities by Edward Snowden. There are three U.S. cyber-attacks for the period from January 2013 to May 2019 (see Table 4). Like China, the U.S.' strategic objective is to gain military and political intelligence, including commercial data, which will enable it to launch future attacks. Arroweclipse is a defensive operation in which the U.S. degrades China's cyberespionage efforts by conducting man-in-the-middle attacks (refer to **Chyba! Nenalezen zdroj odkazů.** for technical explanation) to observe and modify its espionage operations. Shotgiant is an offensive operation directed at Huawei to uncover its political links with the CCP and political plans and obtain the source code of Huawei's products for future exploitation. However, unlike China, the U.S. also leverages its cyber operations against China to spy on other countries. For instance, hacking Huawei's equipment helps the U.S. to fill intelligence gaps of non-allies, such as Iran, Afghanistan, Pakistan, Kenya and Cuba (Sanger & Perlroth, 2014). Similarly, Fourth Party Collection is a

defensive operation to degrade China's espionage operations against other countries by stealing the tools, tradecrafts and intelligence from China's cyber operation. Unlike China, the U.S. does not conduct tactical disruption operations or short-term cyberespionage operations against non-critical targets.

Table 4: Details of US Cyber Operations

US Cyber Operations *(Period of Operation)*	Nature of Interaction	Type of Operation	Target	Objective
Operation Arroweclipse ***(1 Jul 2009 to 13 Jun 2013)***	Defensive	Degradation and Long-term espionage	Chinese espionage activities on the US	Tactical – To counter China's espionage campaigns (Byzantine series) by attributing its activities to user accounts Strategic – To conduct man in the middle operations to observe and modify the Chinese espionage campaigns
Operation Shotgiant ***(3 Oct 2010 to 13 Jun 2013)***	Offensive	Long-term espionage	Huawei	Strategic – To determine if Huawei is spying for the Chinese leadership and obtain intelligence of the CCP's plans and intentions through monitoring the communications of Huawei's top executive, to exploit Huawei's products for future offensive use through obtaining the source code. Tactical – N.A.
Fourth Party Collection ***(1 Jun 2009 to 13 Jun 2013)***	Defensive	Degradation and Long-term espionage	Chinese foreign espionage activities	Tactical – To degrade and intercept Chinese foreign espionage operations Strategic – To steal tools, tradecraft, targets and intelligence from Chinese foreign espionage operations.

B. Analysing Capabilities through Online Effects and Methods

Similar with China, U.S. cyber operations use complex intrusion and infiltration methods. Arroweclipse and the Fourth Party Collection both feature degradation effects on PLA's cyber operations. The direct and precise attacks on China's military operations imply substantial sunk costs and signal U.S. resolve in this cyber conflict (Valeriano et al., 2018). Particularly, Arroweclipse evidences the US' ability to attribute attacks against its Department of Defense (DoD)

networks. It utilised Tutelage, a man-in-the-middle technique, to monitor, intercept, redirect or slow down cyber-attacks. The technique enabled the U.S. to trace cyber-attacks to IP addresses and billing addresses, which ultimately attribute the perpetrator to be China's PLA (Appelbaum, Horchert, & Stocker, 2013).

Arroweclipse also demonstrates the US' ability to conduct offensive counterintelligence by converting defence mechanisms to attack vantage points. Tools like XKeyscore process and filter different types of network traffic for defensive purposes and identify foreign botnets for exploitation (Lee, Greenwald, & Marquis-Boire, 2015). Its Quantum exploits can trick the foreign botnets into identifying the NSA as their trusted command and control centres, thus allowing it to inject malware alongside the botnet to target the original or new victims (Gallagher, 2015). These tools help to evade detection since the attack vantage points are "throw-away" and "non-attributable" (Constantin, 2015a).

In addition, the U.S. owns a vast trove of other offensive cyber tools listed in the NSA's 50-page Advanced Network Technology catalogue (Appelbaum et al., 2013). It penetrates the firmware of domestic computer security firms such as Cisco, Dell and Hewlett Packard through custom implants in USB cables. The U.S. also injects critical implants in software supply chains to conduct broad-based passive surveillance and active modification and diversion of data (Gallagher, 2013).

Like China, U.S. cyber operations score 'Very High' in first-order effects. They are successful in compromising critical information such as China's cyberespionage infrastructure and military intelligence in all three sophisticated degradation and long-term espionage operations. Shotgiant also imposes common second-order effects of espionage operations such as financial loss and weakening of diplomatic relations. However, the degradation operations in Arroweclipse and Fourth Party Collective create second-order effects not found

in China's cyber operations against the U.S. by successfully thwarting China's espionage objectives and ability to implement cyber policies.

Overall, data on U.S. cyber operations is sparse compared to China's cyber operations[1]. On the one hand, China's cyber defences remain weak compared to the U.S. (Austin, 2018). This implies that detecting, analysing and attributing attacks will be a significant challenge. Chinese authorities may also be more inclined to conceal cyberespionage incidents due to fear of embarrassment and the potential liability (Brookes, 2014). On the other hand, most major cybersecurity companies such as Fireeye, F-secure and Verizon are Western-centric, which implies their ability to detect and analyse attacks in Chinese companies may be more restricted due to a smaller pool of Chinese clients. Finally, the U.S. cyber operations are highly sophisticated and hence technically difficult to trace. The U.S. has little incentive to reveal these attacks since they are already historically proven to be superior in cyber capabilities.

Okomentoval(a): [KLT(4]: Add in more points of comparison between us and china attacks

Despite the sparse data, the cyber incidents recorded were insightful in revealing the U.S.' capabilities and intentions. Such capabilities include detecting and attributing attacks, and converting defence mechanisms into attack points. Besides gaining political and military intelligence about China, the cyber incidents also reflect U.S. covert ambitions to establish a global surveillance network via hacking Chinese software to infiltrate non-partner networks.

[1] Please see Appendix 7 for a full list of cyber operations between the U.S. and China from 1 Jan 2013 to 31 May 2019.

IV. Cyber Hype

The next section presents the methodology for cyber hype and assesses specific aspects of government discourses in the OPM hack and Operation Cloudhopper that contains hype. The study finds that U.S. government officials tend to exaggerate China as an unprecedented threat in cyber-enabled commercial espionage and overstate the life-threatening effects of counterintelligence impacts of political espionage without providing evidence to substantiate their claims.

4.1 Research Methodology

This paper assesses hype according to Dunn Cavelty's (2008a) threat politics framework. Since U.S. government officials are the securitising actors, the study collates publicly available government officials' discourse surrounding selected cyber incidents. Although news media play a role in shaping public perception, they are not used to study cyber hype because they alone do not create or influence the threat frames formed in political circles. Rather, media content amplifies and raise public awareness of political issues (Dunn Cavelty, 2008a). Due to time and space constraints, not all cyber incidents are assessed for cyber hype. Instead, purposive sampling is used to strategically select cyber incidents such that they address the research goals (Bryman, 2016). For each type of strategic objective – a) military and civil intelligence and b) commercial intelligence, cyber incidents that generated the most political discourse among U.S. government officials were selected. Cyber incidents with tactical objectives are not sampled since they impose short-term and negligible impacts that are not key to U.S. threat perception of Chinese cyber-attacks.

The number of news articles generated from Nexis, an online news database, is used as a rough indicator of the availability of government statements surrounding a cyber incident. Relevant news articles for each cyber incident identified in the 'Cyber Reality' chapter are retrieved through the following keyword search statement: "Cyber Incident" SAME SENTENCE ("breached"

OR “hack” OR “hacked” OR “hacking” OR “attacked” OR “compromised” OR “intruded” or "infiltrated" or "hackers" or "spies" or "cyberespionage") AND ("U.S." OR "U.S." OR United States" OR "China" OR "Chinese"). The search is limited to “U.S. Newspapers and Wires”, with the date limits set from the discovery date to one year after the end of the cyber incident. To reduce the number of repeated or irrelevant sources, the location for the keywords of “Cyber Incident ” is set to “Major Mentions”. The search results yielded the top five cyber incidents with the greatest number of news articles: the OPM hack (66), Operation Cloudhopper (30), Anthem breach (24), Community Health Systems breach (23) and Boeing espionage (18). The OPM hack and Operation Cloudhopper are selected as cases of cyber incidents with strategic objectives to gain political and commercial information respectively since they yield the highest number of news articles (purposive sampling).

Statements by past and present government officials are sourced from primary U.S. government sources such as indictment records of the Department of Justice, press releases of the Department of State, digital library of the Department of Homeland Security (DHS), Department of Defense and congressional records. Secondary sources of news articles found in the Nexis database are also examined for any comments or statements by U.S. government officials. Since all sources are publicly available, no major ethical considerations exist. However, care has been taken to ensure that the government officials’ statements are accurately and fairly represented. The statements from different government officials in each source are numbered (See Appendix 5). Dunn Cavelty’s (2008a) threat politics framework drives data collection by defining the coding categories of the government statements. Since the study focuses on the process of threat framing or securitisation, only the components of ‘problem recognition’, ‘frame actor’ and ‘diagnostic threat frame’ in the threat politics framework will be analysed. The categories coded are shown in Figure 11.

Thereafter, the study employs Fairclough's (1995a) framework of Critical Discourse Analysis (CDA) for data analysis. His analytical framework focuses on the three elements of a communicative event: text, discourse practice and sociocultural practice. Textual analysis involves linguistic factors such as vocabulary, grammar and textual structures while sociocultural practice encompasses economics, politics and culture (Fairclough, 1995b). Discourse practice refers to the production and consumption of texts that interfaces between both interconnected and mutually reinforcing factors of text and sociocultural practice. Though similar CDA frameworks exist (van Dijk, 1993; Wodak, 2011), their emphasis on historical contexts of discourse (Wodak, 2011) and sociocognition of the discourse's audience (van Dijk, 1993) extends beyond the scope of this study. This paper centres on textual analysis and briefly discusses discourse production to elucidate how U.S. government officials' statements echo or deviate from one another.

The interpretative nature of the CDA method implies that biases are present due to the lack of structure in identifying and analysing texts (Phillips & Hardy, 2002; Stubbs, 1997; Widdowson, 1998). For instance, texts can be cherry-picked to serve the researcher's purposes (Widdowson, 1998). However, this study uses all government statements found due to the limited data available. To mitigate potential bias, Habermas' (1984) theory of communication action framework is used for textual analysis. Unlike other linguistic methods of textual analysis (Bell, 1984; Cheng, 2013; Fowler, 1991), Habermas' framework considers the meaning of the text along with situational facts and political context in conjunction with linguistic dimensions of syntactics and semantics. It provides a structured way to test empirical data by stipulating four validity criteria, i.e. truth, sincerity, legitimacy and comprehensibility to map onto textual elements (See Table 5).

The 'truth' criterion tests for the validity of the argument i.e. whether the argumentation made in the claim is factually correct, logically consistent and complete (Cukier, Ngwenyama, Bauer, & Middleton, 2009). Truth is assessed

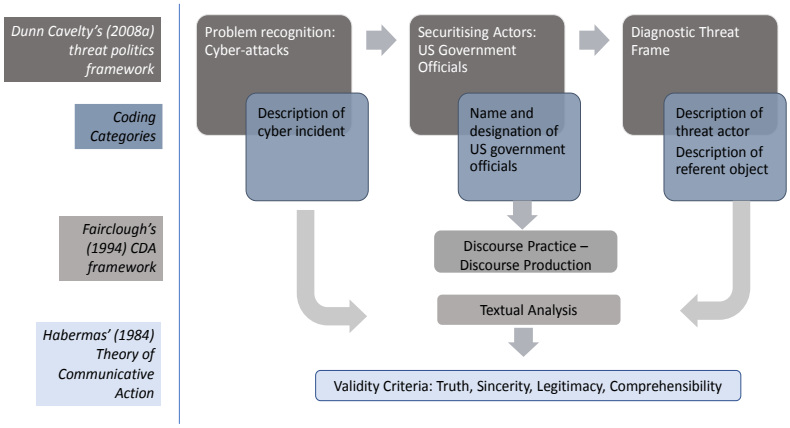
from the cyber incident data coded under the 'Cyber Reality' chapter. Sincerity examines whether the speaker is honest by comparing what is stated to how it is stated i.e. whether hyperboles and metaphors are used to reinforce a claim. Legitimacy addresses whether the government statement matches the social context and whether contrasting opinions are represented.

Table 5: Habermas' (1984) Theory of Communication Framework applied to Textual Analysis of CDA

Validity Claim	Criteria for Ideal Communication	Potential Distortion	Speech Dimensions for analysis
Truth	Claims by government officials are factual.	Misrepresentation of facts	Argumentation and evidence
Sincerity	Government officials are sincere and honest in their claims.	Exaggeration to promote certain understanding by attempting to invoke an emotional response	Hyperbole, Metaphors and other connotative words
Legitimacy	Claims by government officials are right and appropriate considering existing norms and values.	Suppression or exclusion of certain viewpoints	Use of people who are deemed to be experts, Silences of certain groups
Comprehensibility	Claims are comprehensible or intelligible.	Obfuscations due to incomprehensible language, use of jargon	Syntactic and semantics

This paper also assesses discourse practice under the 'legitimacy' claim to understand the motivations of government officials behind the discourse. Lastly, comprehensibility involves analysing the syntactics and semantics of the statement to determine the degree of linguistic or technical clarity (Cukier et al., 2009) (See Figure 11 for an overall analytical framework). The following section analyses the OPM hack and Operation Cloudhopper by conducting textual analysis of the cyber incident, threat actor and referent object using the Habermas' (1984) four validity criteria.

Figure 11: Overall Analytical Framework for Cyber Hype Analysis



4.2 Presentation of Findings

4.2.1 Case Study 1 – The OPM Hack

A. Background

The first OPM hack occurred on March 20, 2014, when information about OPM servers was exfiltrated. OPM implemented a remediation strategy, dubbed the "Big Bang" on May 27, 2014. While Big Bang eliminated X1 from OPM's systems, it overlooked another hacker, X2. X2 intruded the system on May 7, 2014 and secured a foothold in the system post Big-Bang. From July 2014 to early 2015, X2 exfiltrated vast troves of information including security clearance background investigation files on 21.5 million individuals, 4.2 million former and current personnel records and 5.6 million fingerprint data (Constantin, 2015b). OPM subsequently detected X2 on April 15, 2015. The exact scope of the hack is indiscernible due to potential direct or indirect linkages of the OPM database with the intelligence community's security clearance database (Finklea, Christensen, Fischer, Lawrence, & Theohary, 2015; Takala, 2015).

B. Textual Analysis of Claims

- Analysing Truth of claims

The government officials primarily assert that the OPM hack is 'massive' and impose 'serious' national security consequences via intelligence and counterintelligence impacts (see Table 6). According to the law enforcement officials and intelligence officials, the sensitive nature of personal information stolen allows China to possess an information edge to recruit spies and gain military intelligence (OPM60)[1] or to retaliate against the officers undergoing covert missions (OPM17). As a result, they project that many lives, especially those of law enforcement personnel, will be endangered (OPM42).

Given the sheer number of the individuals implicated, the OPM hack is indeed 'massive' (see Table 6). The sensitive nature of information undoubtedly increased the U.S.' vulnerability to China's intelligence and counterintelligence threats. The CIA has reportedly withdrawn its officers from the U.S. embassy in China under precautionary reasons (Nakashima & Goldman, 2015). Despite the precautionary measure taken by the U.S. to 'mitigate the damage in the intelligence and counterintelligence arena' (OPM37), U.S. officials' claims about the irreversible impacts of the hack (OPM14, OPM11) are true because limiting the scale of damage does not recover critical information that was compromised. The U.S. intelligence capabilities are permanently eroded, since the CIA officials adept in gathering Chinese intelligence are forced to abort operations.

Though intelligence impacts are true, claims that the perpetrators of the OPM breach will use the stolen data to inflict physical harm on specific U.S. individuals and their family members cannot be ascertained (see Table 6). Five years after the OPM hack, the only evidence to date that demonstrates the illicit

[1]The individual government claims in the OPM hack are numbered with the prefix 'OPM'. Please see the numbered sources under Appendix 5.

use of OPM data was a bank fraud and identity theft case in which the perpetrators took out car and personal loans using the PII of OPM victims (Weiner & Hawkins, 2018).

By focusing on the future impacts of the hack, U.S. government officials neglect to mention the present consequences of the hack. For instance, the financial impact of the hack is absent from the government statements. Apart from tens of millions spent to modernise OPM's antiquated technology systems (Miller, 2018), large monetary sums are needed for credit and identity monitoring, identity theft insurance and identity restoration services at least till 2026 (OPM, 2019). The U.S. government officials may have chosen to exclude these facts to underscore the importance of other national security or counterintelligence implications.

In addition to intelligence and counterintelligence impacts, the increased sophistication of Chinese hackers also bear truth (see Table 6). U.S. government officials asserted that China must possess the big data management tools to aggregate and analyse the sheer volume of data (OPM6). Given the prevalence of tailored advertising, big analytics software can likewise be modified for intelligence analysis purposes (Gertz, 2016). U.S. government officials also acknowledged the U.S. also bore responsibility for the OPM hack since inadequate cybersecurity measures made OPM an easy target. OPM was slow to overhaul its antiquated systems despite several warnings by the inspector general since 2007 (OPM40).

Notably, majority of U.S. government officials are reluctant to explicitly name China as the perpetrator. Among 32 statements describing the threat actor, eight directly referred to Chinese government as the perpetrator while the others use generic terms such as "enemies", "adversary", "intruders" or "hackers" (see Table 7). The restraint in calling out China aligns with the Obama administration's decision against publicly attributing blame to China (Nakashima, 2015). The U.S. does not want to risk exposing its intelligence-

collection capabilities such as intercepting global communication (OPM68). It distinguishes between political and commercial espionage (OPM5, OPM37, OPM63). While commercial espionage warrants criminal charges, political espionage invokes counterintelligence effects (Finklea et al., 2015). The OPM hack falls within the limits of traditional espionage and thus legal action against the OPM hackers will imply that the NSA spies in China will also be subject to the same standards (Sanger, 2015). Since both nations engage in political espionage for national security purposes, U.S. response against the OPM hack has been muted.

Overall, the truth criterion is partially met. The U.S. government officials rightly asserted consequences on U.S. intelligence abilities, identified China as a sophisticated actor and acknowledged its own responsibility in failing to implement adequate cybersecurity measures. However, U.S.' claims of China's culpability in using the stolen data to harm U.S. intelligence officials i.e. counterintelligence impact, albeit conceivable in theory, are not supported with publicly available evidence.

Table 6: OPM Hack: Assessing Truth Claims of Cyber Incident, Threat Actor and Referent Object

No.	Coding Category	Description	Sources	Examples
1	Cyber incident	The OPM hack is 'massive' and the number of records stolen are 'staggering'.	OPM5, OPM22, OPM32, OPM41, OPM55, OPM56, OPM58, OPM59, OPM60, OPM62	"China is building massive databases" "massive theft of data" "massive data breach" "Today's new number is staggering" "extent of the breaches is enormous"
2	Cyber incident	The OPM hack has a 'serious' impact on 'national security'.	OPM13, OPM17, OPM20, OPM49, OPM51, OPM55, OPM56, OPM58, OPM59, OPM60, OPM62	"This is a very serious issue" "certainly one of the most damaging losses" "very big deal from a national security perspective" "profound impact on our national security" "very serious national security threat" "serious blow to our national security"
3	Cyber incident	The OPM hack imposes 'devastating' intelligence and counterintelligence consequences because of increased information edge in recruiting spies or targeting individuals.	OPM1, OPM5, OPM6, OPM7, OPM9, OPM10, OPM13, OPM17, OPM27, OPM37, OPM60, OPM62	"This is potentially devastating from a counter-intelligence point of view" "very big deal [...] from a counterintelligence perspective" "a setback that will have long-lasting and painful counterintelligence consequences" "Only the imagination limits what a foreign adversary could do with detailed information..."
4	Cyber incident	The consequence inflicted by the hack is irreversible.	OPM14, OPM11	"There's no fixing it" "cannot undo this damage"
5	Cyber incident	The OPM hack poses 'danger' to the lives of individuals.	OPM42, OPM55, OPM56, OPM60	"The very lives of Federal law enforcement officers are now in danger, and their safety and security of innocent people, including their families, are now in jeopardy" "It has put people's lives and our Nation at risk"
6	Threat actor	'Foreign power' will use the stolen OPM data to inflict 'harm' on the US by recruiting spies, 'unmasking identities', blackmailing or retaliating.	OPM1, OPM3, OPM5, OPM8, OPM9, OPM17, OPM60, OPM66	"makes them easier to recruit for foreign espionage on behalf of a foreign country" "They could start unmasking identities" "They can find specific individuals they want to go after, family members" "And they're trying to harm us"
7	Threat actor	China is an increasingly sophisticated adversary.	OPM5, OPM6, OPM7, OPM8, OPM9, OPM54, OPM57	"They're becoming much more sophisticated in tying it all together" "It certainly requires greater sophistication on their part in terms of being able to take out this much data" "a sophisticated nation-state adversary"
8	Referent object	The OPM is to be blamed for inadequate cybersecurity measures and slow response to the hacks.	OPM30, OPM35, OPM37, OPM40, OPM42, OPM45, OPM47, OPM48	"we need to acknowledge our own culpability in failing to adequately protect so obvious a target" "The fact OPM was breached should come as no surprise given its troubling track record on data security" "OPM's abysmal failure and its continued ignorance in the severity of the breach."
9	Referent object	The US also practises cyber espionage for intelligence collection activities.	OPM26, OPM46, OPM64, OPM68, OPM69,	"I did not say it's a good thing. I'm just saying that both nations engage in this" "If I [as head of the NSA] could have done it, I would have done it in a heartbeat."

Table 7: OPM Hack: Naming of the Threat Actor

Description of Threat actor	Source	Count
China/Beijing/Chinese government hackers/Chinese government/Chinese counterintelligence authorities	OPM5, OPM17, OPM23, OPM62, OPM38, OPM8, OPM7, OPM9	8
Chinese	OPM6, OPM14, OPM18, OPM26, OMP46	5
Foreign power, Foreign intelligence service, Foreign entities	OPM66, OPM10, OPM49	3
Adversary	OPM2, OPM27, OPM44, OPM52, OPM57	5
Cyber intruders	OPM54	1
Hackers	OPM55	1
Enemies	OPM60	1
Perpetrators	OPM61	1
They	OPM1, OPM3, OPM19, OPM51, OPM58	5
Can't confirm identity, or refuse to make attributions	OPM21, OPM68	2
	Total	32

- Analysing sincerity of claims

The sincerity criterion examines whether the speech text matches the speaker's underlying agenda. Rhetorical devices such as hyperboles, imagery, emotive language or syntactical structures, which may reinforce or suppress certain perspectives (Cukier, Bauer, & Middleton, 2004). This section identifies the rhetorical devices used to reinforce the negative portrayal of the cyber incident and the threat actor.

