UNIVERSITY
OF OSLO

Master thesis

Information as a Key to Power:

Reframing Chinese Cyber Operations as a Tool for Decision Advantage

Mathilde Israelsen

Spring 2023

Master Program in Peace and Conflict Studies

Department of Political Science

Faculty of Social Sciences

University of Oslo

Word Count: 30 291

Abstract

Private cyber security companies have predominantly described Chinese cyber operations as information gathering. The existing literature in political science on cyber operations, however, have largely ignored this aspect of the phenomenon. Instead, the focus has been on the potentially destructive effects of cyber operations on digital systems and what this might mean for international politics. This thesis takes a more holistic view, seeking to establish to what extent Chinese cyber operations in the context of the South China Sea region align with the Chinese government's publicly stated policy objectives.

To illuminate this research objective, I develop a theoretical framework to categorise cyber operations as either decision advantage, compellence, or brute force. I draw on numerous sources of information to create a data set of likely Chinese cyber operations between 2014 and 2023. I apply the framework to this data and find that most incidents classify as information extraction.

My findings show that Chinese cyber operations align well with their foreign policy. I infer the extent of alignment between cyber operations and policy by connecting the target of the operations and the effect applied to digital systems to the context in which the operations occurred. The research design presents an embedded case study to capture this logic of inference. The overall conclusion is that China collects information through cyber operations to obtain decision advantage, understood as a means of reducing the uncertainty of other states' intentions in international politics.

The implications of my findings are twofold. Firstly, it underscores the need to analyse the alignment between cyber operations and policy. Secondly, it stresses the necessity of studying cyber operations as an instrument to achieve decision advantages more broadly. My work highlights the importance of developing a more nuanced understanding of the utility of cyber operations in international relations.

Acknowledgements

I want to express my sincere gratitude to Torbjørn Kveberg at the Defence Research Institute (FFI) for valuable guidance, constructive feedback, and encouragement during the work on this thesis. I would also like to thank my co-supervisor Ilaria Carrozza from Peace Research Institute Oslo (PRIO), for her contributions and insights during this process. Their knowledge and expertise have enriched the quality of this thesis.

I would also like to direct a heartfelt expression of gratefulness to our stellar social and academic community at Peace and Conflict Studies at the University of Oslo. I am thankful for all the suggestions and comments on my thesis during our workshops. The past two years have been a wonderful experience.

And finally, of course, a warm thank you to my friends and family for heaps of hugs, encouragement, care, and patience during this process and every year preceding it.

All mistakes are entirely of my very own making.

Mathilde Israelsen
Blindern, May 2023

Table of Contents

1 Introduction

A fierce debate on the utility of cyber operations in international relations has been raging for the past 30 years (see Ronfeldt and Arquilla 1993). This academic debate has mainly revolved around the value of cyber operations in warfare, whether cyber operations can be applied to achieve effects of coercion or deterrence towards adversaries, or how cyber operations can be used to achieve strategic objectives of warfare without violent state action (see i.e., Borghard and Lonergan 2017; Harknett and Smeets 2020a; Nye 2011). Yet, few studies have analysed how cyber operations align with a state's foreign policy objectives. In particular, there is a gap in the literature on how cyber operations can support a state's publicly stated foreign policy goals. This thesis seeks to evolve our understanding of cyber operations' utility in international politics by analysing the alignment of Chinese cyber operations to publicly stated foreign policy objectives. Taking this as a starting point, this thesis will seek to answer the following question:

> *To what extent do Chinese cyber operations in the context of the South China Sea region align with the Chinese government's publicly stated policy objectives?*

The research objective is important for four reasons. The first relates to the overarching literature: if we want to understand the utility of cyber operations in international relations, it is vital to illuminate how cyber operations relate to foreign policy objectives. The second relates to China in particular: China has been declared the second strongest cyber power in the world (Voo, Hemani, and Cassidy 2022). Therefore, it is essential to create a more nuanced understanding of Chinese cyber activity. Moreover, China has engaged in conflicts over territory in the South China Sea for decades (see i.e., McGregor 1993; Storey 1999). Therefore, understanding the utility of cyber operations is valuable because it exemplifies how cyber operations plays out in international conflict situations. The fourth reason concerns the scope of this thesis: delimiting the research objective to China and the South China Sea makes it possible to analyse the highly complex phenomenon of cyber operations while at the same time including of the contextual conditions surrounding it.