Of 69 sources, 27 contain negative connotative language regarding the impact of the hack. The choice of emotive language, hyperbole and imagery devices reinforces negative perceptions of the hack (see Table 8). Emotive words such as "devastating" (OPM1), "disturbing" (OPM17) and "disconcerting" (OPM41) emphasise the adverse impact on U.S. intelligence capabilities. Such use of emotive words is reasonable following the withdrawal of U.S. intelligence officials from Beijing. Government officials also analogised the hack as "terrorism", "9/11" and "Pearl Harbour" to invoke disastrous images of the hack

associated with these well-known events. However, noting that these events involve large number of human deaths, the statements are clearly exaggerations given that no publicly available evidence to date shows the lives of American citizens being endangered by China's information advantage from the OPM hack. Such hyperbolic statements are possibly made to create a sense of urgency among top decision-makers and spur countermeasures. Additionally, the imagery technique is used to describe the information stolen. Metaphors like "Holy Grail" (OPM17) and "crown jewels" (OPM10) emphasise the value of the stolen data and indirectly reinforce the significance of the hack.

While many sources describe the negative impact of the hack, only three contain negative connotative language about the threat actor. China is portrayed an antagonistic villain intent on waging a "cyber war" (OPM58) and "harm(ing)" U.S. interests (OPM8). OPM18 also use parallel clauses of "they know…" to highlight the information advantage attained by China from their knowledge of sensitive or embarrassing secrets.

In sum, the empirical data illustrates that some government officials used rhetorical devices in their speech to reinforce the negative impact of the OPM hack. While some rhetorical devices are reasonable, U.S. government officials misrepresented the nature of the hack using inappropriate metaphors, violating the sincerity criterion.

Table 8: OPM Hack: Examples of Rhetorical Devices

Coding Category	Rhetorical device	Language with negative connotation	Source
Cyber Incident	Emotive language	"devastating"	OPM1, OPM60
		"disturbing"	OPM17, OPM23
		"very disconcerting"	OPM41
		"much scarier than identity theft"	OPM62
	Hyperbole	"one of the most damaging losses"	OPM20
		"an order of magnitude greater than … in the past"	OPM22
		"Only the imagination limits what a foreign adversary could do"	OPM27
	Imagery	"Cancer"	OPM3
		"It's a Pearl Harbour"	OPM28
		"As one who represents the city that was attacked by 9/11, … I consider this attack, … a far more serious one to the national security"	OPM51
		"wake-up call" to the "dangers of cyber-terrorism"	OPM61
Threat agent	Emotive language	"trying to harm us"	OPM8
	Imagery	"vacuum cleaner"	OPM8
		"They are literally, you know, at cyber war with us"	OPM58
	Syntactics	After all, *they know* their vices … Do you have friends in foreign countries…*They know* all about them. That embarrassing dispute… *they know* about that too. Your college drug habit? Yes, that too.	OPM17
Referent object	Imagery	"treasure trove"	OPM13, OPM14
		"Holy Grail"	OPM17
		"crown jewels"	OPM10

- Analysing Legitimacy of Claims

The legitimacy of claims centres around the production of discourse and examines what is absent in the discourse. The government officials hold varying degrees of authority depending on the role they play in various federal departments (see Table 9). Government officials in security and law enforcement agencies, intelligence and investigative congressional committees and cybersecurity positions of federal agencies hold more credibility due to their relevant knowledge and higher degree of familiarity with the subject. Compared with U.S. officials working in general positions, top decision makers such as the Former President of United States, Barack Obama, hold more authority.

However, U.S. government officials' statements also reflect embedded interests of the department they represent. For instance, James Comey, the former Director of FBI, emphasised intelligence or counterespionage consequences (OPM13). Jason Chaffetz, the former Chairman of the House Oversight and Government Reform Committee attributed blame to OPM's poor cyber defences (OPM45). In contrast, Andy Ozment, a former DHS Assistant Secretary for Cybersecurity and Communications, highlighted that his department's implementation of cybersecurity measures led to the discovery of the breach (OPM34).

Authoritative figures like the Director of National Intelligence, James Clapper and the former head of the CIA and NSA, Michael Hayden, acknowledged that the U.S. also conducts espionage akin to the OPM hack, increasing the legitimacy of the discourse. However, few officials noted the impact on the financial and personal security of individuals as the majority focuses on national security implications (see Table 6).

Overall, the discourse surrounding the OPM hack largely holds legitimacy because most government officials (48 of 69) hold relevant positions which grant them greater access to information and thus deeper understanding of the incident.

Table 9: OPM Hack: Types of Government Officials

Types of Government Officials	Example	Source	No.
Officers in law enforcement or intelligence agencies	- (Former)Director of National Intelligence, James Clapper - (Former) Director of FBI, James Comey - (Former) Head of CIA and NSA, Michael Hayden	OPM1, OPM4, OPM7 to OPM11, OPM13, OPM14, OPM17, OPM42, OPM46, OPM63, OPM64, OPM69	15
Government officials in congressional intelligence or investigative committees	- Chairman of House Intelligence Committee, Adam Schiff - (Former) Chairman of House Oversight and Government Reform Committee, Jason Chaffetz - Member on Senate Committee on Homeland Security and Governmental Affairs — Permanent Subcommittee on Investigations, Ron Johnson	OPM20 to OPM23, OPM27, OPM29, OPM30, OPM35, OPM37, OPM41, OPM43 to OPM45, OPM47 to OPM49, OPM51, OPM55 to OPM57, OPM62, OPM65 to OPM67	25
Cybersecurity professionals	- (Former) OPM Chief Information Officer, Donna Seymour - (Former) DHS Assistant Secretary for Cybersecurity and Communications, Andy Ozment - (Former) Chief Information Officer at the Office of Management and Budget, Tony Scott	OPM15, OPM16, OPM34, OPM39, OPM50, OPM52 to OPM54,	8
Top government officials	-(Former) President of United States, Barack Obama - White House National Security Adviser, John Bolton	OPM19, OPM38	2
Anonymous government officials or politicians with no direct exposure to cyber incidents	- Member on the House Committee on Energy and Commerce, Tim Walberg - Member on House Committee on Science, Space and Technology, Barbara Comstock	OPM2, OPM3, OPM5, OPM6, OPM12, OPM18, OPM23 to OPM25, OPM28, OPM31 to OPM33, OPM36, OPM40, OPM58 to OPM61, OPM68	19

- Analysing comprehensibility of claims

The comprehensibility criterion tests whether a claim has technical and linguistic clarity. No evidence suggests that this criterion is violated as the government statements examined follow syntactic and semantic rules. The statements are also grammatically sound and do not contain technical jargon.

Overall, the government discourse regarding the effects of the OPM hack largely focused on intelligence and counterintelligence impacts arising from the

potential use of data stolen. Although the intelligence impacts are true, they are not necessarily existential to U.S. national security. The physical harm associated with speculation of Chinese counterintelligence measures is also hypothetical in the absence of public evidence. Hype is evident in inflated terms like "war", "terrorism" and "Pearl Harbour", which misrepresented the nature of the hack to include physical repercussions. However, the government officials spoke truth by recognising China as a sophisticated actor and acknowledging responsibility in failing to strengthen cyber defences. While U.S. government officials also neglected present impacts of financial loss and effects on individuals, their claims are largely legitimate and comprehensible.

4.2.2 Case Study 2 – Operation Cloudhopper

A. Background

On December 20, 2018, Zhu Hua and Zhang Shilong, members of the APT10, were indicted by the U.S. for a series of global cyber operations from 2006 to 2018. The hackers operated through Huaying Haitai Science and Technological Development Company, a company associated with the Chinese MSS' Tianjin State Security Bureau (Yang & Bland, 2018). APT10 conducts cyber operations mainly to obtain IP and sensitive business information which are closely aligned with Chinese strategic interests (Pricewaterhouse Coopers (PwC) & BAE Systems, 2017). Among their targets are 45 U.S. technology companies and several U.S. government agencies (Department of Justice, 2018c), including eight MSP targets, including Hewlett Packard Enterprise, International Business Machines Corp, Fujitsu and Tata Consultancy Services (Stubbs, Menn, & Bing, 2019). the MSPs' clients e.g. Ericsson, a telecommunications company; Sabre, a travel reservation system and Huntington Ingalls Industries, the largest builder of U.S. Navy's nuclear submarines are also implicated in the hack.

B. Textual Analysis of Claims

- Analysing truth of claims

Most claims regarding Operation Cloudhopper centre on the impact on the U.S. national security through erosion of economic interests, and the attendant benefits that China gains from boosting its high technology industries (see Table 10). The claims allege that APT10 stole the "fruits" of American research (OCH10[2]) and helped Chinese firms gain a competitive edge by simply stealing "free" information (OCH2) which would otherwise require significant economic investment. The economic impact on the U.S. holds true even without China's monetisation of commercial intelligence. According to a 2018 study by Ponemon Institute, companies suffer significant remediation costs from forensic investigation activities, provision of notifications and credit report monitoring services, business disruption and reputation loss, among others (Ponemon Institute, 2018).

However, the U.S. government statements are puzzling for several reasons. First, the indictment did not charge the APT10 hackers for "Theft of trade secrets" under Title 18 of the United States Code, Section 1832 i.e. 18 U.S.C.§1832 (1996), which seeks to "convert a trade secret" for the "economic benefit anyone other than the owner". This is incommensurate with government claims that China gains an "unfair advantage" (OCH1, OCH4) or an "upper hand" (OCH10) by stealing their IP and sensitive business information (OCH2, OCH4). The absence of charges under 18 U.S.C.§1832 also suggests the prosecutors may have decided not to reveal the evidence even if they have found any.

Second, despite acknowledging that the APT10 hackers acted "in association with the Chinese Ministry of State Security's Tianjin State Security Bureau, the indictment did not charge the hackers under 18 U.S.C.§1831 (1996), "Economic Espionage". Economic Espionage refers to the offense for stealing

[2] The individual government claims in Operation Cloudhopper are numbered with the prefix 'OCH'. Please see the sources under Appendix 6.

trade secrets while "intending or knowing" that they will "benefit any foreign government, foreign instrumentality or foreign agent" The absence of economic espionage offense does not support most officials' assertions that the Chinese government is the initiator of the cyber operation (see Table 11).

Third, the indictment did not indicate any personal financial motives on behalf of the Chinese hackers. Even though they were charged for "Fraud and related activity in connection with computers" under 18 U.S.C.§1030 (1984), it did not include the sub-charges under 18 U.S.C.§1030(c)(2)(B)(i), which indicates "purposes of commercial advantage or private financial gain". Other charges relating to wire fraud and identity theft also did not indicate any financial motive of the hackers. In short, the absence of evidence supporting that China, its technology sectors, or the Chinese hackers gained economic benefits from the hack is perplexing.

Next, U.S. government officials allege that China violated the 2015 U.S.-China agreement, which forbids hacking for purely "with the intent of providing competitive advantages to companies or commercial sectors" (The White House, 2015) (see Table 10). Nevertheless, the line between legitimate espionage for national security purposes and illegitimate commercial espionage is ambiguous. Stealing IP or other sensitive business information does not necessarily imply pure commercial motives. The U.S. collects science and technology (S&T) intelligence to appraise global developments in S&T, guide R&D in future capabilities and understand adversaries' strategic intent behind their investments (National Commission for the Review of the Research and Development Programs, 2013). Chinese intelligence agencies may collect trade secrets and sensitive business information for similar reasons. Moreover, some APT10 targets, (e.g. Huntington Ingalls Industries, the ship supplier of the U.S. Navy) are make legitimate U.S. government targets. The 2019 Worldwide Threat Assessment report authored by the U.S. intelligence community acknowledged that cyberespionage against key U.S. technology sectors may address "a significant national security or economic goal" (Coats, 2019). The

overlapping of national security competitive advantage objectives in commercial espionage weakens the claim that China violated its commitment.

Furthermore, there are striking omissions from the officials' claims. APT10's targets also include government entities, such as the U.S. Navy, therefore underscoring that China's intention comprises a complex blend of political, military and commercial objectives behind the cyber incident. However, only two sources (OCH3, OCH10) acknowledged that the effects from political espionage while the rest centre on the theft of commercial data. Even if the Chinese government utilises the hacked information to benefit its local enterprises, it will not necessarily be able to convert stolen technology into competitive products. The increased complexity in cutting edge weapons systems makes replication or imitation harder. Chinese companies are often hamstrung by the lack of technological know-how because such knowledge is increasingly uncodified and require expertise from different fields (Gilli & Gilli, 2019). Admittedly, commercial technology may be easier to absorb and assimilate compared to military technology. Other sensitive business information, such as acquisition plans or financial data, can be immediately leveraged for advantage.

Finally, U.S. government officials correctly noted the sophistication of Chinese hackers in being able to leverage available tools to avoid attribution (OCH15) and the shift in China's strategy from attacking individual targets to focusing on MSPs to compromise multiple targets at once (see Table 9). The latter claim echoes a report by PwC and BAE Systems, which states that APT10 has begun targeting MSPs from 2014 (PwC & BAE, 2017).

In essence, the absence of theft of trade secrets and economic espionage offences in the public indictment does not reflect U.S. officials' claims. US officials also omitted truths regarding the political aspects of APT10's cyber operation and the challenges concerning the conversion of commercial intelligence into business advantage. However, U.S. government officials are

truthful in acknowledging China as a sophisticated hacker and the economic implications on the targeted U.S. firms.

Table 10: OCH: Assessing Truth Claims of Threat Actor and Referent Object

No.	Coding Category	Description regarding Operation Cloudhopper	Sources	Examples
1	Cyber incident	OCH threatens US national security by harming its economic interests.	OCH4, OCH5, OCH7, OCH10	"the threat that these actions pose to the prosperity and security of the United States" "undermines the national security… present a very real threat to the economic competitiveness of companies in the United States" "a real and present commercial threat."
2	Cyber incident	OCH benefits the Chinese economy by boosting the growth of its high technology industries	OCH1, OCH2, OCH4, OCH10, OCH16,	"gives China an unfair advantage at the expense of law-abiding businesses and countries that follow the international rules" "American companies ... spent years of research and countless dollars to develop their intellectual property, while the defendants simply stole it and got it for free" "they can steal sensitive business information that gives competitors an unfair advantage"
3	Cyber incident	OCH violates the 2015 US-China cyber agreeement, which forbids hacking for purely commercial purposes.	OCH4, OCH5	"In 2015, China promised to stop stealing trade secrets... through computer hacking "with the intent of providing competitive advantages to companies or commercial sectors...violates the commitment that China made to members of the international community" "violates the 2015 U.S.-China cyber commitments"
4	Cyber incident	OCH threatens US national security by stealing sensitive political or military intelligence	OCH3, OCH10	"The theft of sensitive defense technology and cyber intrusions are major national security concerns… illegally access information technology systems of the U.S. Department of Defense and the Defense Industrial Base" "APT 10's theft of personally identifiable information from more than 100,000 U.S. Naval service members"
5	Threat actor	China shifts from attacking individual targets to compromising multiple targets in a single attack.	OCH4, OCH6, OCH8, OCH12, OCH13, OCH14, OCH17	"labor intensive, one-off compromises of individual targets" to "force multiplier effects that enable them to compromise multiple targets through a single attack" "Malicious cyber actors working on behalf of the Chinese government have been targeting managed cloud service providers"
7	Threat actor	China is a sophisticated hacker.	OCH15, OCH22, OCH23	"In general, they are using widely available tools or living-off-the-land, That's part of what makes attribution so difficult." The hacking was "high leverage and hard to defend against"

Table 11: Operation Cloudhopper: Naming of the Threat Actor

Description of Threat Actor	Source	Count
China/China's intelligence service/Chinese government	OCH1, OCH4, OCH5, OCH6, OCH9, OCH10, OCH12, OCH13, OCH16, OCH19, OCH21, OCH23, OCH25	13
Chinese hackers/Chinese hacking campaign	OCH7, OCH14	2
skilled adversary	OCH22	1
attackers	OCH26	1
they	OCH20	1
	Total	*18*

- Analysing sincerity of claims

U.S. officials used emotive language and hyperbole to underscore the negative impact of APT10's cyber campaign. They characterised the cyber operation as an "increasing concern" with "galling" and "unacceptable" consequences (see Table 12). They also deemed that the threat posed by Chinese hackers have "never been more pervasive or more potentially damaging" (OCH10). The syntactical repetition in "*our* research, *our* economic investment, *our* development and *our* hard work" (italics added in OCH10) reinforces the harm to American interests. However, such statements stand weak given the lack of publicly available evidence of economic espionage and theft of trade secrets in the indictment.

Most of the other rhetorical devices judged China to be an immoral actor. Four sources described China to be a thief using emotive language like "brazen thievery" or "outright cheating and theft". Other sources reproached China as "unethical", for not playing by the rules by the "flout(ing) the rule of law" and "violat(ing)" 2015 U.S.-China agreement, hence gaining an "unfair advantage" (see Table 11). China was also compared to a "drunken burglar" (OCH26) that attacked "without pulling any punches" (OCH10). U.S. government officials made these word choices to highlight China as the sole violator of global norms, contrasting other "law-abiding" countries (OCH1, OCH10). Yet, Russia and Iran, and even allies such as France also conduct industrial espionage (France24,

2011; National Counterintelligence and Security Center, 2018a). China's actions may be immoral but is not truly exceptional.

Hyperbolic claims describe China as "the most active and aggressive" (OCH19) in cyberspace and that "no country poses a broader, more severe and long-term threat" to the U.S. However, unattributed threat groups such as Xenotime, which is known to compromise industrial control systems, arguably pose a more severe, destructive threat (Ranger, 2019). Finally, syntactical devices are incorporated in the government statements to create powerful discourses.

In summary, language devices have been used extensively in the government statements (17 of 26) to portray China as an exclusive, immoral actor. However, these claims are insincere because industrial espionage by nature is not unique to China. Furthermore, the hyperbolic claims about the unprecedented consequence of the hack are also insincere since the public indictment did not reveal evidence to support such bold claims.

Table 12: Operation Cloudhopper: Examples of Rhetorical Devices

Coding Category	Rhetorical device	Language with negative connotation	Source
Cyber Incident	Emotive language	"galling"	OCH2
		"unacceptable"	OCH4
		"deeply concerned"/"increasing concern"	OCH10, OCH18
	Hyperbole	"countless dollars"	OCH2
		"threats we face have never been more pervasive or more potentially damaging to our national security"	OCH10
Threat agent	Emotive language	"outright cheating and theft"/"brazen thievery"/"theft"/"rampant theft"	OCH1, OCH2, OCH3, OCH10
		"unfair advantage"	OCH1, OCH4, OCH10
		"violates the commitment"/"violates our laws"/"flout the rule of law"/"departs from international norms"	OCH4, OCH5, OCH10
		"malicious actors"/"malicious cyber actors"/ "malign"	OCH5, OCH12, OCH21
		"unethical"	OCH10
	Imagery	"Chinese government's not pulling any punches"	OCH10
		"sweeps up collateral targets of opportunity"	OCH14
		"drunken burglars"	OCH26
	Hyperbole	"no country poses a broader, more severe, and long-term threat"	OCH10
		"most active and aggressive"	OCH19
Referent Object	Syntactics	"our research, our economic investment, our development, and our hard work for their own gain"	OCH10
		"American businesses, American jobs, and American consumers"	OCH10
	Imagery	"reads like a shopping list from China's strategic plans"	OCH6
		"fruits of our research"	OCH10

- Analysing Legitimacy of Claims

Most of the claims (20 of 26) are made by government officials in the Department of Justice, FBI and cybersecurity positions. Their relevant expertise and familiarity with cybersecurity incidents grant them greater credibility to discuss about Operation Cloudhopper (See Table 13). The statements of top government officials such as the Secretary of State also imply greater authority

and hence credibility compared with regular government officials. Additionally, the congruency across multiple federal agencies condemning APT10's cyber operation demonstrates that the indictment is a government-wide effort based on prior consensus.

The legitimacy of claims also depends on the degree to which actors with contrasting opinions are included. The U.S. and global companies may bear part of the responsibility in APT10's successful cyber operation. Many companies that conduct business in China accepts the risk of commercial espionage to profit from the vast market opportunities (Sullivan & Schuknecht, 2019). Some U.S. companies also have poor cybersecurity practices which make them easy targets of cyber-attacks (Varonis, 2018). Since, the government statements are taken from public sources, they naturally exclude these sensitive factors. Nevertheless, the US officials' claims regarding Operation Cloudhopper are largely legitimate.

Table 13: Operation Cloudhopper: Types of Government Officials

Types of Government Officials	Example	Source	Number
Officers in law enforcement or intelligence agencies	- Deputy Attorney General Rod J. Rosenstein - Assistant Attorney General John Demers - FBI Director, Christopher Wray - Director of Defense Criminal Investigative Service of DoD, Dermot T. O'Reilly	OCH1, OCH2, OCH3, OCH4, OCH10, OCH17, OCH18, OCH19, OCH20, OCH23, OCH24, OCH25	12
Government officials in congressional intelligence or investigative committees	- Chairman of Senate Committee on Intelligence, Mark R. Warner - (Former) NSA Senior Advisor, Rob Joyce	OCH21, OCH22	2
Cybersecurity professionals	- Chief of Cyber Threat Analysis at the Cybersecurity and Infrastructure Security Agency, Rex Booth - Director of Cybersecurity and Infrastructure Security Agency, Christopher Krebs - Incident Response Engagement Lead at DHS, Casey Kahsen	OCH6, OCH7, OCH8, OCH9, OCH11, OCH15	6
Top government officials	- Secretary of State, Michael R. Pompeo - Secretary of Homeland Security Kirstjen Nielsen	OCH5	1
Anonymous government officials or politicians with no direct exposure to cyber incidents	- Anonymous DHS Official - Head of stakeholder engagement at DHS, Bradford Wilkie	OCH12, OCH13, OCH14, OCH16, OCH26	5

- Analysing comprehensibility of claims

Most of the government claims display linguistic and technical clarity. Only one source includes the technical term “living-off-the-land” (OCH15), which refers to a type of technique that hackers use to infiltrate target networks. The nature of statements also imply that they follow syntactic and semantic rules and are also grammatically sound. Hence, no evidence suggests that the claims are incomprehensible.

In conclusion, the discourse analysis of APT10's cyber campaign illustrates that government officials' claims are largely legitimate and comprehensible, but incongruous with evidence in the public indictment. Claims of Chinese companies benefiting from the stolen information are largely unsubstantiated given the absence of charges related to theft of trade secrets in the indictment. In addition, the use of language devices in the statements to condemn China unfairly frames China as the sole villain in cyberspace and may be intended to rally international support to pressure China into stopping cyberespionage for commercial purposes. Finally, the economic implications of the cyber incident to U.S. companies are undoubtedly present even though the benefit accrued to Chinese companies is ambiguous.

Comparing the case studies, a distinct difference lies in the way government officials portray the cyber operations. China is not clearly presented as the perpetrator in the OPM hack while government officials clearly link APT10 to the Chinese government in the formal indictment. The sensitive nature of the OPM hack as political espionage makes attribution and punishment tricky due to the existence of shared norms of espionage for national security purposes among states.

Additionally, U.S. government claims in both case studies are largely unsubstantiated in view of publicly available evidence. Speculation on the potential use of sensitive OPM information may have sparked fears of worst-case scenarios. Although claims that Chinese competitor firms will leverage sensitive business material stolen by Chinese intelligence agencies are conceivable, the lack of, or the decision not to provide any evidence in the Operation Cloudhopper indictment was glaring.

The impacts on diplomatic relations with China are also minimal in these two cases. In the OPM hack, China was not officially recognised as the perpetrator due to retaliation concerns and its nature of traditional espionage. The hackers

indicted in Operation Cloudhopper are also not apprehended by U.S. authorities due to the lack of a bilateral extradition agreement (Groffman, 2019).

The two cyber incidents also impacted public confidence on the government's ability to protect personal data or critical information, given that the sheer scale of both hacks would have generated substantial public attention through widespread media reporting. However, since there is no known physical injury or death from the loss of data, public confidence in the U.S. government's ability to maintain public safety and social order is not adversely affected.

V. Discussion

The following discussion concludes findings from both chapters on cyber reality and cyber hype. It discusses the extent of hype versus reality in three key areas: a) espionage of commercial data, b) espionage for political purposes, and c) the possibility of espionage converting into destructive attacks. Each topic presents simultaneously the aspects of hype and legitimate threats to provide an objective threat assessment. The last part of the discussion examines how the hype identified in U.S. government discourse regarding Chinese cyber-attacks fits into the larger debate regarding the rise of China and the attendant growing U.S.-China rivalry, and how the U.S. should respond to a stronger and more assertive China.

5.1 Cyber-enabled theft of Commercial data

Theft of commercial data imposes a negative impact on U.S. firms through direct and indirect costs. Direct costs include the loss of IP, which can be appropriated by adversaries to build the same or similar products, resulting in increased competition and lost business (CSIS, 2013). Indirect costs include detection and forensic investigation activities, notification costs, post-breach remediation costs and lost business stemming from system disruption and reputation loss (Ponemon, 2018). Research by various independent and governmental American institutions has also assessed the economic impact of China's espionage of commercial data. The National Bureau of Asian Research estimated in 2017 that the theft of trade secrets to the U.S. economy may reach U.S.$600 billion, complementing a 2015 report by the ODNI that estimated economic espionage by computer hacking at U.S.$400 billion (Blair et al., 2017). Another report by the White House determined malicious cyber activity, which includes theft of proprietary data, IP and sensitive business information to vary between U.S.$57 billion and U.S.$109 billion in 2016 (The Council of Economic Advisers, 2018). The evidence shows that the undeniable impact that Chinese espionage of commercial data impose on U.S. economic prosperity, and by extension national security.

Due to the negative impact borne by U.S. firms from Chinese espionage, claims that the Chinese government "steal and cheat" gained bipartisan recognition across Republicans and Democrats in the U.S. (Beinart, 2019). However, such claims are less legitimate since they do not consider certain types of commercial espionage which the U.S. deems as legitimate. Following revelations regarding the NSA's spying on Brazilian oil giant Petrobas, Former Director of National Intelligence, James R. Clapper, published a statement in 2013 that the U.S. conducts economic espionage for legitimate reasons, one of which includes "providing insight into other countries' economic policy or behaviour which could affect global markets". However, he emphasises that "What we do not do […] is use our foreign intelligence capabilities to steal trade secrets of foreign companies on behalf of – or give intelligence we collect to – U.S. companies to enhance their international competitiveness or increase their bottom line." (Clapper, 2013).

While Clapper's statements forbid espionage on behalf of private firms or to benefit specific firms, they do not preclude spying on private firms to advance the U.S.' economic interests on a broad level. The U.S.' spying on Petrobas is a case in point. Being a huge state-owned oil giant, the U.S. could have exfiltrated intelligence about Petronbas' oil reserves and plans for allocation of oil exploration licenses to assess the impact of such policies on the American oil companies in Brazil. The U.S. also considers spying on international trade negotiators legitimate even though it ultimately benefits the commercial sector (Sanger, 2014). The narrow distinction between permissible commercial espionage i.e. stealing commercial intelligence that benefits the industries' overall competitiveness, and impermissible commercial espionage i.e. stealing commercial intelligence to benefit specific firms, implies that Chinese espionage activities on U.S. firms may be within the orbit of permissible commercial espionage. However, U.S. officials' accusations of Chinese espionage on U.S. firms do not reflect this distinction and assume all Chinese commercial espionage are to benefit specific firms.

More crucially, the 2009 Quadrennial Intelligence Community Review authored by Clapper's office reveals that the U.S. condones stealing proprietary information from foreign firms. The report, which is released by Snowden, anticipates the risk that the U.S.' technological supremacy will be outstripped by foreign multinational corporations, and recommends a strategy titled "Technology Acquisition by All Means", which is hinged on "a multi-pronged, systematic effort to gather open source and *proprietary* information through overt means, *clandestine penetration "through physical and cyber means*) and counterintelligence" (emphasis added). Specifically, one of the ways is to put implants in "hardware and software used by foreign researchers and *manufacturers*" (emphasis added) and conduct cyber operations on "foreign R&D intranet (ODNI, 2009, pp. 12–13). The illustrative example in the report also reveals that the U.S. will use cyberespionage to boost the competitive advantage of U.S. firms. The illustrative example in the report states that the Intelligence Community will "assess whether and how its findings" from cyber operations on foreign research facilities will be "useful to the U.S. industry" (ODNI, p. 13). In this light, the U.S. officials' claim that China violated the 2015 cyber agreement is less sincere since the U.S. intelligence community acknowledges that stealing proprietary information, which includes trade secrets, to benefit U.S. firms is acceptable (Greenwald, 2014).

While the APT10 indictment does not evidence that Chinese companies benefit from the espionage of state hackers, the indictment of APT1 in 2014 explicitly charges PLA officers of theft of trade secrets, supporting the U.S. officials' claims that the Chinese government conducts commercial espionage to benefit Chinese competitor firms. The 2018 Office of U.S. Trade Representative (USTR) Section 301 report provided evidence that the Chinese government provides commercial intelligence through cyber operations to its state-owned enterprises (SOEs) via an official 'request and feedback loop' and exchanges information through 'a classified communication system' (USTR, 2018). However, SOEs are not the main driver of China's economic growth. The

private sector contributes 60% of China's GDP and is responsible for 70% of innovation (Guluzade, 2019). The USTR report did not provide evidence that Chinese government hackers also pass on proprietary information to private firms. Therefore, the extent of Chinese firms benefiting from coordinated and government-backed cyber-enabled commercial espionage may be more limited than what U.S. government officials perceive.

Much of the theft of IP is also conducted by Chinese citizens and entities, who are emboldened by the cloak of anonymity and difficulty of attribution in cyberspace (Libicki, 2009) to advance personal financial motives (Blair et al., 2013). The attribution problem, however, has become less pertinent due to increased public indictments of Chinese hackers by the U.S.. China's enforcement of IP rights still remains relatively weak due to powerful local interests despite recent improvements in judicial law to reduce IP theft (Blair et al., 2019). Some Chinese companies are also victims of hacking by their local competitors. The number of cases in which Chinese companies sue each other over patents exceeds any other country (Schumpeter, 2019). The permissive legal environment thus allows many private companies to conduct cyberespionage for their own commercial interests with relative impunity without the Chinese government's direct involvement.

Second, cyberespionage only constitutes one method among China's panoply of technology acquisition tools. There are various vectors through which China directly or indirectly provides support to companies to acquire U.S. technology. While many collection methods are covert, some methods occur under the legal framework of joint ventures, foreign direct investments and venture capital investments (O'Connor, 2019). To reach aggressive commercial goals, U.S. companies often willingly enter into legally negotiated joint venture arrangements that circumvent investment restrictions (Roach, 2018). They agree to transfer advanced technology and know-how in exchange for the Chinese partner firm's existing distribution network and dominant market position (Morgan & Bockius, 2008). The study conducted by the National

Bureau of Economic Research in 2018 confirmed that joint ventures are a very effective means of facilitating transfer of the most technologically advanced products or procedures to Chinese partner firms compared to other forms of investment vehicles such as wholly foreign-owned enterprises (Jiang, Keller, Qiu, & Ridley, 2018).

In addition, China's cybersecurity laws raise the risk of security breaches for foreign companies. It mandates foreign companies that are "operators of critical information infrastructure", including technology firms, transport and finance companies to localise the storage of network data. A broad range of companies outside the critical sectors are also subject to security reviews where local authorities can physically inspect or remotely access private networks to assist investigation regarding national security issues or crimes (Zhuang, 2016). They are also required to source their servers, routers and other equipment from Chinese suppliers to comply with data security standards of the Chinese government, which may be fitted with backdoor access (Watts, 2019). Such measures may implicitly force foreign companies to share their IP and source code in order to operate in China. Other non-mandatory cybersecurity guidelines also pressure foreign companies to submit their IP and source code as part of their product review process (Sacks & Li, 2018). Through containing and restricting data flow from the country to ostensibly raise cybersecurity standards, China implicitly gains access to foreign products and technology.

China also uses other non-traditional and traditional forms of covert technology acquisition methods. Non-traditional methods use collectors in legitimate settings to evade suspicion. This includes academic solicitations from researchers in relevant S&T fields of U.S. universities, seeking employment within targeted companies and organising conferences or trade shows to link targeted technologies with relevant experts (Defense Security Service, 2019). In particular, the openness and collaborative nature of university research makes universities easy targets for espionage (Harrell, 2018). Traditional methods commonly constitute physical theft of IP using insider access. A recent

indictment in October 2018 revealed that an MSS director targeted a U.S. aircraft engine supplier by soliciting one of its employees to give a presentation on its key technology under the cover of a S&T association (Department of Justice, 2018a). In another case, a Chinese company set up by the Chinese government employed insiders in the target firm – Micron Memory Taiwan Co., Ltd – to steal a critical semiconductor technology known as dynamic random-access memory (Department of Justice, 2018b).

Unlike previous indictments related to cyberespionage, these individuals involved in physical espionage were explicitly linked to the Chinese government and charged with theft of trade secrets and economic espionage. Even though technological advancement has added the cyber paradigm to espionage, the human factor plays a crucial role in acquisition of technology and remains a core threat vector in Chinese theft of IP. The most successful cases of cyberespionage combine human elements of bribed employees, physical intrusion and wire-tapping, among others (Gorton, 2013). The variety of traditional and non-traditional collection vectors implies that the Chinese government does not necessarily need to rely on cyberespionage to gather U.S. technology in order to pass them to Chinese firms. In fact, the requirement to process voluminous data in cyberespionage may present a more cumbersome method to gather IP compared to physical espionage or legal means of acquiring technology.

In sum, U.S. officials have exaggerated the benefits or competitive advantage that Chinese firms gain through cyberespionage. Not only is the line between espionage for national security purposes and commercial benefit ambiguous, private firms and intelligence officers also engage in rampant theft of trade secrets independent of the government given the weak law enforcement climate. Court indictments of Chinese hackers for stealing commercial data do not always reflect charges surrounding the theft of trade secrets, showing that there is little publicly available evidence to prove that discrete Chinese companies benefit from cyberespionage. Cyberespionage of trade secrets is a threat to the

U.S. but it forms a small piece of puzzle in the larger Chinese mechanism for stealing IP. The threat also lies in the widespread use of traditional and non-traditional human collectors, legal investment vehicles in conjunction with an ecosystem of weak enforcement of laws and biased investment and cybersecurity policies.

5.2 Destructive Cyber-attacks

The cyber-attacks by APT10 on MSPs point to a larger trend on the increasing threat Chinese hackers pose to the global supply chain. A group of Chinese-speaking individuals hacked software supply chains of at least six companies including computer maker Asus and computer clean up tool CCleaner over the past three years (Greenberg, 2019). As argued by (Fazzini, 2019), Lieberthal & Singer (2012) and Lindsay (2015), attacks on global supply chain can cause disruption and destruction of critical infrastructure. The cyber incident dataset shows that China currently conducts espionage operations on a wide range of U.S. critical infrastructure ranging from dams, satellites and aerospace industries. Similarly, U.S. intelligence officials have warned of rising Chinese cyber-attacks targeting critical infrastructure including energy, financial, transportation and healthcare sectors (Finkle & Bing, 2018). The latest Worldwide Threat Assessment of the U.S. Intelligence Community notes that China has developed the capability to inflict "localised, temporary disruptive effects on critical infrastructure" in the U.S. (Coats, 2019). Given the inherent uncertainty and unpredictable consequences in cyberspace (Kello, 2017), there is a likelihood of escalation such that these espionage incidents may one day be converted to actual destructive attacks (Bejtlich, 2013).

However, the cyber incidents dataset clearly shows that China has not conducted any destructive cyber incident thus far. These findings concur with Valeriano et al.'s (2018) argument that China's actions in cyberspace are stable and predictable, involving cyberespionage to gain valuable information. It also complements Laskai and Segal (2018) and Lindsay et al.'s (2015) assertion that

China favours the long-term approach of gradually altering the balance of power by conducting economic and military espionage as opposed to launching short-term disruptive attacks. Moreover, China's capability to impose disruptions or destructions to critical infrastructure does not imply an intention to do so. Its overall strategic guidelines of "active defence" indicates that its mission in cyberspace is defensive and non-destructive. Its primary principle is to attack only when provoked, and to develop sufficiently strong defence capabilities to survive and counter an offensive cyber-attack on its critical information infrastructure (Lyu, 2019). Factors such as economic interdependence between states, nuclear deterrence, and the role of democracy have reduced the use of military power by states. These factors are consistent with the shift from cyber war to low-intensity conflicts below the threshold of an armed attack (Demchak, 2012; Blank, 2017). In the same vein, being a weaker military power relative to the U.S., China prefers to advance its interests via economic, geopolitical and informational methods (Mazarr, 2019). Cyberspace is just one of the platforms in which China seeks to accrue these economic, geopolitical, and informational advantages.

Nevertheless, China's espionage operations may escalate into destructive attacks should its core national security interests such as the independence of Taiwan and territorial claims on the South China Sea be seriously threatened. The cyber incident dataset shows that China has already launched tactical disruptive attacks against the U.S., one of which was against a U.S. aircraft carrier with visiting foreign officials before the international tribunal ruling on its claims to the South China Sea. Apart from the U.S., China has also launched a series of cyber-attacks on the contesting claimants of the South China Sea, such as Vietnam and Philippines, amidst heightened tensions to gain strategic information edge over its rivals (Piiparinen, 2015). A small incident in the South China Sea can escalate into a serious crisis if miscommunication occurs. In such an event, China could also use cyber-attacks to inflict destructive effects by crippling its adversary's military communication networks. However, past

crises in the South China Sea have demonstrated U.S.' hesitance to engage in a direct conflict with China. For instance, when China seized control of the Scarborough Shoal from the Philippines in 2012, the U.S. declined to assist the Philippines by sending military backup to the disputed waters. Hence, in the current climate of peace, China is unlikely to launch destructive cyber-attacks and is likely to continue to accrue its information advantage via economic, political and military espionage.

5.3 Cyber-enabled Political Espionage

Political espionage is common in Chinese cyber-attacks. The OPM hack case study represents just one episode behind the larger backdrop of Chinese espionage operations to obtain personal data of American citizens. The cyber incident dataset reveals other hacks from Community Health Systems, United States Postal Office, Anthem, United Airlines and Marriott hotel to siphon large troves of PII. Should China piece the disparate datasets together, a comprehensive dataset involving an individual's background information, detailed personal information and travel records can effectively be constructed for targeting purposes, imposing intelligence and counterintelligence impacts on the U.S. (Leyden, 2015). Other possible uses of the data include tracking population trends, inferring interpersonal connections among individuals and countering Chinese spies serving America (Newman, 2018). Nevertheless, whether China will be able to fully exploit the potential of the immense dataset to fuel hostile objectives toward the U.S. depends on the extent of development of their machine learning capabilities. Cyber-enabled political espionage does pose a threat to the U.S., but its dangers are not unlike the classic threat of traditional espionage.

As noted by Lindsay (2015), the U.S. is not only a victim but also a perpetrator in conducting cyber-attacks. The Snowden revelations in 2013, Shadow Brokers dump of NSA's exploits and hacking tools in 2016 and the subsequent Wikileaks on the CIA's hacking weapons have proven that the US possesses a

large variety of offensive cyber capabilities (Appelbaum et al., 2013; Cox, 2016; Wikileaks, 2017). A report also revealed that the U.S. is the largest buyer of zero-day exploits i.e. software vulnerabilities (Menn, 2013), and it once paid U.S.$1 million for a zero-day exploit in an iPhone to investigate a shooter in a massacre (Gilbert, 2017). Notably, the documents released by the Shadow Brokers, a hacker group, revealed that the NSA attacked large technology firms such as Cisco, Juniper Networks and Huawei, which provide software and hardware solutions to commercial and corporate customers globally (Cox, 2017). According to Kaspersky Lab, the Moscow-based security software maker, the NSA also obtained the source codes of hard drives produced by Western Digital Corp, Seagate Technology Plc, Toshiba Corp, IBM, Micron Technology Inc and Samsung Electronics Co Ltd, among others (Menn, 2015).

The hacking of such software and hardware supply chain firms mirrors APT10's targets of MSPs and helps the NSA extend its already expansive global surveillance reach. The NSA reportedly automated the deployment of implants in computers globally using a hacking architecture named TURBINE (National Security Agency, 2009). Top-secret documents released by Snowden also revealed the NSA's partnership with telecommunication companies to place secret servers at chokepoints of the Internet backbone, including the United Kingdom and Japan, to serve malicious exploits in the victims' computers. An estimated 85,000 to 100,000 implants were already deployed in 2014, suggesting that this number is even higher at the time of this research (Gallagher and Greenwald, 2014).

The large cyber arsenal and rampant cyber-attacks conducted by the U.S. and China confirms the prevalence of militarisation of cyberspace (Dunn Cavelty, 2012) and supports the argument that there is an offensive advantage in cyberspace (Buchanan, 2017; Kello, 2017). This offensive climate is exacerbated by the uncertainty and ambiguity between offence and defence in cyberspace (Kello, 2017). As described in the Fourth Party Collection operation, the U.S. converted cyber defences against Chinese cyber-attacks into attack

vectors to conduct counterintelligence. A recent report also disclosed that Chinese intelligence officers acquired the NSA's hacking tools during an attack on their own computers (Perlroth, Sanger, & Shane, 2019). However, contrasting what Buchanan (2017) and Kello (2017) assert, offensive cyber-attacks are not necessarily escalating or destabilising since the dataset shows that U.S. and Chinese cyber-attacks are confined to espionage. Espionage activities can help to build confidence between cyber powers by increasing knowledge about the adversary's motivations and capabilities. They also increase predictability and stability among both powers by preventing unnecessary escalation arising from rash decisions (Fickling, 2019).

Huawei – The Emblem of U.S. Fears of Political Espionage

While the OPM case study shows that government officials were reticent in attributing blame to China for cyber incidents involving political espionage (Walker, 2015), the same reticence is not reflected in the ongoing Huawei saga as officials were very direct in blaming Huawei for cooperating with its government to conduct global espionage. The U.S. Secretary of State, Mike Pompeo, and U.S. Vice President, Mike Pence have warned that using Huawei's equipment will cause networks to be susceptible to Chinese espionage through backdoors installed in their networking equipment (Doffman, 2019). Two Chinese laws also sparked concerns among foreign governments regarding the security of data. The 2017 National Intelligence Law states that any "organisation or citizen", including Huawei, will "support, assist, and cooperate with state intelligence work in accordance with the law". The 2014 Counter-espionage law also asserts that organisations and individuals "may not refuse" such a request (Kharpal, 2019). In addition to legislative requirements, Huawei's organisational structure and its founder's former roles with the PLA further raised security concerns about using Huawei's equipment among U.S. government officials (BBC, 2019).

Although these concerns are valid, the recent U.S. indictment against Huawei did not reveal espionage charges that Huawei uses its network equipment to spy on Internet traffic. The first charge alleged Huawei's illicit business dealings with Iran while the second charge relates to theft of technology from U.S. phone company T-mobile, a civil case that had been settled in 2014 (BBC, 2019). Confidentiality or other unexplainable reasons may have prevented U.S. government from publicising concrete evidence to prove Huawei's cooperation with the government. However, the weak evidence presented against Huawei in the indictment only makes U.S. government officials' assertions less credible.

Furthermore, the Chinese intelligence law is also not especially unique. The U.S. government has laws in place which can compel local companies to surrender their data or install backdoors in their products. It was revealed that the U.S. Foreign Intelligence Surveillance Court has approved over 99 per cent of all surveillance requests. Non-compliance with court order to hand over data results in severe fines of U.S.$250,000 per day, as seen in the Yahoo case (Whittaker, 2014). However, the U.S. judiciary system is more transparent and allows for contestation, contrasting the authoritative and opaque judicial system in China.

The U.S. also inappropriately hypes national security concerns surrounding Huawei by conflating them with trade goals. As part of the ongoing trade war between China and the U.S., President Trump had issued an executive order to prohibit transactions related to acquiring information and communications technology or services from any party that is considered a national security threat (The White House, 2019). On the same day, the U.S. Department of Commerce added Huawei and its affiliates to the "Entity List", which is the blacklist of companies that require the government's approval before they can procure products from U.S. companies (Bureau of Industry and Security, 2019). Both moves were essentially directed at Huawei by hampering its access to U.S. components and software essential for its production of smartphones and laptop. Google, Intel, Qualcomm and ARM have complied with the order to stop key technology required to manufacture Huawei's products (Naughton, 2019).

Excluding Huawei from the Western 5G networks may be a pragmatic argument since there are valid U.S. national security concerns regarding assigning the production of a critical technology to a foreign power. However, banning the sales of software or hardware to Huawei for manufacturing exported products outside of the U.S. neither addresses U.S. national security concerns and nor the core structural issues in China that lie at the heart of the current trade war. These actions appear to be an attempt to constrain the Chinese technology giant. The ban also has negligible impact on the usage of Huawei's products in the U.S. since President Trump's ban of its government use of Huawei components in 2018 (Kastrenakes, 2018).

The trade sanctions on Huawei was subsequent relaxed at the end of June 2019. While Huawei remains on the "Entity List", more licenses will be granted to allow trade of "general merchandise" such as computer chips and software (Marks, 2019). The fluctuating stance of the Trump administration indicates that the U.S. may have leveraged Huawei as a bargaining chip in trade talks, effectively undermining its claims regarding the national security threat that Huawei poses.