Chinese cyber operations have predominantly been described as information gathering, by retrieving files from systems or surveillance of systems (see i.e., Bermejo, Huang, and Lei 2017; Check Point Research 2020; Fraser et al. 2019; Insikt Group 2021; Symantec 2023).

This activity diverges from a widespread focus on cyber operations that cause destructive or disruptive effects to systems (see i.e., Borghard and Lonergan 2017; 2021; Buchanan 2016; Buchanan and Cunningham 2020; Fischerkeller and Harknett 2017; Kello 2017; Libicki and Tkacheva 2020; Lindsay and Gartzke 2018). The main focus of the literature has resulted in a gap on how to understand cyber operations as information extraction.

To provide a solution to this gap, I develop a theoretical framework to categorise cyber operations as decision advantage, compellence, or brute force and apply it to original data collected for the period between 2014 and 2023. The theoretical framework is developed with common effects that malware may create in digital systems as a reference point. Malware is a program the intruder installs on a system to change its functionality. The effect can range from information extraction by retrieving files or conducting surveillance to more disruptive or destructive effects, such as taking down the system or deleting or deleting files. Information extraction is understood as an activity conducted to achieve a decision advantage. Disruptive and destructive effects are understood as activities to achieve either compellence or brute force.

Taken together, I approach the topic in several innovative ways. Firstly, I ask an original question of how cyber operations align with broader foreign policy objectives. Despite the interest in the utility of cyber operations in international politics, there needs to be more research on the relationship between policy and cyber operations. Secondly, I develop a theoretical framework that encompasses a more nuanced understanding of cyber operations compared to existing theories. Thirdly, I apply this framework to an original dataset developed to allow for a more empirically grounded analysis compared to a large portion of the previous research on cyber operations.

In the analysis, I find that the overall character of Chinese cyber operations is information extraction. This activity in the South China Sea region fits well with publicly stated policy objectives. As a result, Chinese cyber operations can be understood as an effort to collect information to obtain a decision advantage. The core of this activity is that China gathers information to reduce the uncertainty of other states' intentions, consequently gaining an advantage in relations to other states.

1.1 Theoretical Framework

Successful intrusions into systems create effects by deleting files, modifying the system's functionality, or blocking access. Additionally, it could result in the exfiltration of files or the surveillance of activity on the system. I develop a theoretical framework to analyse cyber operations as decision advantage, compellence, or brute force. The perspective of decision advantage is a novel contribution to the field and builds on intelligence literature. Decision advantage is achieved when a state has access to private information about other states' intentions and capabilities. This situation reduces uncertainty, resulting in a higher degree of outcomes in line with the state's policy objectives (Sims 2022). Compellence is achieved through the threat of harm to redirect their current course of action or to take an action that the initiator of the cyber operations prefers (Schelling 2008). Brute force achieves desired outcomes directly by reducing the adversary's strength by denying access to information or taking down systems to induce confusion or panic in the target (Schelling 2008; Siedler 2016). Overall, these categories of cyber operations are understood as means of controlling or shaping outcomes of international relations in your favour.

1.2 Research Design

To better understand how Chinese cyber operations align with their policy objectives, I create a scheme to classify cyber operations as either information extraction, compellence, or brute force and apply that to an original dataset of cyber operations. This framework, in turn, is discussed against the backdrop of Chinese policy in the same time frame. The extent of alignment between these observations is inferred by connecting the target chosen for intrusion and the effect applied to the system to the context in which these operations occurred. The research design presents an embedded case study to capture this logic of inference. The case study has been described as an analysis of a contemporary phenomenon within its context (Yin 2009, 18). Cyber operations are the phenomenon, and policy objectives are regarded as the context in which the phenomenon occurs. The research design is chosen because placing the phenomenon in its context is vital to answer the research objective of finding out whether policy and practice are aligned. The embedded aspect of the research design is introduced through one case but multiple units of analysis. These units will be called cyber units, understood as the actors conducting cyber operations.