The U.S.' insistence to put Huawei under the spotlight in its trade dispute with China hints at other underlying motives beyond national security concerns. The U.S. has traditionally been the innovation powerhouse producing top technology giants like Microsoft, Google and Apple. Technological prowess is inextricably linked to economic advantage and military predominance (Roberts, Moraes, & Ferguson, 2019). However, China has been moving aggressively to establish itself at the forefront of technological innovation. Huawei is a major technological challenger and it provides a whole range of products from the global level, i.e. fibre optic lines and undersea cables, network level, i.e. routers, switches and 5G equipment to the personal devices level such as smartwatches (Moriuchi, 2019). According to the 2018 Global Innovation Index report published by distinguished institutions including Cornell University, INSEAD and the World Intellectual Property Organisation, China is in the 17th position

out of 126 countries. Though the U.S. still ranks much higher than China at the sixth position, China has consistently improved its ranking. It tops the globe in the number of patent filings, scientific publications and researchers, while its research and development expenditures trails closely behind the U.S. (Dutta, Lanvin, & Wunsch-Vincent, 2018). With the rise of a strong competitor, the U.S. has an incentive to protect its technological supremacy that possesses major security and economic implications.

5.4 The Wider Implications on U.S.-China Relations

Overall, the prolonged trade war, that has begun since the start of 2018 (Pramuk & Schoen, 2019), seems to confirm Allison's (2017) warning about the Thucydides' trap i.e. the inevitability of a conflict between an incumbent and a rising power. However, the U.S.-China rivalry does not have to be conflictual as predicted by realists like Mearsheimer (2001) and Goldstein (2013). China shares U.S. concern of the theft of IP as it hurts indigenous innovation. China also bears the imperative to innovate and move their economy up the value chain due to economic vulnerabilities such as slowing economic growth, weak credit growth and weak domestic consumption. Although the economy benefits in the short run, firms will be disincentivised to innovate in the long run since they are unable to gain exceptional returns that cover their sunk costs from research and development. Moreover, like U.S. companies, innovative Chinese companies also suffer from the prevalence of IP theft and have called for better legal enforcement regime (Brant, 2019). In a recent article, President Xi Jinping acknowledged that China's "lack of strength in innovation ability" is the "Archilles heel" of the Chinese economy (Blanchard & Perry, 2019). In addition, the U.S. should recognise improvements made in China's protection of IP rights. According to the Guangdong Provincial Higher People's Court, the courts in Guangdong handled 41% more IP cases involving foreign interests in 2018 compared to the previous year (Yan, 2019). China also prosecuted 8,325 people in 2018 for offences including infringement of patent and trademark rights and trade secrets – an increase by 16.3 per cent from the previous year (Xie, 2019).

These improvements, albeit minor, address a key source of tension between China and the U.S. to protect IP.

Cooperation in technology sectors also benefits both countries. The U.S. and China can share data and expertise on major challenges in the applications of artificial intelligence such as healthcare, weather modelling and tracking the effects of climate change (Hass & Balin, 2019). China and the U.S. need to collaborate to jointly solve the social and economic problems introduced by Artificial Intelligence technology (Li, 2019). Not only is mutual cooperation beneficial, it is also crucial. The trade war is reportedly delaying the deployment of 5G in the U.S. and both countries may not be able to deploy 5G anytime soon without mutual help (Laskai & Sacks, 2018). While the U.S. restricts Chinese investment of U.S. technology firms, the opposite dynamic of U.S. firms such as Google, Intel and Nvidia acquiring Chinese start-ups for their talent and expertise is concurrently occurring. U.S. innovation also relies on the contributions of Chinese R&D, China's efficient manufacturing supply chain access and its large market to generate substantial revenue that covers the costs of continuous R&D. However, a broad decoupling from China will slow down breakthroughs in innovation, decrease the competitiveness of U.S. technology firms and increase the costs to American consumers (Laskai & Sacks, 2018).

The lack of trust between the U.S. and China may exaggerate security concerns and overstate the perceived benefits of cooperation. In the light of the Chinese rising technological dominance through legitimate and illicit means, the U.S. has implemented broad-based protectionist measures to decouple the technology sector from China by banning the use of Chinese telecommunication equipment, expanding export controls and tightening regulations of Chinese investments and joint research (Laskai and Sacks, 2018). In response, China has moved aggressively toward self-sufficiency in crucial core technologies such as AI sensors, computer chips, operating systems and quantum communication equipment to reduce economic dependence on the U.S. (Nathan, 2019). As China improves its self-sufficiency and accelerates its technological progress,

the U.S., being the incumbent power, will increasingly perceive China in zero-sum terms of eroding its economic prosperity and national security.

Domestic politics in both countries may also worsen the antagonistic dynamics between the two countries. The Trump administration's villain rhetoric of China in commercial espionage and the Huawei case is political fodder to popular sentiments among the American public and thus there is a strong political incentive to fuel the anti-China message (Beinart, 2019). Confronted with Democratic opponents in the upcoming elections 2020, the Trump administration is also compelled to be hard on China to prevent any perceived weakness by the American public to deal with an unfair trading partner (Lee, 2019). China's nationalist sentiments may also be fed by the U.S.' protectionist measures which it perceives as attempts to suppress its rise (Fifield, 2018).

In sum, both the realist and liberal perspectives play out in the U.S.-China dynamics. While the U.S. adopts an increasingly aggressive stance toward China, its antagonistic measures are still limited to the trade domain, mirroring liberal scholars' view that economic interdependency reduces the chance for aggressive confrontation between two powers (Ikenberry, 2013; Twomey, 2013). The recent truce established by both nations in the Japan G20 summit to suspend any rise in tariffs and reverse the trade ban on Huawei also highlights the important role that economic independence plays in buffering tense bilateral relations (Bradsher, 2019). China and the U.S. continue to be entangled in "competitive co-existence" (Shambaugh, 2013), where both countries straddle opposing objectives of interdependence and independence to ensure security and economic competitiveness.

VI. Conclusion

This paper seeks to understand the severity of the threat that Chinese cyber-attacks pose to the U.S. and assess whether U.S. government officials' discourse surrounding Chinese cyber-attacks is congruent with the actual threat. Cyber incidents between the U.S. and China were collated from various databases and media reports and coded using a modified version of Valeriano et al.'s (2017) codebook. The study analysed the coded data using a tailored version of Steinberg's (2009) threat assessment framework to meet the study's objectives. The second part of the study examines U.S. government officials' discourse of Chinese cyber-attacks against the observed effects. The OPM hack and Operation Cloudhopper are selected as case studies because they each represent the two main purposes of China's strategic cyberespionage – to gain political-military intelligence and commercial intelligence respectively. They are illustrative, but not necessarily representative, of the broader governmental discourse surrounding Chinese cyberespionage operations. The study collates government statements from official government sources and English-language news media reports, and subsequently codes and analyses the data using a combination of three theories involving Dunn Cavelty's (2008a) threat politics framework, Fairclough's (1994) CDA framework, and Habermas' (1984) Theory of Communication Action. Dunn Cavelty's (2008a) framework drives data collection by defining coding categories, while the latter two theories structure data analysis.

Based on the two-part analysis, I have argued that Chinese cyber-attacks exert economic, diplomatic and social impacts but do not pose an existential threat to U.S. national security. This finding contrasts with U.S. government officials claims that tend to exaggerate the threat and depict Chinese cyber-attacks as an existential threat.

Specifically, Chinese cyber-attacks show a consistent trend of long-term and short-term cyberespionage attacks that leverage information for political,

military and economic gains. These attacks result in first-order impacts, in which large amount of critical information (e.g. weapon system designs, PII and IP) are lost. However, second-order impacts are limited to the U.S. economy, U.S.-China diplomatic relations and U.S. public's confidence without destructive consequences to its public safety or military defences. Given the consistent espionage trend observed from Chinese cyber-attacks, China's cyberespionage on critical infrastructure is unlikely to escalate into destructive cyber-attacks given its preference to exert economic and political power rather than military aggression. However, the U.S. should beware of red-button issues that concerns China's sovereignty i.e. Taiwan's independence and territorial claims on the South China Sea. Any escalatory military actions surrounding these issues may trigger a destructive cyber-attack on the U.S. because China views these issues as existential threats to its survival.

Examining the impacts of China's cyberespionage efforts, China's cyber-enabled political espionage threatens U.S. national security by accruing intelligence and counterintelligence advantages. The OPM hack illustrates that U.S. government officials exaggerated intelligence and counterintelligence impacts by suggesting that Chinese cyber operations impose a mortal danger without providing any public evidence. While intelligence effects were evidenced following the withdrawal of CIA agents from China, no counterintelligence impact has been revealed in the public to date. The U.S.' vacillating stance regarding trade with China, specifically Huawei, also demonstrates that the U.S. may have deliberately hyped national security concerns surrounding cyber-enabled political espionage to achieve trade goals, therefore gaining a competitive edge in the broader technological competition.

While the U.S. officials were restrained in linking the OPM hack to Chinese officials, their direct accusation that Huawei is colluding with the Chinese government to conduct political espionage is insincere given their own culpability in own cyberespionage capabilities and refusal to provide the public with evidence to prove their claims. Evidence of the U.S.' expansive global

cyberespionage capabilities and ability to convert cyber defence mechanisms into attack vectors demonstrates the U.S.' ability to understand and respond to the threats posed by Chinese cyber-attacks. The espionage capability of the U.S. is arguably even greater than China given its Five Eyes intelligence capabilities and cooperation with other like-minded countries (Barkin, 2018). In sum, regarding cyber-enabled political espionage, China poses as much of a national security threat to the U.S. as the U.S. does to China.

This study also shows that China's cyberespionage on IP and other sensitive business information causes economic harm to the U.S. by increasing the competitiveness of Chinese firms. The governmental discourse surrounding Operation Cloudhopper accurately illustrates the economic implications on national security. However, the absence of theft of trade secrets and economic espionage charges in the Operation Cloudhopper indictment does not support U.S. government officials' claims regarding China's culpability in directing the cyber operations to benefit Chinese domestic firms. The charges are also inconsistent with hyperbolic terms describing China as the most aggressive threat actor posing an exceptionally severe threat. Given that the U.S. has found evidence of an official communication platform in which the Chinese government exchanges commercial information with its SOEs, the U.S. may have chosen to adopt the policy of ambiguity and silence to maintain intelligence operations (Efrony, 2019). By choosing not to disclose evidence in the public indictment, the U.S. officials' bold claims appear exaggerated and less credible.

However, the scale of Chinese firms benefiting the government's intelligence may be more limited than what U.S. government officials claimed. Only Chinese SOEs seem to reap the benefits from the government's intelligence operations while no publicly available evidence proves that the Chinese government also provides the same advantage to majority of private firms. Furthermore, private firms are often by personal commercial interests to conduct cyberespionage for acquiring technology from U.S. firms. Nevertheless,

the Chinese government is indirectly involved in commercial espionage by individuals by allowing a permissive legal environment for them to conduct commercial espionage with relative impunity.

Moreover, Chinese cyber-attacks are not the main source of threat behind the theft of IP or sensitive business information from U.S. firms. The larger threat lies in China's creative manipulation of investment and cybersecurity laws, employment of legal investment vehicles, and use of traditional and non-traditional human spies. These elements synchronise to form a coherent strategy that enables a large-scale and effective transfer of technology to China.

The U.S. effort to defend its cyberespionage efforts while condemning that of China by distinguishing between national security and commercial espionage is futile given these two objectives often overlap in a cyberespionage operation. Moreover, U.S. claims asserting China poses an unprecedented threat in stealing technology also holds less credibility when the secret document from the U.S. intelligence agency reveal the same intentions.

This study has provided a realistic appraisal of the threats that Chinese cyber-attacks pose to the U.S. and assessed the actual threats against the U.S. government discourse. The objective appraisal helps the U.S. government focus on the specific areas where they should invest their resources in. By illuminating the hype on the Chinese threat, U.S. and Chinese top policymakers also avoid antagonistic policies that may result in an escalating spiral of conflict. Moreover, the comparison of U.S. government discourse against the actual threats of Chinese cyber-attacks reveals the U.S.' adversarial stance toward China. The U.S. has an incentive to paint China as an exceptional villain because this will encourage other nations to join itself in denouncing and decoupling China from the global economy. By understanding U.S. personal interests in protecting its world hegemonic status, states will have a deeper awareness of the U.S.' frequent conflation of national security interests and trade goals the to make informed decisions regarding China.

Overall, U.S. adversarial stance toward China is counterproductive as it does not mitigate the threats from Chinese cyber-attacks or the larger problems of political and industrial espionage. To counter cyber-enabled political espionage, the U.S. should accelerate efforts to strengthen cybersecurity defences of its civil and military departments that possess critical information and inculcate its employees with cyber hygiene knowledge. To manage the threat from industrial espionage, the U.S. should exert coordinated and consistent pressure on China by creating enduring coalitions with international partners to condemn China's coercive intelligence laws and cybersecurity laws and synchronise export controls and investment review mechanisms of critical or dual-use technologies to China. While doing so, the U.S. should avoid containing China's opportunity to participate in the world economy, which will damage its international reputation and undermine the economic interests of all nations.

Finally, this paper will conclude by addressing any limitations and proposing recommendations for further studies. By using open-source data, this study fails to capture a complete picture of cyber incidents between China and the U.S. Government officials' statements extracted from media websites or unclassified government sources inherently present biased views and incomplete truths since they exclude sensitive details to suit public consumption. The sources used are also predominantly Western since Chinese news media's reporting on cyber incidents involving U.S. firms are superficial given their own culpability. Cyber incidents involving Chinese firms are also rare due to the fear of responsibility of the security lapse and weaker detection and attribution cybersecurity capabilities.

Despite using Habermas' validity claims to structure the analysis, my inherent subjective mental models may still introduce biases into the results due to the interpretative nature of CDA. Rhetorical devices may indicate the sincerity of government officials' claims, but such use of rhetorical devices does not impute a deliberate effort by the U.S. officials to deceive. Evidence regarding the second-order impacts of the cyber incidents may not be readily available since

not all impacts are visible or quantifiable. Hence, judgement involved in the coding process may affect the reliability of the data. Ascertaining complete government responsibility is also difficult since state and criminal motives often overlap and are increasingly indistinguishable. Time constraint and the level of detail required to assess language of the texts limits this study to two representative samples for analysing cyber hype. Future research may expand the scope of this study by using quantitative content analysis software to assess a larger corpus of government texts from a greater number of cyber incidents.

This study has also demonstrated how the cyber situational awareness framework integrates political, social and some technical elements to analyse the cyber-attacks. Going forward, such an integrative model should be used for a multidisciplinary assessment of cyber-attacks. The impact factors in the coding template can be updated to incorporate changing trends in cyber-attacks or examine the cyber threat of other U.S. adversaries such as Russia or Iran. The study can also serve as a foundation for future collaboration with cybersecurity professionals for deeper technical analysis. The technical analysis may encompass research of China's capabilities and cyber-attack infrastructure to better understand the threat it poses and a technical evaluation of U.S. cyber defences, which will address the opportunity element in Little & Rogova's (2008) threat function.

VII. Appendices

Appendix 1 – List of Technical Terms and Definitions

Cyber-attack Process: Comprises pre-attack, attack and post-attack phases. The pre-attack phase consists of reconnaissance and scanning activities to identify potential targets and scan for vulnerabilities in people, processes and technologies. The attack phase occurs when the identified vulnerabilities are exploited. The attacker gains access and escalates privileges for complete control to ex-filtrate data or spread malware to degrade, disrupt or destroy the system. After the attack, malware is installed to maintain future access to the system. The attacker would also obfuscate the attack to make attribution and forensic examination difficult.

Phishing: Technique used in a cyber-attack that deceives the target into installing malware or accessing malicious websites through sending fraudulent emails from a seemingly legitimate source. Targets large numbers of people simultaneously.

Spear-phishing: Technique is the same as phishing, except that spear-phishing personalises attacks to specific targets

Worms and Viruses: Malware that compromise regular functionalities by corrupting or deleting data. However, unlike worms, viruses attach themselves to programs and self-replicate.

Trojans: Malware that masquerade as legitimate programmes which contains malicious code

Ransomware: Malware that encrypts data until a ransom has been paid off

Rootkits: Malware that grants the attackers total control of the system while evading detection

Bots: Malware that assemble a large malicious network through compromising individual clients

Logic Bomb: Malware that causes a network or system to cease operations, involving elimination of all data

Keystroke Logging: Malware that tracks keys being inputted into the computer and replicate them for infiltration into the network.

Sniffers or beacons: Monitoring techniques that search for specific information and usually inflict no malicious harm.

Man-in-the-Middle Attack: Technique used in a cyber-attack that intercepts cyberspace communication to between two parties to steal or modify data.

Distributed Denial of Service: Technique used in a cyber-attack that compromises the system through loading it with excessive information such that it is unable to perform regular functions.

Structured Query Language (SQL) injection: Technique used in a cyber-attack that targets websites and the accompanying databases to reveal sensitive information including usernames, passwords, personal, and banking information.

Zero-day exploits: Technique used in a cyber-attack that leverage on discovered vulnerabilities with no developed solutions

Cross-site scripting: Technique used in a cyber-attack that attacks legitimate website or web application by running malicious scripts in order to infect targets who visit the compromised website.

Watering Hole: Technique used in a cyber-attack in which attackers target websites that are frequently visited or are trusted by the targets to increase operational success.

Password attacks: Technique used in a cyber-attack that leverages common weak passwords and previously hacked passwords to gain access to targets' systems.

Confidentiality: One of the information goals to maintain the privacy of data.

Integrity: One of the information goals to maintain the non-alteration of data without proper authorisation.

Availability: One of the information goals to maintain the ability to access the system.

Information Operations: Comprises of four tenets – a) psychological operations, b) electronic warfare, c) operations security and d) military deception. (Definition according to US DoD Joint Publication 3-13)

- *Psychological Operations* – Using planned information to influence foreign target audiences, including friendly and adversarial governments, individuals and organisations into subscribing to an agenda by manipulating their emotions, motives, objective reasoning. (Definition according to US DoD Joint Publication 3-13)
- *Electronic Warfare* – Involves attacking the electromagnetic spectrum such as jamming radio communication systems.
- *Operations Security* – Involves identifying and analysing critical information to ensure the functioning of military operations
- *Military Deception* – Related to psychological operations, but focuses on disinformation, but only applies to adversarial military, paramilitary or violent organisations.

Cyberspace Operations: Achieve objectives in or through cyberspace by executing cyberspace capabilities.

- Offensive Cyberspace Operations – Intent is to project power in and through cyberspace.
- Defensive Cyberspace Operations – Intent is to defend DoD information networks and other key cyber terrains from malicious cyberspace activity to preserve the freedom of manoeuvre in cyberspace.

US Presidential Policy Directive 21: Critical infrastructure sectors comprise of the chemical sector, commercial facilities sector, communications sector, critical manufacturing sector, dams sector, defense industrial base sector, emergency services sector, energy sector, financial services sector, food and agriculture sector, government facilities sector, healthcare and public health sector, information technology sector; nuclear reactors, materials and waste sector, transportation systems sector, water and wastewater systems sector.

Advanced Persistent Threat: Actors that use sophisticated techniques to intrude a computer system and maintain a persistent presence for a prolonged period of time to create potentially destructive consequences

Living-off-the-land: Technique used in a cyber-attack which leverages pre-existing software in the target systems or run attacks in the memory to evade detection

Appendix 2 – Coding Table

Coding Numbers	0	1	2	3	4
Name of Cyber Incident					
Initiator					
Defender					
Threat Group					
Target					
Discovery Date					
Start Date					
End Date					
Third Party Initiator	No	Yes			
Third Party Target	No	Yes			
Nature of Interaction		Nuisance	Defensive	Offensive	
Type of Target		Private/Non-state	Government non-military	Government military	
Interdependency with CI		Low interdependence	Medium interdependence	High interdependence	
Type of Operation		Disruption	Short-Term Espionage	Long-term Espionage	Degradation
Methods		Vandalism	Denial of Service (DoS) or Distributed denial of service (DDoS)	Intrude and Infiltrate	Hijacking
Operational Success	No	Yes			
Immediacy		Immediate	Delayed		
Directness		Direct	Indirect		
Objective		Tactical – In response to coerce or preparation for political events (Taiwan, SCS, trade talks);	Strategic – Gain intelligence (and counterintelligence) regarding the target's military departments (number of weapons, forces, military plans, military research) and civil departments (resources and finance, personnel, interrelations of individuals and organisations) for national security	Strategic – Gain industrial or commercial intelligence (intellectual property and technology know-how) for national security purposes or to benefit local firms	
Objective Description					
Behavioural change - Whether attack invoked	No	Yes			

Coding Numbers	0	1	2
First Order Effects		**Espionage**	**Disruption and degradation**
Low - 1		System is penetrated but there is no misuse by the initiator e.g. Use of sniffers for reconnaissance or scanning for specific information.	Temporary disruption of a few government or private networks or websites through defacement or DDoS to cause inconvenience but effects are usually reversible.
Medium - 2		Stealing of sensitive information such as policy documents which has no immediate tactical or strategic applications	Temporary and large-scale disruption of government or private networks or websites through defacement or DDoS to cause inconvenience but effects are usually reversible.
High - 3		Stealing of targeted critical information (less than 5 million records or cyber incident lasted less than a year) from the government, economic, military or critical private sector such as military intelligence, weapon system designs, personally identifiable data and intellectual property, that has direct tactical or strategic applications, including planning for future attacks.	Targeted degradation of single or few networks or systems to affect core functionalities through modifying or deleting data and are usually irreversible
Very High - 4		Stealing of vast troves of critical information (more than 5 million records or cyber incident lasted more than a year) from the government, economic, military or critical private sector such as military intelligence, weapon system designs, personally identifiable data and intellectual property that has direct tactical or strategic applications, including planning for future attacks.	Widespread degradation of multiple networks or systems to affect core functionalities through modifying or deleting data and are usually irreversible
Official Government Statement From US			
Official Government Statement From China			
Security Firm Forensics			
Sources			

Coding Numbers	0	1	2	3	4	5	6	7
Second Order Effects		**Economic (US$)**	**Policy implementation and provision of public service**	**Safety**	**Defense**	**Public Order**	**Public Confidence**	**International Relations**
Low - 1		<1mil	Temporary disruption of a few government operations for policy implementation or public service	Minor injuries	N/A	Localised protest	High confidence in government's ability to provide public services, maintain public safety and	Adversely affect diplomatic relations
Medium - 2		1-10mil	Temporary disruption of multiple government operations for policy implementation or public service	Severe injuries, chronic illness	Minor damage to the ability of the state to defend itself from hostile attacks	Demonstratio ns, lobbying	High confidence in government's ability to provide public services, maintain public safety and	Materially damage diplomatic relations
High - 3		10-100mil	Shut down or substantially disrupt a few government operations for policy implementation or public	Severe injuries, chronic illness and potential casualties	Grave damage to the ability of the state to defend itself from hostile attacks	Widespread industrial action	Moderate confidence in government's ability to provide public services, maintain public	Raise international tensions
Very High - 4		> 100mil	Shut down or substantially disrupt multiple government operations for policy	Widespread loss of lives	Grave damage to the ability of the state and allied forces to defend themselves from hostile	Direct threat to internal stability	Low confidence in government's ability to provide public services, maintain	Seriously damage international relations

Appendix 3 – Description of Coding Factors

Nature of Interaction

- Nuisance – Consists of mostly vandalism and denial of service incidents to disrupt daily operations or reconnaissance and scanning activities but are usually reversible and easily removable by the target.
- Defensive operation – Initiator must be responding to a cyber-incident in which it was a target.
- Offensive – Consists of mostly intrusions and infiltrations, in which the initiator attempts to disrupt a specific national strategy or policy of the target or engage in espionage to steal critical information.

Type of Target

- Private/non-state – Mostly consists of critical infrastructure sectors such as communications, energy, transportation and information technology sectors.
- Government non-military – Consist of civil departments, ministries or government websites, such as US State Department and the People's Republic of China (PRC) Ministry of Foreign Affairs.
- Government military – Consists of defence departments such as the US Department of Defence and the PRC Ministry of National Defence.

Type of Operation

- Disruption – Usually consist of low cost and low intensity operations such as vandalism of websites, DDoS attacks
- Short-Term Espionage – Mainly used for tactical purposes to leverage critical information that enables a state to gain an immediate advantage. Time period for short-term espionage is stipulated to be six months or less.
- Long-Term Espionage – Mainly used for strategic purposes to gain a future advantage through leveraging information gathered to enhance its capability and raise credibility in hope to alter the target's decision calculus or foreign policymaking
- Degradation – Usually consist of high intensity operations that aims to inflict physical damage on a target's capabilities

Methods

- Vandalism – Involves the use of Structured Query Language or cross-site scripting to perform website defacements.
- DoS or DDoS – Involves flooding websites, servers or routers with requests exceeding the website's capacity to eventually shut it down and prevent access or usage. Such attacks are usually accomplished with botnets (see Appendix 2 for definition)
- Intrude and infiltrate – Intrusion involves the use of force via "Trapdoors", "Trojans" or "Backdoors" to establish a connection with the target network, hence gaining access. These are unauthorised software introduced to a software program or network which allows future access for the initiator. They are commonly used for stealing of sensitive information directly or via man-in-the-middle attack (see Appendix 1). Spear phishing or manual injection via portable drives are typically used to introduce trapdoors into the target's network. Infiltration infects legitimate processes and forces the target's computers or networks to undertake unauthorised tasks of the initiator via logic bombs, viruses, worms keystroke logging or sniffers (see Appendix 1).
- Hijacking – Involves a network attack in which the attacker takes control of a communication. E.g. man-in-the-middle attack (see Appendix 1)

Operational Success

- Refers to whether the operation – either disruption, short-term espionage, long-term espionage or degradation achieves its intended purposes. E.g. Whether the disruptive operation successfully manages to shut down a website via DDoS.

Immediacy

- Refers to the speed at which the consequence of the cyber operation manifests itself.

Directness

- Examines the chain of causation of a cyber operation and whether its effects are originally intended by the initiator.

(Inter)dependency with other critical infrastructure

- Dependence exists when the state of one service or infrastructure influences or is correlated to another. Interdependency is bidirectional, in which each service or infrastructure is correlated or influences the other.
- Level of interdependency relates to the degree that a cyber operation would result in a cascading, escalating or common cause failure on other cross-border and/or cross-sector infrastructure or service due to physical, cyber, geographic and/or logical dependencies.
- Low (inter)dependence – State of operations is disconnected to any network, but logical dependencies (due to human decisions or actions) may exist. For example, a cyber operation on one infrastructure may result in demand for its services to shift to another infrastructure that provides similar services.
- Medium (inter)dependence – State of operations is connected to a localised network, indicating cyber dependency. Geographic dependency by other infrastructure in close spatial proximity may exist but no physical dependency by other infrastructure.
- High (inter)dependence – State of operations is connected to a network, indicating cyber dependency and the material output of the infrastructure or service is depended on by other cross-border or cross-sector infrastructure (physical dependency).

Objective

- Cyber attackers conduct cyber operations for tactical and strategic purposes.
- Tactical cyber-attacks are in response to external events that are deemed detrimental to the initiator's interests.
- Strategic cyber-attacks consist of two variations:
    - To gain intelligence or counterintelligence regarding the target's military and government.
    - To loot steal technology and trade secrets to benefit its private firms and state-owned enterprises.

Behavioural change

- Refers to whether the target changed its foreign policy or make any type of concessions in response to the cyber incident. E.g. Trade concessions, dropping of indictment charges, change in processes or procedures, change in foreign policy

First order effects

- First order effects manifest online and consist of two variants – espionage and disruption.
- Espionage – Mainly concerns data theft in which confidentiality of data is compromised even though it is still in the possession of the target. Espionage could also appear to be benign in which access is to the secured network is obtained but no further action is taken.
- Disruption and degradation – Range from temporary DDoS attacks or defacement of websites, which cause disruption of daily services, to more serious harm of modifying and destroying data which damages the core functionality of the system.

Second Order Effects

- Second order effects usually result from online effects to impact on economic, psychological, social, physical, national security or foreign relation aspects.
- Economic – Refers to economic impact of a cyber incident. It includes losses due to degradation of the network or system itself, loss of assets or information, costs of recovery, investment in cybersecurity and == estimated loss due to cascading impacts and any cascading impact on other critical infrastructure
- Policy implementation and provision of public service – Refers to the ability of the government to function and operate by implementing its policies and providing public services.
- Safety – Refers to the physical wellbeing of individuals including illnesses, injuries and loss of lives
- Defence – Refers to the ability of the government to protect its population from malicious attacks of stealing of critical information or degradation of critical infrastructure. There is no low impact category due to the nature of this impact.
- Public Order – Refers to the impact on social stability after a cyber incident. The impact may arise from disclosure of confidential information of the public or the unavailability of a critical public service.
- Public Confidence – Refers to the perception by the public of the government's ability to protect data, provide public services, maintain public safety and social order.
- International Relations – Refers to impact on diplomatic relationships, including demonstrations against the initiating state, expulsion of diplomats of the initiating state, severance of trade relations with the initiating state or imposition of trade sanctions on the initiating state.

Appendix 4 – Privacy Notice for Retention and sharing of PGT Dissertation

Privacy Notice for Retention and sharing of PGT Dissertation

Your Personal Data

The University of Glasgow will be what's known as the 'Data Controller' of your personal data processed in relation to retention and sharing of PGT Dissertations. This privacy notice will explain how The University of Glasgow will process your personal data.

Why we need it

We are collecting your basic personal data such as name, email address/contact details in order to retain and share your PGT Dissertation with future students. We will only collect data that we need in order to provide and oversee this service to you.

Legal basis for processing your data

We must have a legal basis for processing all personal data. In this instance, the legal basis is 'Consent' (Article 6(1)(a) of the GDPR.

What we do with it and who we share it with

- All the personal data you submit is processed by staff at the University of Glasgow in the United Kingdom

How long do we keep it for

Your data will be retained by the University for five years. After this time, data will be securely deleted.

What are your rights?*

You can request access to the information we process about you at any time. If at any point you believe that the information we process relating to you is incorrect, you can request to see this information and may in some instances request to have it restricted, corrected or, erased. You may also have the right to object to the processing of data and the right to data portability.

Where we have relied upon your consent to process your data, you also have the right to withdraw your consent at any time.

If you wish to exercise any of these rights, please contact dp@gla.ac.uk.

*Please note that the ability to exercise these rights will vary and depend on the legal basis on which the processing is being carried out.

Complaints

If you wish to raise a complaint on how we have handled your personal data, you can contact the University Data Protection Officer who will investigate the matter.

Our Data Protection Officer can be contacted at dataprotectionofficer@glasgow.ac.uk

If you are not satisfied with our response or believe we are not processing your personal data in accordance with the law, you can complain to the Information Commissioner's Office (ICO) https://ico.org.uk/

Contact Details

If you have any questions relating to this consent form or the way we are planning to use your information please contact **socpol-schoolprogram-pgadmin@glasgow.ac.uk**

Permission to use student assessments in teaching future PGT students:

Academic staff are often asked by PGT students if they have examples of previously assessed student work that they may share with them. We would be grateful if you would consider giving permission for your academic work to be used in this way in future PGT teaching.

Your written dissertation work	**Please initial if you give permission for this to be used in future teaching**
1. Dissertation project (paper copy available for borrowing by staff and students and/or electronic copy saved to Enlighten)	KLT

I hereby give my consent for my assessments to be used in the ways that I have indicated above and in line with the attached Privacy Notice.

Name: Kai Lin Tay

Student id no.: 2337200T

Signature:

Date: 24 July 2019

Appendix 5 – Sources of Government Claims for the OPM hack

Statement No.	Source	Type
OPM1 to OPM4	Nakashima, E. (2015, June 12). Chinese hack of federal personnel files included security-clearance database. *The Washington Post*. Retrieved July 25, 2019, from https://www.washingtonpost.com/world/national-security/chinese-hack-of-government-network-compromises-security-clearance-files/2015/06/12/9f91f146-1135-11e5-9726-49d6fa26a8c6_story.html?noredirect=on&utm_term=.43fe3f42753b	News Media
OPM5 to OPM9	Nakashima, E. (2015, June 5). With a series of major hacks, China builds a database on Americans. *The Washington Post*. Retrieved July 25, 2019, from https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html?utm_term=.42ca47387df6	News Media
OPM10 to OPM16	U.S. House, Committee on Oversight and Government Reform. (2016, September 7). *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*(J. Chaffetz, M. Meadows, & W. Hurd, Authors) [H.R. Rept. Majority Staff Report from 114 Cong.]. Retrieved July 25, 2019, from https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf	Government source
OPM17 and OPM18	Geraghty, J. (2017, October 10). 'The OPM Hack Was Just the Start and It Won't Be the Last.' Retrieved July 25, 2019, from https://www.nationalreview.com/corner/opm-hack-was-just-start-and-it-wont-be-last-jim-geraghty/	Online Journal

OPM19	The White House, Office of the Press Secretary. (2015, June 8). *Remarks by President Obama in Press Conference after G7 Summit* [Press release]. Retrieved July 25, 2019, from https://obamawhitehouse.archives.gov/the-press-office/2015/06/08/remarks-president-obama-press-conference-after-g7-summit	Government source
OPM20, OPM21	Sanger, D. E., & Davis, J. H. (2015, June 10). Hackers May Have Obtained Names of Chinese With Ties to U.S. Government. *The New York Times*. Retrieved July 25, 2019, from https://www.nytimes.com/2015/06/11/world/asia/hackers-may-have-obtained-names-of-chinese-with-ties-to-us-government.html	News Media
OPM22 to OPM25	Liptak, K., Schleifer, T., & Sciutto, J. (2015, June 6). China might be building vast database of federal worker info, experts say. *CNN*. Retrieved July 25, 2019, from https://edition.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management/	News Media
OPM26	Welna, D. (2015, July 2). In Data Breach, Reluctance To Point The Finger At China. *National Public Radio*. Retrieved July 25, 2019, from https://www.npr.org/sections/parallels/2015/07/02/419458637/in-data-breach-reluctance-to-point-the-finger-at-china	News Media
OPM27 to OPM30	Levin, M. (2015, June 25). China Is 'Leading Suspect' in Massive Hack of US Government Networks. *ABC News*. Retrieved July 25, 2019, from https://abcnews.go.com/US/china-leading-suspect-massive-hack-us-government-networks/story?id=32036222	News Media
OPM31 to OPM37	Nakashima, E. (2015, July 9). Hacks of OPM database compromised 22.1 million people, federal authorities say. *The Washington Post*. Retrieved July 25, 2019, from https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.52f99013d763	News Media
OPM38	Smith, I. (2018, September 21). Bolton Confirms China was Behind OPM Data Breaches. Retrieved July 25, 2019, from https://www.fedsmith.com/2018/09/21/bolton-confirms-china-behind-opm-data-breaches/	Online Journal

OPM39	Koerner, B. I. (2016, October 23). Inside the Cyberattack That Shocked the US Government. Retrieved July 25, 2019, from https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/	Online Journal
OPM40	Congressman Jim Langevin. (2015, June 16). *Langevin Floor Statement on OPM Data Breach*[Press release]. Retrieved July 25, 2019, from https://langevin.house.gov/press-release/langevin-floor-statement-opm-data-breach	Government source
OPM41 to OPM44	U.S. House, Committee on the Oversight and Government Reform. (2015, June 24). *OPM: Data Breach Part II* (C. Jason, K. Archuleta, A. Barron-DiCamillo, R. Giannetta, E. A. Hess, P. E. McFarland, et al., Authors) [H.R. Rept. 81 from 114 Cong., 1 sess.]. Retrieved July 25, 2019, from Hearing: Full Committee Hearing, https://www.hsdl.org/?view&did=792216	Government source
OPM45, OPM47 to OPM54	U.S. House, Committee on Oversight and Government Reform. (2015, June 16). *OPM: Data Breach* (C. Jason, W. Hurd, R. Kelly, K. Archuleta, D. K. Seymour, A. Ozment, et al., Authors) [H.R. Rept. from 114 Cong., 1 sess.]. Retrieved July 25, 2019, from https://www.hsdl.org/?abstract&did=793071	Government source
OPM55 and OPM56	U.S. Senate, Committee on Homeland Security and Governmental Affairs,. (2015, June 25). *Under Attack, Federal Cybersecurity and the OPM Data Breach*(R. Johnson, J. McCain, T. R. Carper, J. Tester, C. A. Booker, J. Ernst, et al., Authors) [S. Rept. from 114 Cong., 449 sess.]. Retrieved July 25, 2019, from https://www.hsdl.org/?abstract&did=793785	Government source
OPM57	U.S.Cong., Committee on Oversight and Government Reform. (2016, November 16). *Federal Cybersecurity After the OPM Data Breach: Have Agencies Learned Their Lesson?*(R. P. Wynn, J. Alboum, & R. Klopp, Authors) [Cong. Rept. 125 from 114 Cong.]. Retrieved July 25, 2019, from https://www.hsdl.org/?view&did=801099	Government source

OPM58 to OPM61	U.S. House, Committee on Science, Space, and Technology (2011). (2015, July 8). *Is the OPM Data Breach the Tip of the Iceberg?*(B. Comstock, D. Lipinski, B. Loudermilk, D. S. Beyer, L. S. Smith, M. R. Esser, et al., Authors) [H.R. Rept. 28 from 114 Cong., 1st sess.]. Retrieved July 25, 2019, from https://www.hsdl.org/?view&did=791143	Government source
OPM62	Sasse, B. (2018, March 07). Senator Sasse: The OPM Hack May Have Given China a Spy Recruiting Database. Retrieved July 25, 2019, from https://www.wired.com/2015/07/senator-sasse-washington-still-isnt-taking-opm-breach-seriously/	Online Journal
OPM63 and OPM64	U.S. Senate, Committee on Armed Services,. (2015, September 29). *United States Cybersecurity Policy and Threats*(J. R. Clapper, R. Work, & M. S. Rogers, Authors) [S. Rept. 398 from 114 Cong., 1st sess.]. Retrieved July 25, 2019, from https://www.hsdl.org/?view&did=792559	Government source
OPM65	Nakashima, E. (2015, June 4). Chinese breach data of 4 million federal workers. *The Washington Post*. Retrieved July 25, 2019, from https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html?utm_term=.e547831ece72	News Media
OPM66 and OPM67	Rushe, D. (2015, June 5). OPM hack: China blamed for massive breach of US government data. *The Guardian*. Retrieved July 25, 2019, from https://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances	News Media
OPM46, OPM68 and OPM69	Nakashima, E. (2015, July 21). US decides against publicly blaming China for data hack. *The Washington Post*. Retrieved July 25, 2019, from https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html?utm_term=.4dff579daa6a	News Media

Appendix 6 – Sources for Government Claims of Operation Cloudhopper

Statement No.	Source	Type
OCH1 to OCH3	U.S. Department of Justice. (2018, December 20). *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information* [Press release]. Retrieved July 25, 2019, from https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion	Government source
OCH4	U.S. Department of Justice. (2018, December 20). *Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers* [Press release]. Retrieved July 25, 2019, from https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-announces-charges-against-chinese-hackers	Government source
OCH5	U.S. Department of State. (2018, December 20). *Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen Nielsen: Chinese Actors Compromise Global Managed Service Providers* [Press release]. Retrieved July 25, 2019, from https://www.state.gov/joint-statement-by-secretary-of-state-michael-r-pompeo-and-secretary-of-homeland-security-kirstjen-nielsen-chinese-actors-compromise-global-managed-service-providers/	Government source
OCH6 to OCH8	Johnson, D. B. (2019, February 6). China-linked hacker group has gone quiet, but DHS expects resurgence. Retrieved from https://fcw.com/articles/2019/02/06/cisa-apt10-china-johnson.aspx	Online Journal
OCH9	Marks, J. (2019, February 12). The Cybersecurity 202: Senate Committee leaders worry no one's in charge on cybersecurity. *The Washington Post*. Retrieved July 25, 2019, from https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/02/12/the-cybersecurity-202-senate-committee-leaders-worry-no-one-s-in-charge-on-cybersecurity/5c61bd741b326b66eb098681/?noredirect=on&utm_term=.0c4ab05ddf92	News Media

OCH10	Federal Bureau of Investigation. (2018, December 20). *FBI Director Christopher Wray's Remarks Regarding Indictment of Chinese Hackers* [Press release]. Retrieved July 25, 2019, from https://www.fbi.gov/news/pressrel/press-releases/fbi-director-christopher-wrays-remarks-regarding-indictment-of-chinese-hackers	Government source
OCH11	Lyngaas, S. (2019, February 06). DHS briefs industry on shift in Chinese hacking that 'increases the risk for all of us'. Retrieved from https://www.cyberscoop.com/chinese-hacking-dhs-cisa-webinar/	Online Journal
OCH12 to OCH16	Lynch, J. (2019, February 07). Department of Homeland Security warns of cyberattacks on third-party companies by China. Retrieved July 25, 2019, from https://www.fifthdomain.com/civilian/dhs/2019/02/07/department-of-homeland-security-warns-of-cyberattacks-on-third-party-companies-by-china/	Online Journal
OCH17	Bing, C., Stubbs, J., & Menn, J. (2019, December 20). Exclusive: China hacked HPE, IBM and then attacked clients - sources. *Reuters*. Retrieved July 25, 2019, from https://www.reuters.com/article/us-china-cyber-hpe-ibm-exclusive/exclusive-china-hacked-hpe-ibm-and-then-attacked-clients-sources-idUSKCN1OJ2OY	News Media
OCH18, OCH19	Lyngaas, S., & Stone, J. (2018, December 21). U.S. indicts China-linked APT10 over rampant hacks of U.S. organizations. Retrieved July 25, 2019, from https://www.cyberscoop.com/apt10-charges-china-hackers-ministry-of-state-security/	Online Journal
OCH20	Uchill, J. (2018, December 20). DOJ indicts 2 Chinese agents for hacking U.S. organizations. Retrieved July 25, 2019, from https://www.axios.com/doj-indicts-chinese-agents-hacking-cloudhopper-20618046-0ec1-4cb6-910d-53752080c9ed.html	Online Journal
OCH21	Wilber, D. Q. (2018, December 20). Chinese hackers charged with stealing data from Navy, JPL and U.S. companies. *Los Angeles Times*. Retrieved July 25, 2019, from https://www.latimes.com/politics/la-na-pol-chinese-espionage-indictment-20181220-story.html	News Media

OCH22 to OCH26	Stubbs, J., Menn, J., & Bing, C. (2019, June 26). Special Report: Inside the West's failed fight against China's 'Cloud Hopper' hackers. *Reuters*. Retrieved July 25, 2019, from https://www.reuters.com/article/us-china-cyber-cloudhopper-special-repor/special-report-inside-the-wests-failed-fight-against-chinas-cloud-hopper-hackers-idUSKCN1TR1DK	News Media

Appendix 7 – U.S.-China Cyber Incidents Database (from 1 Jan 2013 to 31 May 2019)

No.	Name	Initiator	Defender	Third Party Initiator	Third Party Target	Threat Group	Target	Discovery Date	Start Date	End Date	No. of months	Nature of Interaction	Type of Target	Interdependency with oth	Information stolen	Type of Operation	Methods	Operational Success	Immediacy	Directness	Objective	Behaviour Change in Tar	Online effects	Secondary effects	Official Government Statement	Official Government Statement Fro	Security Firm Forensics?
1	Aspen Institute hack	China	US	0	0	APT 1/Comment Crew	Aspen Institute	06-Jan-13	Nov-12	06-Jan-13	2.20	3	1	2	1	2	3	1	2	1	2	0	1.2	-	No	No	FBI
2	NY Times attack	China	US	0	0	APT 12	The emails, computer systems and passwords of NY journalists, including NYT's Shanghai Bureau Chief,	30-Jan-13	13-Sep-12	30-Jan-13	4.63	3	1	2	1	2	3	1	2	1	1	0	1.2	1.1, 7.1	Yes	Yes	Mandiant
3	Operation Beebus	China	US	0	0	APT 1/Comment Crew	US Defense contractors and drone technology	Feb-13	Apr-11	Apr-13	24.37	3	3	2	3	3	3	1	2	1	3	0	1.4	1.4, 7.1	Yes	No	Fireeye
4	Department of Labour hack	China	US	0	1	APT 19/Deep Panda/Black Vine	Department of Labour	01-Mar-13	Apr-13	May-13	0.03	1	2	2	1	2	3	1	2	1	2	0	1.3	-	No	No	Crowdstrike, Cisco
5	US Army Corps of Engineers' National Inventory of Dams	China	US	0	0	-	Corps of Engineers' National Inventory of Dams	01-May-13	Jan-13	01-May-13	4.00	3	2	3	1	2	3	1	2	1	2	0	1.3	1.4, 6.3	No	No	US intelligence agencies
6	US Transcom hack	China	US	0	0	Multiple APT groups	US Transportation Command contractors	Sep-14	01-Jun-12	01-May-13	11.13	3	3	3	1	3	3	1	2	1	2	0	1.4	1.4, 7.1	Yes	Yes	Committee on Armed Services, US Senate Fireeye
7	Arrow Eclipse	US	China	0	0	NSA	Chinese espionage activities	17-Jan-15	01-Jul-09	13-Jun-13	48.10	2	3	3	1	3,4	3	1	1	1	1,2	0	1.4	2.1	Yes	Yes	Snowden
8	Operation Shotgiant	US	China	0	0	NSA	Huawei	Mar-14	03-Oct-10	13-Jun-13	32.80	3	1	3	1	3	3	1	2	1	2,3	0	1.4	1.4, 7.1	Yes	Yes	Snowden
9	Fourth Party collection	US	China	0	1	NSA	Chinese foreign espionage incidents	17-Jan-15	01-Jul-09	13-Jun-13	48.10	3	3	3	1	3,4	3	1	2	1	1,2	0	1.4	2.2, 7.2	Yes	Yes	Snowden
10	Operation Ephemeral Hydra	China	US	0	0	APT 17/Deputy Dog/Axiom/Wicked Panda	US based NGO website	08-Nov-13	Nov-13	Nov-13	0.23	3	2	2	1	2	3	1	2	2	2	0	1.2	-	No	No	Fireeye
11	Operation Snowman	China	US	0	0	APT 17/Deputy Dog/Axiom/Wicked Panda	US Veterans of Foreign Wars (VFW) website	11-Feb-14	01-Feb-14	12-Feb-14	0.37	3	2	2	1	2	3	1	2	1	2	0	1.3	-	No	No	Fireeye
12	Boeing espionage and indictment of Su Bin	China	US	0	0	Chinese PLA	Boeing Company	01-Jun-14	01-Oct-08	31-Mar-14	66.90	3	1	2	1	3	3	1	2	1	3	0	1.4	1.4, 7.2	Yes	No	FBI, indictment
13	Indictment of 5 in China army	China	US	0	0	APT 1/Comment Crew	Westinghouse, SolarWorld, U.S. Steel, ATI, the USW, and Alcoa,	01-May-14	01-Jan-06	30-Apr-14	101.37	3	1	2	1,3	3	3	1	2	1	3	0	1.4	1.4, 7.2	Yes	Yes	DOJ Indictment
14	US and European aerospace and satellite industries hack	China	US	0	1	APT 2/Putter Panda	US defense industries - satellite and aerospace	01-Jan-12	01-Jan-07	01-Jun-14	90.27	3	1,3	3	1,3	3	3	1	2	1	2,3	0	1.4	1.4, 7.1	No	No	Crowdstrike
15	DHS employee hack through USIS	China	US	0	0	-	DHS employees with security clearance	01-Jun-14	01-Apr-13	01-Jun-14	14.20	3	2	2	2	3	3	1	2	1	2	0	1.3	1.4	No	No	FBI
16	Community Health Systems Inc.	China	US	0	0	APT 18/Dynamite Panda	Community Health Systems Inc.	01-Jun-14	01-Apr-14	01-Jun-14	2.03	3	1	2	2,3	2	3	1	2	1	2	0	1.3	1.4, 6.2	No	No	Fireeye, Crowdstrike
17	Major US think tanks on Middle East	China	US	0	0	APT 19/Deep Panda/Black Vine	Middle East experts at major US think tanks	01-Jul-14	18-Jun-14	01-Jul-14	0.43	3	2	2	1	2	3	1	2	1	2	0	1.3	-	No	No	Crowdstrike