The dataset includes cyber operations conducted by cyber units in the South China Sea region. The process of gathering information has included establishing which actors were active in the region in the given period and retrieving information on specific activities conducted by the different cyber units. The main source of information on these activities are private security companies, which offer security solutions to computer systems. These security companies use different names to mean the same actor. Therefore, collecting information on Chinese cyber operations included merging information on aliases for the same actor used by different companies.

This information collection resulted in a list of 50 incidents of cyber operations from 2005 to 2023. While limited in size, no previous study has approached this topic in such a comprehensive way (see i.e., Harknett and Smeets 2022; Lindsay and Gartzke 2018). Instead, existing research has focused on theoretical concepts, referring to specific incidents of cyber operations to support a theoretical argument (see i.e., Lindsay and Gartzke 2018; Nye Jr. 2016; Smeets 2018). Consequently, the dataset is an attempt to broaden the empirical scope by systematically including all the openly available information on Chinese cyber activity in the South China Sea region. The period between 2014 and 2023 yielded the most detailed information on cyber activity. Accordingly, the analysis will award more in-depth attention to this period.

1.3 Case Selection

The thesis focuses on analysing China as a case study for several reasons. Firstly, China has been described as the second strongest cyber power in the world (Voo, Hemani, and Cassidy 2022). If we assume that cyber operations are a source of power through increased influence, it becomes essential to deepen our understanding of how China employs this source of power in relations with other states. Secondly, South-East Asia emerged as the primary target for cyber operations in 2022, with 31% of all cyber operations reported in that area (IBM Security X-Force 2023, 7). The South China Sea region is also described as a region of heightened conflict. By examining Chinese cyber activities in this region, we can gain insights into the application of cyber operations toward countries with whom China shares an antagonistic relationship.

Furthermore, publicly available information provided by private security firms reveals that Chinese cyber activities deviate from the prevailing understanding found in the majority of the existing literature (see i.e., Bermejo, Huang, and Lei 2017; Check Point Research 2020; Fraser et al. 2019; Insikt Group 2021; Symantec 2023). These companies characterise Chinese cyber activity as espionage or intelligence operations, primarily focused on retrieving information through file extraction or surveillance of the systems. Consequently, examining Chinese cyber operations in the context of the South China Sea can shed light on an alternative perspective on how states engage in cyber operations. The need for an alternative perspective gains further support from previous research indicating that the destructive potential of cyber operations is limited. For instance, increasing the effectiveness of cyber operations makes them more easy to be detected (see Maschmeyer 2021). This research underscores the need to explore state activities in cyberspace that involve information extraction.

1.4 Structure of the Thesis

The thesis is structured in the following way. Firstly, I will introduce some technical details of cyber operations that I will use as a reference point for the theoretical framework. Secondly, I present the theoretical framework I have developed, consisting of decision advantage, compellence, and brute force. Thirdly, the research design and case selection are presented. The research design introduces the logic of the analysis, the strategy of the embedded case study, and the case selection of China in the South China Sea. The research design chapter also introduces some reflections on issues connected to drawing inferences based on the openly available empirical material on Chinese cyber operations. Lastly, the analysis is presented, followed by a section on suggestions for future research.

2 Means of Intrusion in Cyber Operations

Any analysis of cyber operations requires understanding some technical details. The following section will introduce the technical details of cyber operations that this thesis will use as a reference point. Cyber operations, in general, start with an intrusion into a computer or system. An intrusion could be achieved using a range of methods. A commonly used technique is to introduce malware to the system. Malware is designed to modify how a system functions or to gain access to the computer or system without authorisation. Actors, who have access to significant resources may develop customised malware with a specific system or program in mind. However, there are also malware programs that are publicly available. These are often developed with a widely used program in mind, such as Microsoft Outlook.