No.	Name	Initiator	Defender	Third Party Initiator	Third Party Target	Threat Group	Target	Discovery Date	Start Date	End Date	No. of months	Nature of Interaction	Type of Target	Interdependency with oth	Information stolen	Type of Operation	Methods	Operational Success	Immediacy	Directness	Objective	Behaviour Change in Tar	Online effects	Secondary effects	Official Government Statement	Official Government Statement Fro	Security Firm Forensics?
18	DHS employee hack through	China	US	0	0	-	DHS employees with security clearance	01-Sep-14	01-Dec-13	01-Sep-14	9.13	3	2	2	2	3	3	1	2	1	2	0	1.3	1.3	No	No	FBI
19	Multiple hacks into Department of Energy	China	US	0	0	APT 10/Cloudhopper/Stone Panda	US Department of Energy	01-Feb-13	15-Oct-10	01-Oct-14	48.23	3	2	2	1	3	3	1	2	1	2,3	0	1.4	1.2, 6.2	No	No	FBI
20	Hikit	China	US	0	1	APT 17/Deputy Dog/Axiom/Wicked Panda	Small defense contractors, Government, high tech information technology, defense, research, media and	Oct-14	01-Sep-08	27-Oct-14	74.90	3	1,2,3	2	1,3	3	3	1	2	1	3	0	1.4	1.4, 7.1	Yes	Yes	Consortium of security companies led by Novetta
21	USPS hack	China	US	0	0	-	United States Postal Service	15-Sep-14	08-Nov-14	10-Nov-14	0.07	3	2	2	2	2	3	1	2	1	2	0	1.3	1.1, 6.2	No	No	FBI
22	Anthem Breach	China	US	0	0	APT 19/Deep Panda/Black Vine	Health insurance giant - Anthem	29-Jan-15	18-Feb-14	30-Nov-14	9.50	3	1	2	2	2	3	1	2	1	2	0	1.4	1.4, 6.2	No	No	Fireeye, Symantec
23	Forbes website watering hole breach	China	US	0	1	Codoso/Sunshop	Defense sector firms, financial service companies, Chinese dissident groups and other political targets	01-Dec-14	28-Nov-14	01-Dec-14	0.10	3	1,3	2	1,3	2	3	1	2	1	2,3	2,3	1.3	1.3	No	No	iSight, Invincea
24	Premera Blue Cross breach	China	US	0	0	APT 19/Deep Panda/Black Vine	Premera Health Insurance firm	Jan-15	May-14	29-Jan-15	9.10	3	1	2	2	3	3	1	2	1	2	0	1.4	1.4, 6.1	No	No	Fireeye, ThreatConnec
25	University of Connecticut Engineering hack	China	US	0	0	-	University of Connecticut School of Engineering	01-Mar-15	24-Sep-13	09-Mar-15	17.70	3	2	2	1,2	3	3	1	2	1	2	0	1.3	1.1, 4.2	No	No	Dell Secureworks
26	Github	China	US	0	0	-	Github pages - Greatfire.org The New York Times Chinese edition	18-Mar-15	17-Mar-15	30-Mar-15	0.43	1	1	2	-	1	2,3	1	1	1	1	0	2.1	-	No	No	Greatfire, Netresec, Errata security
27	Office of Personnel	China	US	0	0	X1, X2	Government employees with security clearence	01-Mar-14	01-Nov-13	15-Apr-15	17.67	3	2	2	2	3	3	1	2	1	2	0	1.4	1.2, 6.2, 7.	Yes	Yes	Fireeye
28	Operation Blackcoffee	China	US	0	1	APT 17/Deputy Dog/Axiom/Wicked Panda	U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations via Microsoft Technet.	late 2014	Apr-13	May-15	25.33	3	1,2	2	1,3	3	3	1	2	1	2	0	1.4	1.4, 7.1	No	No	Fireeye
29	Indictment of 10 Chinese intelligence officers and co-conspirators	China	US	0	1	Jiangsu Province Ministry of State Security (may be from APT 3 or APT 10)	Steal turbofan jet engine technology	Oct-18	Jan-10	May-15	64.87	3	1	2	3	3	3	1	2	1	3	0	1.4	1.3, 7.2	Yes	Yes	Cisco Talos, DOJ indictment
30	US government agency hack	China	US	0	1	-	US government agency	May-15	06-May-15	May-15	0.83	3	2	2	1	2	3	1	2	1	2	0	1.2	-	No	No	Paloaltonetworks
31	United Airlines	China	US	0	0	APT 19/Deep Panda/Black Vine	United Airlines	May-15	May-15	01-Jun-15	1.03	3	1	2	2	2	3	1	2	1	2	0	1.3	1.4, 6.2	No	No	-
32	University of Virginia	China	US	0	0	-	University of Virginia	Jun-15	Jun-15	Jun-15	0.33	3	2	2	1	2	3	1	2	1	2	0	1.2	-	Yes	No	Fireeye

No.	Name	Initiator	Defender	Third Party Initiator	Third Party Target	Threat Group	Target	Discovery Date	Start Date	End Date	No. of months	Nature of Interaction	Type of Target	Interdependency with	Information sto	Type of Operation	Methods	Operational Success	Immediacy	Directness	Objective	Behaviour Change in	Online effects	Secondary effects	Official Government State	Official Government Stater	Security Firm Forensics?
33	US Top National Security and Trade Officials Personal Emails hacked	China	US	0	0	Dancing Panda/Legion Amethyst	Private emails of top national security and trade officials	Apr-10	Apr-10	10-Aug-15	65.23	3	3	2	1	3	3	1	2	1	2	0	1.4	1.1, 7.1	No	No	NSA, Intelligence officials
34	University of Pennsylvania state engineering	China	US	0	0	-	University of Pennsylvania School of Engineering	Sep-12	Sep-12	15-Sep-15	36.97	3	1	2	1,2	3	3	1	2	1	2	0	1.3	1.1, 4.2	No	Yes	Fireeye
35	Iron Tiger	China	US	0	1	APT 27/Emissary Panda/TG-3390/Bronze Union/Luckymouse	US military and defense contractors, aerospace, automobile technology, energy, and pharmaceuticals, education, legal and organisations focused on international	Aug-15	15-Jan-13	Sep-15	32.47	3	1	2	1,3	3	3	1	2	1	2,3	0	1.4	1.4, 7.1	No	No	Dell Secureworks, TrendMicro
36	Woods Hole Oceanographic Institution (WHOI)	China	US	0	0	APT 40/ Temp.Periscope/ Leviathan/ Mudcarp	WHOI	Jun-15	Feb-13	Oct-15	32.40	3	2	2	3	3	3	1	2	1	3	0	1.4	1.4, 7.1	No	No	Fireeye (Mandiant), iDefense (Accenture)
37	US government and contractor networks hacked	China	US	0	1	APT 6/Group 19	US-China relations experts, Defense Department entities, federal government	Feb-16	Jan-11	Apr-16	63.90	3	2,1	2	1,3	3	3	1	2	1	2,3	0	1.4	1.4, 7.1	Yes	No	Fireeye, Kaspersky Lab
38	US aircraft carrier	China	US	0	1	-	Foreign officials who visited USS Ronald Reagan vessel in South	Oct-10	11-Jul-16	12-Jul-16	0.03	3	3	2	1	2	3	0	-	-	1	0	-	-	No	No	Fireeye
39	US-Taiwan Security conference	China	US	0	1	-	Defense officials attending US-Taiwan security conference	Oct-16	Oct-16	Oct-16	0.90	3	3	2	1	2	3	0	-	-	1	0	-	-	No	No	Volexity
40	Overseas Chinese language new websites	China	US	0	1	Winnti Umbrella	China Digital Times, Epoch Times	Feb-17	Jan-15	Feb-17	25.40	3	1	2	1	3	3	1	2	1	2	0	1.2	-	No	No	Citizen Lab
41	Operation Tradesecret	China	US	0	0	APT 10/Cloudhopper/Stone Panda	Registration page for meetings on the National Foreign Trade Council website	Feb-17	Feb-17	01-Mar-17	0.93	3	2	2	2	2	3	1	2	1	2	0	1.1	-	No	No	Fidelis Cybersecurity
42	Indictment of 3 Chinese nationals behind hacking of Siemens, Trimble, Moody's	China	US	0	1	APT 3/Boyusec/Gothic Panda/UPS Team	Information regarding Siemens energy, technology and transportation business	Nov-16	Jan-11	May-17	77.07	3	1	2	3	3	3	1	2	1	3	0	1.4	1.4, 7.2	Yes	Yes	Recorded Future, Crowdstrike
43	Hijacking of Local Internet Service Provider	China	US	0	1	-	Border Gateway Protocol between autonomous networks	2018	Sep-15	Jul-17	22.30	3	1	3	1,3	3	4	1	2	1	2,3	0	1.4	1.4, 4.2, 6.	No	No	Research by academics
44	Guo Wengui	China	US	0	1	-	Law firm (Clark Hill) and think tank (Hudson Institute) linked to US based activist	Oct-17	Sep-17	Oct-17	0.13	1	1	2	1	2	2, 3	1	1	1	1	1	2.1	7.1	No	Yes (Denial)	-
45	Operation PZChao	China	US	0	1	APT 27/Emissary Panda/TG-3390/Bronze Union/Luckymouse	Government, Technology, Education, Telecommunications sector in the USA and	Feb-18	Jul-17	Feb-18	7.17	3	1,2	2	3	3	3	1	2	1	3	0	1.4	1.4, 7.1	No	No	Bitdefender

No.	Name	Initiator	Defender	Third Party Initiator	Third Party Target	Threat Group	Target	Discovery Date	Start Date	End Date	No. of months	Nature of Interaction	Type of Target	Interdependency with	Information stol	Type of Operation	Methods	Operational Success	Immediacy	Directness	Objective	Behaviour Change in	Online effects	Secondary effects	Official Government State	Official Government Stater	Security Firm Forensics?
45	Operation PZChao	China	US	0	1	APT 27/Emissary Panda/TG-3390/Bronze Union/Luckymouse	Government, Technology, Education, Telecommunications sector in the USA and	Feb-18	Jul-17	Feb-18	7.17	3	1,2	2	3	3	3	1	2	1	3	0	1.4	1.4, 7.1	No	No	Bitdefender
46	Thrip campaign	China	US	0	1	Thrip	Satellite communications, telecommunications, Geospatial imaging,	2017	Oct-17	Jun-18	8.10	3	1	3	1	3	3	1	2	1	2	0	1.4	1.4, 7.1, 6.2	No	No	Symantec
47	Opportunity Alaska	China	US	0	0	-	The Alaska Communications Systems Group Alaska Department of Natural Resources Alaska Power & Telephone Company State of Alaska Government TelAlaska	2018	Apr-18	Jun-18	2.03	3	2	2	1	2	3	1	2	1	2	0	1.1	-	No	No	Recorded Future
48	Indictment of 2 Chinese hackers from APT 10 (Operation Cloudhopper)	China	US	0	1	APT 10/Cloudhopper/Stone Panda	Managed service Providers, technology companies, US government agencies, includnig Dept of Energy's National Laboratory and NASA's jet propulsion lab, US	Apr-17	01-Jan-06	Sep-18	154.20	3	1,2,3	3	2,3	1	3	1	2	1	2,3	0	1.4	1,4, 6.2, 7.	Yes	Yes	DOJ indictment Fireeye Recorded Future
49	Marriott Hotel	China	US	0	1	-	Mariott-owned Starwood hotel guest reservation database containing names, addresses, phone numbers, birth dates, email addresses credit card information and passport details, arrival and departure information, reservation date	Sep-18	01-Jan-14	Sep-18	56.80	3	1	1	2	3	3	1	2	1	2	0	1.4	1.4, 6.2	No	Yes	FBI investigation
50	US Navy espionage	China	US	0	1	APT 40/ Temp.Periscope/ Leviathan/ Mudcarp	Contractor for the Navy Undersea Warfare Centre, universities with military research labs that develop advanced technology for use by the Navy or other service	Jan-18	Apr-17	Dec-18	20.30	3	3	2	1	3	3	1	2	1	2	0	1.4	1.4, 4.2, 7.	Yes	Yes	Fireeye, Proofpoint, Accenture Security

VII. Bibliography

Allison, G. T. (2017). *Destined for war: Can America and China escape Thucydides's trap?* Melbourne, London: Scribe.

Amnesty International (2018). *Why we're taking the UK government to court over mass spying.* Retrieved March 14, 2019, from Amnesty International, UK: https://www.amnesty.org.uk/why-taking-government-court-mass-spying-gchq-nsa-tempora-prism-edward-snowden.

Appelbaum, J., Horchert, J., & Stocker, C. (2013). *Shopping for Spy Gear: Catalog Advertises NSA Toolbox.* Retrieved July 23, 2019, from Spiegel: https://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

Applegate, S. (2011). Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare. *IEEE Security & Privacy Magazine, 9*(5), 16–22.

Arquilla, J. (2012). *Cyberwar Is Already Upon Us.* Retrieved March 14, 2019, from Foreign Policy: https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy, 12*(2), 141–165. Retrieved October 21, 2018, from https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch2.pdf.

Austin, G. (2015). *The Pentagon's Law of War for Cyberspace.* Retrieved January 16, 2019, from The Diplomat: https://thediplomat.com/2015/12/the-pentagons-law-of-war-for-cyberspace/.

Austin, G. (2018). *How Good Are China's Cyber Defenses?* Retrieved July 23, 2019, from The Diplomat: https://thediplomat.com/2018/07/how-good-are-chinas-cyber-defenses/.

Austin, G. (Ed.). 2019. *Civil Defence Gaps Under Cyber Blitzkrieg.* Canberra.

Axelrod, R., & Iliev, R. (2014). Timing of cyber conflict. *Proceedings of the National Academy of Sciences of the United States of America, 111*(4), 1298–1303.

Baldwin, D. A. (1997). The concept of security. *Review of International Studies, 23*(1), 5–26.

Barkin, N. (2018, October 12). Exclusive: Five Eyes intelligence alliance builds coalition to counter China. *Reuters.* Retrieved July 24, 2019, from https://www.reuters.com/article/us-china-fiveeyes/exclusive-five-eyes-intelligence-alliance-builds-coalition-to-counter-china-idUSKCN1MM0GH.

Barrett, B. M. (2005). Information Warfare: China's Response to U.S. Technological Advantages. *International Journal of Intelligence and CounterIntelligence, 18*(4), 682–706.

BBC (2012, July 20). Obama warns U.S. on cyber-threats. *BBC.* Retrieved October 21, 2018, from https://www.bbc.com/news/technology-18928854.

BBC (2019). *Huawei faces U.S. charges: The short, medium and long story.* Retrieved July 24, 2019, from BBC: https://www.bbc.co.uk/news/world-us-canada-47046264.

Beinart, P. (2019). *China Isn't Cheating on Trade.* Retrieved July 24, 2019, from The Atlantic: https://www.theatlantic.com/ideas/archive/2019/04/us-trade-hawks-exaggerate-chinas-threat/587536/.

Bejtlich, R. (2013). *Don't Underestimate Cyber Spies: How Virtual Espionage Can Lead to Actual Destruction.* Retrieved July 24, 2019, from Foreign Affairs: https://www.foreignaffairs.com/articles/united-states/2013-05-02/dont-underestimate-cyber-spies.

Bell, A. (1984). Language Style as Audience Design: Language in Society. *00474045, 13*(2), 145–204, from http://www.jstor.org/stable/4167516.

Bendrath, R., Eriksson, J., & Giacomello, G. (2007). From 'cyberterrorism' to 'cyberwar', back and forth: How the United States securitized cyberspace. In J. Eriksson & G. Giacomello (Eds.), *Routledge advances in international relations and global politics. International relations and security in the digital age* (pp. 57–82). London: Routledge.

Bennett, 2. (2017). *Why Trump is sticking with Obama's China hacking deal.* Retrieved July 23, 2019, from Politico: https://www.politico.com/story/2017/11/08/trump-obama-china-hacking-deal-244658.

Betz, D. J. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. *Journal of Strategic Studies, 35*(5), 689–711.

Betz, D. J., & Stevens, T. (2011). *Cyberspace and the state: Toward a strategy for cyber-power. Adelphi: Vol. 424.* Abingdon: Routledge.

Blair, D. C., Barrett, C. R., Boustany Jr, C. W., Gorton, S., Lynn III, W. J., Wince-Smith, D., & Young, M. K. (2019). *IP Commission 2019 Review - Progress and Updated Recommendations.* The National Bureau of Asian Research. Retrieved July 24, 2019, from http://www.ipcommission.org/report/ip_commission_2019_review_of_progress_and_updated_recommendations.pdf.

Blair, D. C., Huntsman, J. M., Barrett, C. R., Gorton, S., Lynn III, W. J., Wince-Smith, D., & Young, M. K. (2013). *The IP Commission Report: The Report of The Commission on the Theft of American Intellectual Property.* The National Bureau of Asian Research. Retrieved July 24, 2019, from http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

Blair, D. C., Huntsman, J. M., Barrett, C. R., Lynn III, W. J., Gorton, S., Wince-Smith, D., & Young, M. K. (2017). *Update to the IP Commission*

Report. The National Bureau of Asian Research. Retrieved July 23, 2019, from http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf.

Blanchard, B., & Perry, M. (2019, May 16). Lack of innovation is 'Achilles heel' for China's economy, Xi says. *Reuters.* Retrieved July 24, 2019, from https://uk.reuters.com/article/us-china-politics-xi/lack-of-innovation-is-achilles-heel-for-chinas-economy-xi-says-idUKKCN1SM08G.

Blank, R. M. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations* (Joint Task Force Transformation Initiative). National Institute of Standards and Technology. Retrieved March 14, 2019, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Blank, S. (2017). Cyber War and Information War à la Russe. In G. Perkovich & A. E. Levite (Eds.), *Understanding Cyber Conflict - 14 Analogies* (pp. 81–98). Washington, DC: Georgetown University Press.

Bluestone (2018). *Cyber Threat Report: China.* Retrieved March 15, 2019, from Bluestone: https://www.bluestoneanalytics.com/news/chinathreatreport.

Bradsher, 2. (2019, July 24). A China-U.S. Trade Truce Could Enshrine a Global Economic Shift. *The New York Times.* Retrieved July 24, 2019, from https://www.nytimes.com/2019/06/29/business/us-china-trump-trade-truce.html.

Brant, R. (2019, March 25). How a Chinese firm fell victim to intellectual property theft. *BBC.* Retrieved July 24, 2019, from https://www.bbc.co.uk/news/business-47689065.

Brantly, A. F. (2016). *The decision to attack: Military and intelligence cyber decision-making. Studies in security and international affairs.* Athens: The University of Georgia Press.

Brenner, J., & Lindsay, J. R. (2015). Debating the Chinese Cyber Threat. *International Security, 40*(1), 191–195, from https://muse-jhu-edu.ezproxy.lib.gla.ac.uk/article/589752/pdf.

Brookes, A. (2014). *Is China Swarming With Foreign Spies?* Retrieved July 23, 2019, from Foreign Policy: https://foreignpolicy.com/2014/11/04/is-china-swarming-with-foreign-spies/.

Bryman, A. (2016). *Social research methods* (Fifth edition). Oxford: Oxford University Press.

Buchanan, B. (2017). *The cybersecurity dilemma: Hacking, trust and fear between nations.* New York, NY: Oxford University Press.

Bureau of Industry and Security (2019). *Huawei and Affiliates Entity List Rule.* Retrieved July 24, 2019, from Bureau of Industry and Security: https://www.bis.doc.gov/index.php/documents/regulations-docs/2394-huawei-and-affiliates-entity-list-rule.

Buzan, B., Waever, O., & Wilde, J. d. (1998). *Security: a new framework for analysis.* Boulder, Colo, London: Lynne Rienner Pub.

Caplan, N. (2013). Cyber War: the Challenge to National Security. *Global Security Studies, 4*(1), 93–115. Retrieved October 28, 2018, from http://globalsecuritystudies.com/Caplan%20Cyber.pdf.

Carlin, J. P., & Graff, G. M. (2019). *The dawn of the code war: America's battle against Russia, China, and the rising global cyber threat* (First edition). New York: PublicAffairs.

Center for Strategic and International Studies (2013). *The Economic Impact of Cybercrime and Cyber Espionage.* Santa Clara, CA: McAfee. Retrieved July 23, 2019, from https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4.pdf.

Chan, S. (2018). More Than One Trap: Problematic Interpretations and Overlooked Lessons from Thucydides. *Journal of Chinese Political Science*, 1–14.

Chang, A. (2014). *Warring State: China's Cybersecurity Strategy*. Center for a New American Security. Retrieved March 06, 2019, from https://s3.amazonaws.com/files.cnas.org/documents/CNAS_WarringState_Chang_report_010615.pdf?mtime=20160906082142.

Chazan, G. (2019, March 11). U.S. threatens to cut intelligence sharing with Berlin over Huawei. *The Financial Times.* Retrieved March 14, 2019, from https://www.ft.com/content/00dc81a6-4417-11e9-b168-96a37d002cd3.

Cheng, W. (2013). Corpus-Based Linguistic Approaches to Critical Discourse Analysis. In C. Chapelle (Ed.), *The Encyclopedia of Applied Linguistics* (pp. 1–8). Blackwell Publishing Ltd.

Choucri, N. (2012). *Cyberpolitics in international relations*. Cambridge, Mass: MIT Press.

Office of the Director of National Intelligence (2013). *Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage.* Retrieved July 24, 2019, from Office of the Director of National Intelligence: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economic-espionage.

Clarke, R. A., & Knake, R. K. (2012). *Cyber war: The next threat to national security and what to do about it* (First Ecco paperback edition). New York: Ecco.

Clausewitz, C. v. (1980). *On war.* United States: CreateSpace.

Coats, D. R. (2019). *Worldwide Threat Assessment of the U.S. Intelligence Community*. Senate Select Committee on Intelligence. Retrieved July 23,

2019, from https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Constantin, L. (2015a). *The NSA not only creates, but also hijacks, malware with Quantumbot.* Retrieved July 23, 2019, from CSO from IDG: https://www.computerworld.com/article/2871687/the-nsa-not-only-creates-but-also-hijacks-malware-with-quantumbot.html.

Constantin, L. (2015b). *OPM underestimated the number of stolen fingerprints by 4.5 million.* Retrieved July 23, 2019, from CIO: https://www.cio.com/article/2985713/opm-underestimated-the-number-of-stolen-fingerprints-by-45-million.html.

Cooper, Z. (2018). *Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare.* Washington DC: Foundation for Defense of Democracies. Retrieved March 07, 2019, from https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/REPORT_China_CEEW.pdf.

Costello, J., & McReynolds, J. (2018). *China's Strategic Support Force: A Force for a New Era* (China Strategic Perspectives No. 13). Institute for National Strategic Studies. Retrieved March 14, 2019, from https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

The Council of Economic Advisers (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy.* The White House. Retrieved July 24, 2019, from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

Cox, J. (2016). *What We Know About the Exploits Dumped in NSA-Linked Hack.* Retrieved July 24, 2019, from Vice:

https://www.vice.com/en_us/article/bmv55m/what-we-know-about-the-exploits-dumped-in-nsa-linked-shadow-brokers-hack.

Cox, J. (2017). *NSA Exploit Peddlers The Shadow Brokers Call It Quits.* Retrieved July 24, 2019, from Vice: https://www.vice.com/en_us/article/vv7ja4/nsa-exploit-peddlers-the-shadow-brokers-call-it-quits.

Crowdstrike (2019). *2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed,* from https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/.

Cukier, W., Bauer, R., & Middleton, C. (2004). Applying Habermas' Validity Claims as a Standard for Critical Discourse Analysis. In B. Kaplan, D. P. Truex, D. Wastell, A. T. Wood-Harper, & J. I. DeGross (Eds.), *IFIP International Federation for Information Processing: Vol. 143. Information Systems Research. Relevant Theory and Informed Practice* (pp. 233–258). Boston, MA: Springer Science + Business Media Inc.

Cukier, W., Ngwenyama, O., Bauer, R., & Middleton, C. (2009). A critical analysis of media discourse on information technology: preliminary results of a proposed method for critical discourse analysis. *Information Systems Journal, 19*(2), 175–196.

Cyrill, M. (2018). *What is Made in China 2025 and Why is the World So Nervous?* Retrieved March 15, 2019, from Dezan Shira & Associates: https://www.china-briefing.com/news/made-in-china-2025-explained/.

Dai, Q. (2002). On Integrating Network Warfare and Electronic Warfare. *China Military Science, 1*, 112–117.

Defense Security Service (2019). *Methods of Contact and Methods of Operation (MCMO) Reporting Volume Matrix.* United States. Retrieved

July 24, 2019, from https://www.cdse.edu/documents/ci-countermeasures-matrix.pdf.

Deibert, R. J. (2003). Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. *Millennium: Journal of International Studies, 32*(3), 501–530.

Demchak, C. C. (2012). *Hacking the Next War.* Retrieved October 31, 2018, from The American Interest: http://indianstrategicknowledgeonline.com/web/Hacking%20the%20Next%20War%20-%20Chris%20C.%20Demchak%20-%20The%20American%20Interest%20Magazine.pdf.

Department of Justice (2018a). *Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies*. 18-1318. Retrieved July 24, 2019, from Department of Justice: https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading.

Department of Justice (2018b). *PRC State-Owned Company, Taiwan Company, and Three Individuals Charged With Economic Espionage.* 18-1435. Retrieved July 24, 2019, from Department of Justice: https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage.

Department of Justice (2018c). *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*. 18-1673. Retrieved July 23, 2019, from Department of Justice: https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

Doffman, Z. (2019, February 28). Huawei Claims U.S. Onslaught Is Because Their 5G Technology Prevents Widespread NSA Spying. *Forbes.* Retrieved

July 24, 2019, from https://www.forbes.com/sites/zakdoffman/2019/02/28/huawei-the-u-s-is-afraid-we-will-stop-the-nsa-spying-it-has-nothing-to-do-with-china/#6fd221d2bc00.

Dombrowski, P., & Demchak, C. C. (2014). Cyber War, Cybered Conflict, and the Maritime Domain, *67*(2), 1–27. Retrieved February 26, 2019, from https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1321&context=nwc-review.

Dudney, R. S. (2011). Rise of Cyber Militias. *Air Force Magazine, 94*(2), 88–89. Retrieved March 14, 2019, from http://www.airforcemag.com/MagazineArchive/Documents/2011/February%202011/0211cyber.pdf.

Dunn Cavelty, M. (2008a). *Cyber-security and threat politics: U.S. efforts to secure the information age. CSS studies in security and international relations.* London: Routledge.

Dunn Cavelty, M. (2008b). Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the U.S. Cyber-Threat Debate. *Journal of Information Technology & Politics, 4*(1), 19–36.

Dunn Cavelty, M. (Ed.). 2012. *The Militarisation of Cyberspace: Why less may be better.* Tallinn, Estonia: IEEE.

Dutta, S., Lanvin, B., & Wunsch-Vincent, S. (2018). *Global Innovation Index 2018 - Energiizing the World with Innovation.* Geneva, Switzerland: Cornell University, INSEAD, World Intellectual Property Organization. Retrieved July 24, 2019, from https://www.globalinnovationindex.org/home.

Efrony, D. (2019). *Entering the Third Decade of Cyber Threats: Toward Greater Clarity in Cyberspace.* Retrieved July 24, 2019, from Lawfare:

https://www.lawfareblog.com/entering-third-decade-cyber-threats-toward-greater-clarity-cyberspace.

Eriksson, J. (2001). Cyberplagues, IT, and Security: Threat Politics in the Information Age. *Journal of Contingencies and Crisis Management, 9*(4), 211.

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review, 27*(3), 221–244.

European Union Agency For Network and Information Security (2018). *Good practices on interdependencies between OES and DSPs*. Retrieved July 22, 2019, from https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps.

Fairclough, N. (1995a). *Critical discourse analysis: The critical study of language. Language in social life series.* London: Longman.

Fairclough, N. (1995b). *Media discourse.* London: Arnold.

Fazzini, K. (2019, January 29). China and Russia could disrupt U.S. energy infrastructure, intelligence report warns on heels of Huawei indictments. *CNBC.* Retrieved July 24, 2019, from https://www.cnbc.com/2019/01/29/china-russia-could-disrupt-us-infrastructure-with-cyber-attacks-odni.html.

Fickling, D. (2019). *We Should Let China Spy on Us.* Retrieved July 24, 2019, from The Washington Post: https://www.washingtonpost.com/business/we-should-let-china-spy-on-us/2019/04/20/985dc970-63d1-11e9-bf24-db4b9fb62aa2_story.html?noredirect=on&utm_term=.d16cb08152a1.

Fifield, A. (2018, September 24). China thinks the trade war isn't really about trade. *The Washington Post.* Retrieved July 24, 2019, from https://www.washingtonpost.com/world/asia_pacific/china-thinks-the-

trade-war-isnt-really-about-trade/2018/09/23/67c7b0ec-bb51-11e8-b1c5-7a2126bc722c_story.html?utm_term=.e15ae97e53b3.

Finkle, J., & Bing, C. (2018, December 11). China's hacking against U.S. on the rise: U.S. intelligence official. *Reuters.* Retrieved July 24, 2019, from https://www.reuters.com/article/us-usa-cyber-china/chinas-hacking-against-u-s-on-the-rise-u-s-intelligence-official-idUSKBN1OA1TB.

Finklea, K., Christensen, M. D., Fischer, E. A., Lawrence, S. V., & Theohary, C. A. (2015). *Cyber Intrusion into U.S. Office of Personnel Management: In Brief.* Congressional Research Service. Retrieved July 23, 2019, from https://fas.org/sgp/crs/natsec/R44111.pdf.

Fireeye (2016). *Red Line Drawn: China Recalculates its Use of Cyber Espionage.* California, United States. Retrieved July 22, 2019, from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

Fireeye (2017). *APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat.* Retrieved July 23, 2019, from Fireeye: https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html.

Fisher, D. (2019). *APT Groups Moving Down the Supply Chain.* Retrieved July 23, 2019, from Decipher: https://duo.com/decipher/apt-groups-moving-down-the-supply-chain.

Fowler, R. (1991). Critical Linguistics. In K. Halmkjaer (Ed.), *The Linguistic Encyclopedia.* London: Routledge.

France24 (2011). *France is top industrial espionage offender.* Retrieved July 24, 2019, from France24: https://www.france24.com/en/20110104-france-industrial-espionage-economy-germany-russia-china-business.

Friedberg, A. L. (2005). The Future of U.S.-China Relations: Is Conflict Inevitable? *International Security, 30*(2), 7–45.

Gallagher, S. (2013). *Your USB cable, the spy: Inside the NSA's catalog of surveillance magic.* Retrieved July 23, 2019, from Ars Technica: https://arstechnica.com/information-technology/2013/12/inside-the-nsas-leaked-catalog-of-surveillance-magic/.

Gallagher, S. (2015). *NSA secretly hijacked existing malware to spy on N. Korea, others.* Retrieved July 23, 2019, from Ars Technica: https://arstechnica.com/information-technology/2015/01/nsa-secretly-hijacked-existing-malware-to-spy-on-n-korea-others/.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine, 30*(1), 28–38.

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security, 38*(2), 41–73.

Gertz, B. (2016). *Cybercom: OPM Hack Highlights China Big Data Spying.* Retrieved July 23, 2019, from The Washington Free Beacon: https://freebeacon.com/national-security/cybercom-opm-hack-highlights-china-big-data-spying/.

Gilbert, D. (2017). *The U.S. government is stockpiling lists of "zero day" software bugs that let it hack into iPhones*. Retrieved July 24, 2019, from Vice: https://news.vice.com/en_us/article/8xmjyp/the-u-s-government-is-stockpiling-lists-of-zero-day-software-bugs-that-let-it-hack-into-iphones.

Gilli, A., & Gilli, M. (2019). Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security, 43*(3), 141–189.

Goldman, E. O., & Arquilla, J. (2014). *Cyber Analogies.* Monterey, CA: Department of Defense Information Operations, Naval Postgraduate School. Retrieved July 22, 2019, from https://apps.dtic.mil/dtic/tr/fulltext/u2/a601645.pdf.

Goldstein, A. (2013). First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations. *International Security, 37*(4), 49–89.

Goodman, W. (2010). Cyber Deterrence - Tougher in Theory than in Practice? *Strategic Studies Quarterly*, 102–135. Retrieved July 22, 2019, from https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-04_Issue-3/Goodman.pdf.

Gorton, S. (2013). *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology* (No. 113-67). House Energy & Commerce Committee, Subcommittee on Oversight and Investigations. Retrieved July 24, 2019, from http://www.ipcommission.org/press/Gorton_Testimony_070913.pdf.

Greenberg, A. (2019). *A Mysterious Hacker Group Is On a Supply Chain Hijacking Spree.* Retrieved July 24, 2019, from Wired: https://www.wired.com/story/barium-supply-chain-hackers/.

Greengard, S. (2010). The new face of war. *Communications of the ACM, 53*(12), 20.

Greenwald, G. (2014). *The U.S. Government's Secret Plans to Spy for American Corporations.* Retrieved July 24, 2019, from The Intercept: https://theintercept.com/2014/09/05/us-governments-plans-use-economic-espionage-benefit-american-corporations/.

Groffman, N. (2019). *China's extradition requests must be based in law, not on persuasion.* Retrieved July 24, 2019, from South China Morning Post: https://www.scmp.com/news/china/politics/article/3002355/if-chinas-extradition-powers-are-expand-they-must-be-based-law.

Guluzade, A. (2019). *Explained, the role of China's state-owned companies.* Retrieved July 24, 2019, from World Economic Forum: https://www.weforum.org/agenda/2019/05/why-chinas-state-owned-companies-still-have-a-key-role-to-play/.

Habermas, J. (1984). *Reason an the rationalization of society* (First published in paperback). *The theory of communicative action: volume 1*. Cambridge, UK: Polity Press.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155–1175. Retrieved October 26, 2018, from https://nissenbaum.tech.cornell.edu/papers/digital%20disaster.pdf.

Happa, J., & Fairclough, G. (2017). A Model to Facilitate Discussions About Cyber Attacks. In M. Taddeo & L. Glorioso (Eds.), *Philosophical Studies Series: volume 124. Ethics and Policies for Cyber Operations. A NATO Cooperative Cyber Defence Centre of Excellence Initiative* (pp. 169–185). Cham: Springer International Publishing.

Harrell, P. (2018). *China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses: Testimony before the Senate Judiciary Committee.* Retrieved March 15, 2019, from Center for a New American Security: https://www.cnas.org/publications/congressional-testimony/chinas-non-traditional-espionage-against-the-united-states-the-threat-and-potential-policy-responses.

Hass, R. & Balin, Z. (2019). *U.S.-China relations in the age of artificial intelligence.* Retrieved July 24, 2019, from Brookings: https://www.brookings.edu/research/us-china-relations-in-the-age-of-artificial-intelligence/.

Hathaway, O. A., & Crootof, R. (2012). *The Law of Cyber-Attack* (Faculty Scholarship Series). Yale Law School Legal Scholarship Repository. Retrieved February 25, 2019, from https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4844&context=fss_papers.

Healey, J. (Ed.) (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012.* Vienna, Va.: Cyber Conflict Studies Ass.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security, 4*(2), 49–60.

Hjortdal, M. (2011). China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security, 4*(2), 1–24.

Horowitz, J. (2019, January 29). U.S. unveils its criminal case against Huawei, alleging China giant stole trade secrets and violated Iran sanctions. *CNN Business.* Retrieved March 14, 2019, from https://edition.cnn.com/2019/01/28/business/huawei-charges/index.html.

Horwitz, J. (2018). *U.S. lobbies Germany, Italy, and Japan to ban Huawei 5G equipment.* Retrieved March 14, 2019, from https://www.facebook.com/venturebeat/: https://venturebeat.com/2018/11/23/u-s-lobbies-germany-italy-and-japan-to-ban-huawei-5g-equipment/.

Iasiello, E. (2016). China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities. *Journal of Strategic Security, 9*(2), 47–71. Retrieved March 14, 2019, from https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/Volume-08_Issue-4/iasiello_e.pdf.

Ikenberry, J. G. (2008). *The Rise of China and the Future of the West: Can the Liberal System Survive?* Retrieved March 15, 2019, from ForeignAffairs: https://www.foreignaffairs.com/articles/asia/2008-01-01/rise-china-and-future-west.

Ikenberry, J. G. (2013). The Rise of China, the United States, and the Future of the Liberal International Order. In D. L. Shambaugh (Ed.), *Tangled titans. The United States and China* (pp. 53–72). Lanham, Md.: Rowman & Littlefield.

The Information Office of the State Council (2015). *China's Military Strategy*. Beijing, China: The State Council Information Office of the People's Republic of China. Retrieved March 06, 2019, from http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

Inkster, N. (2015). The Chinese Intelligence Agencies Evolution and Empowerment in Cyberspace. In J. R. Lindsay, T. M. Cheung, & D. S. Reveron (Eds.), *China and cybersecurity. Espionage, strategy, and politics in the digital domain* (pp. 29–51). Oxford: Oxford University Press.

Jensen, B. (2017). The Cyber Character of Political Warfare. *The Brown Journal of World Affairs, 24*(1), 159–171, from ctx_ver=Z39.88-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&rfr_id=info%3Asid%2Fsummon.serialssolutions.com&rft_val_fmt=info%3Aofi%2Ffmt%3Akev%3Amtx%3Ajournal&rft.genre=article&rft.atitle=The+Cyber+Character+of+Political+Warfare&rft.jtitle=The+Brown+Journal+of+World+Affairs&rft.au=Benjamin+Jensen&rft.date=2017-10-01&rft.pub=The+Brown+Journal+of+World+Affairs&rft.issn=1080-0786&rft.eissn=2472-3347&rft.volume=24&rft.issue=1&rft.spage=159&rft.epage=171&paramdict=en-U.S..

Jiang, K., Keller, W., Qiu, L., & Ridley, W. (2018). *International Joint Ventures and Internal vs. External Technology Transfer: Evidence from China.* Cambridge, MA: The National Bureau of Economic Research. Retrieved July 24, 2019, from https://www.nber.org/papers/w24455.

Jiang, S. & Westcott, B. (2019). *China slams U.S. over 'unreasonable crackdown' on Huawei.* Retrieved March 14, 2019, from CNN Business: https://edition.cnn.com/2019/01/28/business/huawei-us-china-response-intl/index.html.

Joint Chiefs of Staff (2014). *Joint Publication 3-13: Information Operations.* United States. Retrieved July 22, 2019, from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

Joint Chiefs of Staff (2018). *Joint Publication 3-12, Cyberspace Operations.* United States. Retrieved August 21, 2018, from http://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/.

Kaspersky (2019). *What Is an Advanced Persistent Threat (APT)?* Retrieved July 22, 2019, from Kaspersky: https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats.

Kastrenakes, J. (2018). *Trump signs bill banning government use of Huawei and ZTE tech.* Retrieved August 13, 2018, from The Verge: https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump.

Kello, L. (2017). *The Virtual Weapon and International Order:* Yale University Press.

Kharpal, A. (2019). *Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice.* Retrieved July 24, 2019, from CNBC: https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

Kingdon, J. W. (2003). *Agendas, alternatives, and public policies* (2. ed.). *Longman classics in political science.* New York: Longman.

Kirshner, J. (2012). The tragedy of offensive realism: Classical realism and the rise of China. *European Journal of International Relations, 18*(1), 53–75.

Klimburg, A. (2011). Mobilising Cyber Power. *Survival, 53*(1), 41–60.

(2012). *National Cyber Security Framework Manual.* (Klimburg, A., Ed.). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Koh, H. H. (2012). *International Law in Cyberspace* (Faculty Scholarship Series). Yale Law School Legal Scholarship Repository. Retrieved February 26, 2019, from https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security* (pp. 24–42). Potomac Books.

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy Magazine, 9*(3), 49–51.

Laskai, L., & Sacks, S. (2018). *The Right Way to Protect Americas Innovation Advantage.* Foreign Affairs. Retrieved July 24, 2019, from https://s3-us-west-2.amazonaws.com/maven-user-documents/viewfromthepeak/content/v-8Duxu2LUWR-cbvhRGa3w/Jt7cAJUbc0qUzSoTHfxtXA/The_Right_Way_to_Protect_Americas_Innovation_Advantage.pdf.

Laskai, L., & Segal, A. (2018). *A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage.* Council on Foreign Relations. Retrieved March 14, 2019, from https://www.cfr.org/report/threat-chinese-espionage.

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics, 10*(1), 86–103.

Le, H. H. (2018). *New wave of Chinese assertiveness in the South China Sea?* Retrieved March 15, 2019, from ISEAS Yusof Ishak Institute: https://www.iseas.edu.sg/medias/commentaries/item/7471-new-wave-of-chinese-assertiveness-in-the-south-china-sea-by-le-hong-hiep.

Lee, D. (2019, May 31). For the U.S. and China, it's not a trade war anymore — it's something worse. *Los Angeles Times.* Retrieved July 24, 2019, from https://www.latimes.com/politics/la-na-pol-us-china-trade-stalemate-20190531-story.html.

Lee, M., Greenwald, G., & Marquis-Boire, M. (2015). *A Look at the Inner Workings of NSA's XKEYSCORE.* Retrieved July 23, 2019, from The Intercept: https://theintercept.com/2015/07/02/look-under-hood-xkeyscore/.

Leyden, J. (2015). *Chinese hackers behind OPM megabreach also pwned United Airlines.* Retrieved July 24, 2019, from The Register: https://www.theregister.co.uk/2015/07/30/chinese_hackers_opm_united_airlines_linkage/.

Li, Y. (2019). *Benign tech competition best for China, U.S.*. Retrieved July 24, 2019, from China Daily: http://www.chinadaily.com.cn/a/201903/04/WS5c7c6d73a3106c65c34ec78f.html.

Liang, Q., & Wang, X. (1999). *Unrestricted warfare.* Beijing, China: PLA Literature and Arts Publishing House.

Libicki, M. C. (Ed.) (2009). *RAND Corporation monograph series. Cyberdeterrence and Cyberwar // Cyberdeterrence and cyberwar*. Santa Monica, CA: RAND.

Lieberthal, K., & Singer, P. W. (2012). *Cybersecurity and U.S.-China Relations.* John L. Thornton China Centre at Brookings. Retrieved February 07, 2019, from https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf.

Liff, A. P. (2012). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies, 35*(3), 401–428.

Lin, H. S. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy, 4*, 63–86. Retrieved August 25, 2018.

Lin, H. S. (2012). Escalation Dynamics and Conflict Termination in Cyberspace. *Strategic Studies Quarterly, 6*(3), 46–70, from http://www.au.af.mil/au/.

Lindsay, J. R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. *International Security, 39*(3), 7–47.

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (Eds.) (2015). *China and cybersecurity: Espionage, strategy, and politics in the digital domain.* Oxford: Oxford University Press.

Little, E., & Rogova, G. (2008). *Theoretical foundations and proposed applications of Threat Ontology to information fusion.* Valcartier: Defence Research and Development Canada. Retrieved March 14, 2019, from http://cradpdf.drdc-rddc.gc.ca/PDFS/unc79/p530554.pdf.

Lutz, C. (2018). *FBI Director Christopher Wray Wants to Talk About More than Russia.* Retrieved March 14, 2019, from The Aspen Institute: https://www.aspeninstitute.org/blog-posts/fbi-director-christopher-wray-wants-talk-about-more-than-russia/.