Malware functions by exploiting vulnerabilities in the system. Computer systems are complex and comprise of multiple software components and layers of defence. Each component and layer are designed to prevent unauthorized access. However, vulnerabilities can exist within these components and layers. A vulnerability could be a programming error, a design flaw, or a configuration oversight. These vulnerabilities provide entry points for malware to penetrate the system's defences. The exploitation of vulnerabilities is accomplished by writing a malware program that may inject malicious code into software, taking advantage of a flaw in how the application handles input. Once the injected code is executed, the intruder may control the system. This control may result in the ability to induce an effect on the systems, such as deletion modification of files or programs, blocking access to the system, or shutting down the system. Blocking access and shutting down the system could be achieved by consuming a lot of the system's resources, thereby causing the system to slow down or crash. If the system has crashed of slowed down, it will make it difficult or impossible to use the system. Alternatively, the malware could function by modifying or disrupting the system's normal operations. Moreover, the malware may give the intruder access to extract data from the system or conduct surveillance of the system.

A widely used method to gain access to a system is called phishing. The central tactic consists of sending files containing the malware program to email addresses associated with the specific system targeted for an intrusion. The malware is installed on the system if the recipient opens the file. Social engineering is often used to execute this technique, wherein the attacker sends an email from a trusted address and uses a convincing topic written in a

familiar language. The attacker can analyse the victim's contacts and previous email exchanges to craft a message that appears authentic and attach a malicious link to the email (Maybaum 2013). Phishing as a method of gaining control over a system or computer accounted for over 80 per cent of the cyber operations analysed by Check Point Research in 2020 and 2021 (Check Point Research 2022, 36).

A second common technique consists of uploading malware onto web servers and tricking users into downloading it onto their computers. With this technique, a successful intrusion can be accomplished by sending emails containing the download link or redirecting users to a customised website that installs the malware on the target system. This method is commonly called a "drive-by compromise" (Maybaum 2013). A third common intrusion technique consists of exploiting weaknesses in a service provider’s infrastructure or systema to gain access to the clients connect to or reliant on that service provider. A service provider can refer to an organization that offers services such as internet connectivity, cloud services or any other service that is used by multiple customers. Service provider as valued targets because their clients may include entities in government, research, or critical infrastructure. This technique is commonly referred to as "supply-chain compromise" (Microsoft 2022). And lastly, intrusions can also be facilitated by the abuse of valid user credentials. This technique enables access to systems without the use of malware but rather through valid usernames and passwords (CrowdStrike 2023, 10).

Having successfully exploited a target system or gained access to the system due to misconfigurations, user mistakes, or valid credentials, the malicious actions intended to be carried out on the target system may require the installation of additional software. Typically, this software is a Remote Access Tool (RAT) that creates a "backdoor" for the attacker to gain control over the system. To be effective, the RAT must be installed discreetly and persistently and be resilient to patches and new software installations, ensuring that it remains undetected by the system's users. Using the RAT, the attacker can establish a command-and-control structure, enabling them to submit commands to the target system by communicating with the RAT. This communication can be concealed within legitimate network traffic, reducing the risk of detection (Maybaum 2013).

Based on how malware can be configured to affect systems in certain ways, this thesis will include a twofold understanding of an incident of a cyber operation. As mentioned above, the

effect could either be the deletion of files, the modification of a system's functionality, or the blocking of access, or it could result in data extraction or surveillance of the system. Based on these technical details, cyber operations are understood as a means to employ disruptive or destructive effects on a system *or* a tool to extract information, such as transferring or copying data or taking screenshots, or by conducting surveillance on systems by, for example monitoring data traffic or capturing the keyboard inputs made by a computer user. One incident of a cyber operation is understood as an attempt to implant these effects on a system. Furthermore, an important characteristic is that an incident of a cyber operation is an intrusion conducted by an actor who gains unauthorised access to systems. In this thesis, this type of actor is referred to as a "cyber unit". The combined set of incidents of cyber operations that these actors initiate is referred to as cyber unit activity. When a set of cyber units is said to work as a part of a state entity or as a contractor of a state entity, the combined incidents of these cyber units are referred to as state cyber activity.

To clarify, I will present the following definitions of central terms that will be used in this thesis.

Table I

Term	Description
Incident of Cyber Operation	Unauthorised access to a system or computer with the aim of retrieving information or implementing an effect.
Information Extraction	Exploit vulnerabilities to extract files, key-log or conduct surveillance of a system.
Disruption	Exploit vulnerabilities to consume a lot of the system's resources, thereby causing the system to slow down or crash.
Destruction	Exploit vulnerabilities to delete or modify files or programs on the system.
Denial	Exploit vulnerabilities to disrupt the systems normal operations.
Cyber Unit	The actor conducting cyber operations, in some cases as a part of a state entity or as a contractor of a state.

Cyber Unit Activity	The combined set of incidents conducted by a specific Cyber Unit.
State Cyber Activity	All the combined incidents of cyber operations attributed to Cyber Units acting on behalf of a specific state.

3 Literature Review

The literature on cyber operations has moved through several waves. In the following sections, I explore each of the debates that characterise the literature on cyber operations. The initial focus in the literature was the potential of cyber operations to create devastating effects on critical infrastructure and thus become a central aspect of modern warfare (Clarke and Knake 2010; Goodman 2010; Lynn 2010; Nye 2011). Subsequently, a discussion on the relevance of traditional strategic concepts, such as deterrence, coercion, escalation, and the security dilemma, became central focal points. The common denominator in all the contributions is that the main effect of cyber operations is regarded as disruption or destruction (Borghard and Lonergan 2017; 2021; Buchanan 2016; Buchanan and Cunningham 2020; Fischerkeller and Harknett 2017; Gartzke and Lindsay 2015; Harknett and Fischerkeller 2019; Kello 2017; Libicki and Tkacheva 2020; Lindsay and Gartzke 2018; Nye 2017).

The pessimistic conclusion of the feasibility of strategic concepts was developed parallel to a turn towards an alternative understanding of cyber operations as a form of covert action (see Devanny, Martin, and Stevens 2021; Gartzke and Lindsay 2015; Rovner 2019; Stout and Warner 2018; Warner 2019). A unifying characteristic of most of these contributions is that they focus on cyber operations as a form of disruption, meaning that cyber operations should and will create some kind of detrimental effect, such as denying access to a system, deleting files, or changing the functionality of a system. These are central loci points for describing how and why cyber operations will influence relations between states.

3.1 An Alarmist Debate

The first article on the utility of cyber operations in international politics was published in 1993 (Ronfeldt and Arquilla 1993). In this article, the authors define a “cyber war” as a situation characterised by targeting systems of information and communication through disruptive or destructive cyber-attacks (Ronfeldt and Arquilla 1993, 45). This perspective was extended when the debate became more active around 2010. The beginnings of this academic debate were focused on what I choose to call an alarmist debate. This early theorising envisioned cyber conflict as warfare. The literature centred around the potential for physical destruction of critical civil and military infrastructure, where conventionally weaker adversaries could severely threaten the civil and military infrastructure of a stronger state. The central assumption was that a low-cost/high-reward calculus would characterise conflict

through cyberspace. Accordingly, given the numerous potential vulnerabilities that might be exploited, a defence would be almost impossible to achieve. Following this logic, the offence would hold the advantage in cyberspace. The main implication of this assumption was a fear of destructive attacks, paralysing critical civilian and military infrastructure. Former US Deputy Secretary of Defense William J. Lynn summarised this perception in the following terms: "A dozen determined computer programmers can, if they find a suitable vulnerability to exploit, threaten the United States' global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target" (2010, 98–99).

Others echoed cyber operations' destructive potential. Clarke and Knake (2010) pointed to a potential change in asymmetrical warfare, where small states could bring strong powers to their knees through cyber-attacks. Small states would get a change to challenge stronger states due to the possible of a surprise attack because battle preparation in cyberspace would not be visible. Moreover, the authors included a description of a hypothetical scenario with severe physical consequences as a result of cyber-attacks. The catastrophic depiction involved aircraft colliding, trains derailing, and nuclear plants shutting down (Clarke and Knake 2010). Since the offence was presumed to hold an advantage in cyberspace, deterrence was identified as the best strategy to avoid escalation. Goodman (2010) argued that deterrence would be possible to achieve if states identified and communicated clear thresholds for acceptable activity in cyberspace. As a part of this strategy, states should communicate the consequences that would follow from stepping over the boundary of acceptable activity (Goodman 2010, 128–29)