Lyu, J. (2019). *What Are China's Cyber Capabilities and Intentions?* Retrieved July 24, 2019, from Carnegie Endowment for International Peace: https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

MacAskill, E., Thielman, S., & Oltermann, P. (2017, March 07). Major cyber-attack on UK a matter of 'when, not if' – security chief. *The Guardian.* Retrieved January 08, 2019, from https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin.

Maher, R. (2018). Bipolarity and the Future of U.S.-China Relations. *Political Science Quarterly, 133*(3), 497–525.

Manjikian, M. M. (2010). From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly, 54*(2), 381–401.

Marks, J. (2019). *The Cybersecurity 202: Trump's Huawei reversal is outraging Republicans.* Retrieved July 24, 2019, from The Washington Post: https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/07/01/the-cybersecurity-202-trump-s-huawei-reversal-is-outraging-republicans/5d18e1b81ad2e552a21d51c1/?utm_term=.4d93025c12eb.

Maurer, T. (2018). Cyber Proxies and Their Implications for Liberal Democracies. *The Washington Quarterly, 41*(2), 171–188.

Mazarr, M. J. (2019). *This Is Not a Great-Power Competition: Why the Term Doesn't Capture Today's Reality.* Retrieved July 24, 2019, from Foreign Affairs: https://www.foreignaffairs.com/articles/2019-05-29/not-great-power-competition.

Mearsheimer, J. J. (2001). *The tragedy of great power politics* (Updated edition). *The Norton series in world politics.* New York, London: W.W. Norton & Company.

Menn, J. (2013, May 10). Special Report: U.S. cyberwar strategy stokes fear of blowback - Reuters. *Reuters.* Retrieved July 24, 2019, from https://in.reuters.com/article/usa-cyberweapons/special-report-u-s-cyberwar-strategy-stokes-fear-of-blowback-idINDEE9490AX20130510?type=economicNews.

Menn, J. (2015, February 17). Russian researchers expose breakthrough in U.S. spying program. *Reuters.* Retrieved July 24, 2019, from

https://www.reuters.com/article/us-usa-cyberspying-idUSKBN0LK1QV20150217.

Miller, J. (2018). *3 years after data breach, OPM still struggling to modernize IT.* Retrieved July 23, 2019, from Federal News Network: https://federalnewsnetwork.com/opm/2018/02/three-years-after-data-breach-opm-still-struggling-to-modernize-its-it/.

The MITRE Corporation (2019). *ATT&CK Matrix for Enterprise.* Retrieved July 22, 2019, from The MITRE Corporation: https://attack.mitre.org/.

Morgan, L., & Bockius (2008). Doing Business in China. In L. Morgan & Bockius (Eds.), *Emerging Life Sciences Companies Deskbook. Doing Business in China* (pp. 261–283).

Moriuchi, P. (2019). *The New Cyber Insecurity: Geopolitical and Supply Chain Risks From the Huawei Monoculture.* Retrieved July 24, 2019, from Recorded Future: https://www.recordedfuture.com/huawei-technology-risks/.

Nakashima, E. (2015). *U.S. decides against publicly blaming China for data hack.* Retrieved July 23, 2019, from The Washington Post: https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html?utm_term=.654ff2be3e12.

Nakashima, E. & Goldman, A. (2015). *CIA pulled officers from Beijing after breach of federal personnel records.* Retrieved July 23, 2019, from The Washington Post: https://www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html?noredirect=on&utm_term=.896aa31a4a1c.

Nakasone, P. (2018). A Cyber Force for Persistent Operations. *Joint Force Quarterly*. (92), 10–14. Retrieved March 14, 2019, from https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

Nathan, A. J. (2019). *How China Really Sees the Trade War: Xi Still Believes He Has the Upper Hand.* Retrieved July 24, 2019, from Foreign Affairs: https://www.foreignaffairs.com/articles/china/2019-06-27/how-china-really-sees-trade-war.

National Commission for the Review of the Research and Development Programs (2013). *Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community: Unclassified Version.* United States, from https://www.intelligence.senate.gov/sites/default/files/commission_report.pdf.

National Counterintelligence and Security Center (2018a). *Foreign Economic Espionage in Cyberspace.* Retrieved July 24, 2019, from https://fas.org/irp/ops/ci/feec-2018.pdf.

National Counterintelligence and Security Center (2018b). *Foreign Economic Espionage in Cyberspace.* Retrieved March 15, 2019, from https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

National Security Agency (2009). *Turbine.* Retrieved July 24, 2019, from National Security Agency: https://search.edwardsnowden.com/docs/TURBINE2014-03-12_nsadocs_snowden_doc.

Naughton, J. (2019). *Trump's banning of Huawei could be the beginning of the biggest trade war ever | John Naughton.* Retrieved July 24, 2019, from The Guardian:

https://www.theguardian.com/commentisfree/2019/jun/02/trump-banning-huawei-beginning-of-biggest-trade-war-ever-united-states.

Newman, L. H. (2018). *If China Hacked Marriott, 2014 Marked a Full-on Assault.* Retrieved July 24, 2019, from Wired: https://www.wired.com/story/marriott-hack-china-2014-opm-anthem/.

NIS Cooperation Group (2018). *Cybersecurity Incident Taxonomy.* Retrieved July 22, 2019, from http://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf.

Nye, J. S. (2010). *Cyber Power.* Cambridge, MA: Belfer Center for Science and International Affairs. Retrieved September 01, 2018, from https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf.

Nye, J. S. (2011). *The Future of Power: Its Changing Nature and Use in the 21st Century* (1st ed.). New York: Public Affairs.

O'Connor, S. (2019). *How Chinese Companies Facilitate Technology Transfer from the United States.* U.S.-China Economic and Security Review Commission. Retrieved July 24, 2019, from https://www.uscc.gov/Research/how-chinese-companies-facilitate-technology-transfer-united-states.

Oliver, P. E., & Johnston, H. (2000). What a good idea: Frames and ideologies in social movements research. *Mobilization: An International Quarterly, 5*(1), 37–54.

Panetta, L. (2012). *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security.* Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security. New York.

Pendergast, A. (February 2014). *The Diamond Model for Intrusion Analysis: A Primer.* SANS Cyber Threat Intelligence Summit. Arlington, VA.

Perlroth, N., Sanger, D. E., & Shane, S. (2019, May 06). How Chinese Spies Got the N.S.A.'s Hacking Tools, and Used Them for Attacks. *The New York Times.* Retrieved July 24, 2019, from https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html.

Petit, F., Brannegan, D., Verner, D., Buehring, Dickinson, David, Guziel, K., Haffenden, R., et al. (2015). *Analysis of Critical Infrastructure Dependencies and Interdependencies.* United States: Argonne National Laboratory, U.S. Department of Energy. Retrieved July 23, 2019, from https://publications.anl.gov/anlpubs/2015/06/111906.pdf.

Phillips, N., & Hardy, C. (2002). *Discourse analysis: Investigating processes of social construction. Qualitative research methods: Vol. 50.* Thousand Oaks, Calif.: SAGE.

Phneah, E. (2012). *Unreported cyberattacks not just due to reputation concerns.* Retrieved July 22, 2019, from Zdnet: https://www.zdnet.com/article/unreported-cyberattacks-not-just-due-to-reputation-concerns/.

Piiparinen, A. (2015). *The Chinese Cyber Threat in the South China Sea.* Retrieved July 24, 2019, from The Diplomat: https://thediplomat.com/2015/09/the-chinese-cyber-threat-in-the-south-china-sea/.

Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. *Computers & Security, 74*, 371–383, from https://www-sciencedirect-com.ezproxy.lib.gla.ac.uk/science/article/pii/S0167404817300822/pdfft?md

5=eec7ac26e8c6fb3ccea9b16d6bbff8dd&pid=1-s2.0-S0167404817300822-main.pdf.

Podkul, C., O'Keeffe, K., & Viswanatha Aruna (2017). *U.S. Confronts China Over Suspected Cyberattack as Fugitive Guo Wengui Appears in Washington.* Retrieved July 22, 2019, from The Wall Street Journal: https://www.wsj.com/articles/chinese-governments-battle-against-fugitive-guo-wengui-spills-into-washington-1507260255.

Ponemon Institute (2018). *2018 Cost of a Data Breach study: Global Overview.* Michigan, U.S.. Retrieved July 23, 2019, from https://www.ibm.com/security/data-breach.

Powers, d. (2012). Notes on Hype. *International Journal of Communication, 6*, 857–873, from https://ijoc.org/index.php/ijoc/article/view/1441.

Pramuk, J., & Schoen, J. W. (2019, June 29). U.S. and China agree to continue tariff talks. Here's a timeline of how the trade war started. *CNBC.* Retrieved July 24, 2019, from https://www.cnbc.com/2019/06/29/us-china-trade-talks-at-g-20-timeline-of-how-the-tariff-war-started.html.

Pricewaterhouse Coopers; BAE Systems (2017). *Operation Cloud Hopper.* Retrieved July 23, 2019, from https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.

Ranger, S. (2018). *Cybercrime and cyberwar: A spotter's guide to the groups that are out to get you.* Retrieved March 15, 2019, from Zdnet: https://www.zdnet.com/article/cybercrime-and-cyberwar-a-spotters-guide-to-the-groups-that-are-out-to-get-you/.

Ranger, S. (2019). *This 'most dangerous' hacking group is now probing power grids.* Retrieved July 24, 2019, from Zdnet: https://www.zdnet.com/article/this-most-dangerous-hacking-group-is-now-probing-power-grids/.

Richards, J. (2014). *Cyber-war: The anatomy of the global security threat. Palgrave pivot.* Basingstoke: Palgrave Macmillan.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies, 35*(1), 5–32. Retrieved August 16, 2018.

Ritchie, J., & Spencer, L. (2002). Qualitative Data Analysis for Applied Policy Research. In A. M. Huberman & M. B. Miles (Eds.), *The qualitative researcher's companion* (pp. 305–329). Thousand Oaks: Sage Publ.

Roach, S. (2018, April 26). Why U.S. has a weak case against China's trade practices. *South China Morning Post.* Retrieved July 24, 2019, from https://www.scmp.com/comment/insight-opinion/article/2143496/why-us-has-weak-case-against-chinas-unfair-trade-practices.

Roberts, A., Moraes, H. C., & Ferguson, V. (2019). *The U.S.-China Trade War Is a Competition for Technological Leadership.* Retrieved July 24, 2019, from Lawfare: https://www.lawfareblog.com/us-china-trade-war-competition-technological-leadership.

Roscini, M. (2010). World Wide Warfare - Jus ad bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law, 14*, 85–130. Retrieved August 25, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1683370.

Sacks, S., & Li, M. K. (2018). *How Chinese Cybersecurity Standards Impact Doing Business In China.* Center for Strategic and International Studies. Retrieved July 24, 2019, from https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

Saltzman, I. (2013). Cyber Posturing and the Offense-Defense Balance. *Contemporary Security Policy, 34*(1), 40–63.

Sanger, D. E. (2014). *Fine Line Seen in U.S. Spying on Companies.* Retrieved July 24, 2019, from The New York Times: https://www.nytimes.com/2014/05/21/business/us-snooping-on-companies-

cited-by-china.html?_r=0https://www.nytimes.com/2014/05/21/business/us-snooping-on-companies-cited-by-china.html?_r=0.

Sanger, D. E. (2015). *U.S. Decides to Retaliate Against China's Hacking.* Retrieved July 23, 2019, from The New York Times: https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html.

Sanger, D. E. & Perlroth, N. (2014). *N.S.A. Breached Chinese Servers Seen as Security Threat.* Retrieved July 23, 2019, from The New York Times: https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare: Prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.* Cambridge, New York: Cambridge University Press.

Schumpeter (2019). Good copy, bad copy. *The Economist, 432*(9129), 58. Retrieved July 24, 2019, from http://link.galegroup.com.ezproxy.lib.gla.ac.uk/apps/doc/A572984910/EAIM?u=glasuni&sid=EAIM&xid=358a9898.

Scott, J., & Spaniel, D. (2016). *China's Espionage Dynasty: Economic Death by a Thousand Cuts.* Institute for Critical Infrastructure Technology. Retrieved July 22, 2019, from https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.07.28.China_Espionage_Dynasty/ICIT-Brief-China-Espionage-Dynasty.pdf.

Segal, A., Hoffman, S., Hanson, F., & Uren, T. (2018). *Hacking for cash.* Retrieved July 22, 2019, from Australian Strategic Policy Institute: https://www.aspi.org.au/report/hacking-cash.

Segal, A. M. (2017). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age* (Second edition). New York: PublicAffairs.

Seldin, J. (2018). *U.S. Officials: China Tops List of Security Threats*. Retrieved March 14, 2019, from Voice of America: https://www.voanews.com/a/us-officials-china-tops-list-of-security-threats-/4698196.html.

Shambaugh, D. L. (Ed.) (2013). *Tangled titans: The United States and China.* Lanham, Md.: Rowman & Littlefield.

Skeath, C. & Kahn, B. (2018). *State Data Breach Notification Laws: 2018 in Review | Inside Privacy.* Retrieved July 23, 2019, from Covington: https://www.insideprivacy.com/data-security/data-breaches/state-data-breach-notification-laws-2018-in-review/.

Snow, D., & Benford, R. (1992). Master Frames and Cycles of Protest. In A. D. Morris (Ed.), *Frontiers in social movement theory* (pp. 133–155). New Haven, Conn.: Yale University Press.

Steiger, S., Harnisch, S., Zettl, K., & Lohmann, J. (2018). Conceptualising conflicts in cyberspace. *Journal of Cyber Policy, 3*(1), 77–95.

Steinberg, A. N. (2009). An Approach to Threat Assessment. In E. Shahbazian, M. J. DeWeert, & G. Rogova (Eds.), *NATO Science for Peace and Security Series C. Harbour Protection Through Data Fusion Technologies* (pp. 95–108). Dordrecht: Springer Netherlands.

Steinberg, J. B., & O'Hanlon, M. E. (2014). *Strategic reassurance and resolve: U.S.-China relations in the twenty-first century.* Princeton, NJ: Princeton Univ. Press.

Stone, J. (2013). Cyber War Will Take Place! *Journal of Strategic Studies, 36*(1), 101–108.

Stubbs, J., Menn, J., & Bing, C. (2019, June 26). Special Report: Inside the West's failed fight against China's 'Cloud Hopper' hackers - Reuters. *Reuters.* Retrieved July 23, 2019, from https://uk.reuters.com/article/uk-china-cyber-cloudhopper-special-repor-idUKKCN1TR1DC.

Stubbs, M. (1997). Whorf's children: Critical comments on Critical Discourse Analysis (CDA)' in Evolving models of language. In A. Ryan & A. Wray (Eds.), *British studies in applied linguistics: Vol. 12. Evolving models of language. Papers from the annual Meeting of the British Association for Applied Linguistics held at the University of Wales, Swansea, September 1996* (pp. 100–116). Clevedon, England: British Association for Applied Linguistics in association with Multilingual Matters.

Sullivan, L. & Schuknecht, C. (2019). *As China Hacked, U.S. Businesses Turned A Blind Eye.* Retrieved July 24, 2019, from National Public Radio: https://www.npr.org/2019/04/12/711779130/as-china-hacked-u-s-businesses-turned-a-blind-eye.

Sutter, R. G. (2010). *U.S.-China relations: Perilous past, uncertain present* (Third edition). Lanham, Boulder, New York, London: Rowman et Littlefield.

Takala, R. (2015). *OPM breach forces CIA agents out of Beijing.* Retrieved July 23, 2019, from Washington Examiner: https://www.washingtonexaminer.com/opm-breach-forces-cia-agents-out-of-beijing.

Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2009). Risk-Based Criticality Analysis. In C. Palmer & S. Shenoi (Eds.), *IFIP Advances in Information and Communication Technology: Vol. 311. Critical Infrastructure Protection III. Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, USA, March 23-25, 2009, Revised Selected Papers* (pp. 35–49). Berlin, Heidelberg: Springer Berlin Heidelberg.

Theohary, C. A. (2018). *Information Warfare: Issues for Congress.* Congressional Research Service. Retrieved March 14, 2019, from https://fas.org/sgp/crs/natsec/R45142.pdf.

Thomas, P. (1997, November 07). CNN - Experts prepare for 'an electronic Pearl Harbor' -. *CNN.* Retrieved October 24, 2018, from http://edition.cnn.com/U.S./9711/07/terrorism.infrastructure/.

Thomas, T. L. (2012). *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker.* Fort Leavenworth.

Tikk-Ringas, E. (Ed.) (2015). *An IISS strategic dossier. Evolution of the cyber domain: The implications for national and global security : an IISS strategic dossier* (First published November 2015). London: Routledge.

Twomey, C. P. (2013). The Military-Security Relationship. In D. L. Shambaugh (Ed.), *Tangled titans. The United States and China* (pp. 235–255). Lanham, Md.: Rowman & Littlefield.

United Nations (1945). Charter of the United Nations: 1 UNTS XVI.

United States Code of Federal Regulations (2018). Theft of trade secrets: Section 18 U.S.C. § 1832.

Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion.* New York, NY: Oxford University Press.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: cyber conflict in the international system.* New York: Oxford University Press.

Valeriano, B., Maness, R. C., & Jensen, B. (2017). *Codebook for the Dyadic Cyber Incident and Dispute Data Version 1.1,* from Brandon Valeriano: http://www.brandonvaleriano.com/books.html.

van Dijk, T. A. (1993). Principles of Critical Discourse Analysis. *Discourse & Society, 4*(2), 249–283.

Varghese, S. (2019). *German industry group says evidence needed for Huawei ban.* Retrieved March 14, 2019, from ITWire: https://www.itwire.com/security/85769-german-industry-group-says-evidence-needed-for-huawei-ban.html.

Varonis (2018). *Data Under Attack:: 2018 Global Data Risk Report.* Retrieved July 24, 2019, from https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf.

Walker, L. (2015). *U.S. Backpedals on Blaming China for Massive Government Hack.* Retrieved July 24, 2019, from Newsweek: https://www.newsweek.com/us-backpedals-blaming-china-massive-government-hack-356286.

Watts, G. (2019, April 16). Hidden dangers of China's Cybersecurity Law. *Asia Times.* Retrieved July 24, 2019, from https://www.asiatimes.com/2019/04/article/hidden-dangers-of-chinas-cybersecurity-law/.

Weiner, R. & Hawkins, D. (2018). *Hackers stole federal workers' information four years ago. Now we know what criminals did with it.* Retrieved July 23, 2019, from Washington Post: https://www.washingtonpost.com/local/public-safety/hackers-stole-feds-information-four-years-ago-now-we-know-what-criminals-did-with-it/2018/06/19/f42ff2b2-73d3-11e8-805c-4b67019fcfe4_story.html?utm_term=.7b82cd68a10a.

Welna, D. (2015). *In Data Breach, Reluctance To Point The Finger At China.* Retrieved July 23, 2019, from National Public Radio:

https://www.npr.org/sections/parallels/2015/07/02/419458637/in-data-breach-reluctance-to-point-the-finger-at-china?t=1563877248903.

The White House (2015). *Fact Sheet: President Xi Jinping's State Visit to the United States.* Washington. Retrieved July 23, 2019, from The White House: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

The White House (2017). *National Security Strategy of the United States of America.* Washington, D.C.: The White House. Retrieved March 14, 2019, from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

The White House (2019). *Executive Order on Securing the Information and Communications Technology and Services Supply Chain | The White House.* Retrieved July 24, 2019, from The White House: https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

Whittaker, Z. (2014). *U.S. government to Yahoo: Comply with PRISM, or we'll make sure you go bankrupt | ZDNet.* Retrieved July 24, 2019, from Zdnet: https://www.zdnet.com/article/u-s-government-to-yahoo-comply-with-prism-or-well-make-sure-you-go-bankrupt/.

Widdowson, H. G. (1998). The Theory and Practice of Critical Discourse Analysis. *Applied Linguistics, 19*(1), 136–151, from https://academic-oup-com.ezproxy.lib.gla.ac.uk/applij/article-pdf/19/1/136/9741619/136.pdf.

Wikileaks (2017). *Vault7 - CIA Hacking Tools Revealed.* Retrieved July 24, 2019, from Wikileaks: https://wikileaks.org/ciav7p1/.

Williams, R. D. (2018). *The 'China, Inc.+' Challenge to Cyberspace Norms* (Aegis Series Paper No. 1803). Stanford, California: Hoover Institution, Stanford University. Retrieved March 13, 2019, from

https://www.hoover.org/sites/default/files/research/docs/williams_webreadypdf1.pdf.

Wodak, R. (2011). Critical Linguistics and Critical Discourse Analysis. In J. Zienkowski, J.-O. Östman, & J. Verschueren (Eds.), *Handbook of Pragmatics Highlights. Discursive Pragmatics* (pp. 50–70). Amsterdam: John Benjamins Publishing Company.

Wueest, 2. (2017). *Attackers are increasingly living off the land.* Retrieved July 23, 2019, from Symantec: https://www.symantec.com/connect/blogs/attackers-are-increasingly-living-land.

Xie, E. (2019). *China made rulings on 40 per cent more intellectual property cases in 2018 - a key area of tension in relations with U.S.*. Retrieved July 24, 2019, from South China Morning Post: https://www.scmp.com/news/china/politics/article/3001407/jump-number-intellectual-property-cases-handled-chinas-courts.

Xu, L. (2017). *Cyberspace Security: Trends, Conflicts and Strategic Stability.* Retrieved October 26, 2018, from China Institute of International Studies: http://www.ciis.org.cn/english/2017-11/10/content_40064730.htm.

Yan (2019, May 12). China Focus: Foreign-invested enterprises benefit from China's IPR protection - Xinhua | English.news.cn. *Xinhuanet.* Retrieved July 24, 2019, from http://www.xinhuanet.com/english/2019-05/12/c_138051361.htm.

Yang, Y. (2019, March 08). Chinese foreign minister Wang Yi backs Huawei's U.S. lawsuit. *The Financial Times.* Retrieved March 14, 2019, from https://www.ft.com/content/176e6dda-4174-11e9-b896-fe36ec32aece.

Yang, Y., & Bland, B. (2018, December 21). Who is the Chinese group blamed for cyber attacks on the west? *The Financial Times.* Retrieved July

23, 2019, from https://www.ft.com/content/9ecc3232-04fa-11e9-99df-6183d3002ee1.

Yin, R. K. (1981). The Case Study Crisis: Some Answers. *Administrative Science Quarterly, 26*(1), 58.

Yin, R. K. (2003). *Case study research: Design and methods* (3. ed.). *Applied social research methods series: Vol. 5*. Thousand Oaks, Calif.: SAGE.

Zhu, Z. (2006). *U.S.-China relations in the 21st century: Power, transition and peace* (1. publ). *Politics in Asia series.* London: Routledge.

Zhuang, P. (2016, November 07). China pushes through cybersecurity law despite foreign business fears. *South China Morning Post.* Retrieved July 24, 2019, from https://www.scmp.com/news/china/policies-politics/article/2043646/china-pushes-through-cybersecurity-legislation-heavily.