Nye (2011, 19) argued that analysts needed to understand how lessons from cyber operations fit into strategic concepts such as offence, defence, deterrence, coercion, escalation, and arms control. Therefore, he argues that there was a need for developing concepts in strategic theory as technology developed further. With the presumed destructive potential of cyber-attacks in mind, he emphasised that research into cyber conflict could learn from nuclear research. Therefore, Nye argued that the analyst should focus on the core strategic concepts of nuclear theory, such as deterrence, coercion, and the potential for escalation. The main reason for this was a perception of cyber operations as an alternative to strategic nuclear competition.

3.2 A Theoretical Turn

A range of scholars answered the call made by Nye in the following years, and a new wave of literature was subsequently developed. I regard the core of this branch of the literature as concerning how cyber operations will influence adversaries, send signals about intentions, and the potential effects of those signals. Central concepts are the potential for deterrence (Borghard and Lonergan 2021; Fischerkeller and Harknett 2017; Kello 2017; Nye 2017), coercion (Borghard and Lonergan 2017; Gartzke and Lindsay 2015; Lindsay and Gartzke 2018), and escalation, either deliberately, but also inadvertently through security dilemma dynamics, misperceptions, and vulnerabilities (Buchanan 2016; Buchanan and Cunningham 2020; Harknett and Fischerkeller 2019; Libicki and Tkacheva 2020; Lin 2012).

Kello (2017) explores the feasibility of deterrence in cyberspace. He posits that deterrence by denial is hard to achieve but that deterrence through punishment has more promising prospects (2017, 197–98). Deterrence through denial could concern building a strong defence, resulting in a higher cost than rewards for the adversary in the case of an attack. Deterrence through punishment, however, involves signalling intentions to hurt the adversary in the event of an attack, significantly increasing the cost of the attack for the adversary. The main argument is that states can threaten to retaliate against the adversary with conventional or nuclear weapons to achieve cross-domain deterrence – deterrence by punishment across different strategic domains (Kello 2017). Relatedly, Nye (2017) theorises how deterrence by punishment could be technically possible in cyberspace by and of itself. While others pointed to the difficulty of attribution in cyberspace – the assumption that the characteristics of cyberspace would hide the perpetrator, making it almost impossible to point them out – as an obstruction of efficient signalling of intentions (Borghard and Lonergan 2017), Nye contends that these issues are not severe enough to stop efficient deterrence by denial. An improved defence will increase the cost of an attack, thus reducing the incentives of this act (Nye 2017).

Related to the discussion on deterrence is the discussion on the possibilities for coercion in cyberspace. Borghard and Lonergan (2017) emphasise the attribution problem in their discussion about the feasibility of coercion and signalling in cyberspace. Their argument is founded in the critical premise of coercion-theory that communication is essential to achieve this strategic objective (see Schelling 2008). Since states do not necessarily know who was behind the cyber operations, they cannot communicate intentions of retaliation to the state behind the incident (Borghard and Lonergan 2017).

The same perception is supported by Gartzke and Lindsay (2015). They contend that the lack of openly available information on attribution limits the possibility of using cyber operations as a tool for strategic signalling. Therefore, the possibility of coercing adversaries in cyberspace will be limited (Gartzke and Lindsay 2015). The same researchers extended their argument to the cost-benefit calculation, which is central to coercion theory. The cost-benefit calculation states that the threat must be perceived as costly for the receiver of the threat (see Schelling 2008). Lindsay and Gartzke (2018) argue that the value of the target of a cyber operation will be unknown. Accordingly, the unknown value will create insecurities over the potential impact of the threat on the cost-benefit analysis of the party receiving the threat. Consequently, the insecurity of the potential impact of the threat creates obstacles to using cyber operations as a coercive tool toward another state (Lindsay and Gartzke 2018).

Borghard and Lonergan (2019) end up with a different conclusion regarding the potential of coercion in and through cyberspace. They demonstrate that cyber power alone has limited effectiveness as a tool of coercion, although it has significant utility when coupled with other elements of national power. Central to the theory of coercion is the cost-benefit analysis of the party that will potentially receive an attack. Borghard and Lonergan highlight that critical infrastructure is a common target of attacks. However, since not all pieces of critical infrastructure are universally valued across states, cost-benefit analysis on the part of the attacker will not be feasible. Consequently, the attacker cannot know the true value of the target. Furthermore, since coercion is unlikely due to the unknown value of the target, a spiral of escalation is unlikely to occur from conflict in cyberspace (Borghard and Lonergan 2019, 461).

The literature on the potential for escalation in cyberspace concerns the difficulty of discerning the intentions behind an attack. Lin (2012) assumes no direct contact between states conducting cyber operations. The lack of direct contact makes it difficult to determine the intent behind an adversary's actions. Therefore, attempts to send signals to an adversary through limited military action are likely highly problematic. The absence of direct contact between adversaries may prompt decision-makers to take a worst-case view of the situation rather than await more information. He contends this dynamic could trigger a spiral of inadvertent escalation (Lin 2012, 57–58).

Buchanan (2016) mirrors the assumption of a lack of direct contact in cyberspace and connects this to the aspiration of states to keep the options open for future cyber operations. Keeping options open might involve training operators, which could be compared to actions included in a traditional security dilemma (2016, 48). Buchanan elaborates on this mechanism further by noting that the discovery of such actions may be perceived as a threat because it could suggest that a state is enhancing its ability to launch an attack. This situation creates a dilemma of interpretation as the intruding state could be preparing for an imminent attack, simply developing contingency options, or may have no intention to attack at all (Buchanan 2016, 49). Contrastingly to a spiral of inadvertent escalation, Libicki and Tkacheva (2020) conceptualise cyber escalation as evolving like a lattice, allowing horizontal spillovers to other domains and vertical movement corresponding to greater intensity of the conflict.

3.3 The "Absolute Weapon" Demystified

Despite the focus on traditional concepts of strategic theory, cyber wars have remained hypothetical. Parallel to the development of the discussion on the applicability and relevance of the theoretical concept of strategic theory in and through cyberspace, several contributions highlighted the lack of empirical evidence of a cyber revolution. They emphasised that cyber operations seemed to fall short of their promise of significantly altering the character of warfare and conflicts short of war. This characteristic is why I have chosen to highlight a demystification of an "absolute weapon", where severe effects could be implemented towards adversaries with little detrimental consequences to the initiator. As a starting point for this discussion, the destructive effect of cyber-attacks, described as the central characteristic of cyberspace in the early literature, was deemed unlikely. These contributions highlighted that there had been no surprise attacks, strategic strikes, or escalation due to state actions in the cyber domain (Gartzke 2013; Rid 2012; 2013).

Gartzke (2013) argues that what he describes as cyberwar cannot achieve conquest or coercion. The main argument is that cyber operations have not constituted a large strategic threat. Rather, as Gartzke concludes, "Even the most successful forms of cyberwar (such as cyber espionage) do not presage much of a transformation" (2013, 73). The contradiction to the doomsday scenarios depicted above, Gartzke contends that "In grand strategic terms, it [cyberwar] remains a backwater" (2013, 72). Furthermore, he presses that the internet is an ineffective replacement for terrestrial force regarding coercion and conquest. Therefore,

cyberwar should not be seen as the final determinant of competition and should not be considered in isolation from conventional forms of political violence (Gartzke 2013, 42).

The main argument of Rid (2013) is that cyber activity has remained below the threshold of war. He characterizes the historical instances of cyber operations up until 2013 in three categories: sabotage, espionage, and subversion. Rid thus argues that cyber war has not and will not occur. The backdrop for this argument he connects to Carl von Clausewitz's three criteria for war as violent, instrumental, and political. According to Rid, no cyberattack meets all of Clausewitz's three criteria. Instead, Rid concludes all political cyber-attacks, both past and present, are merely sophisticated variations of three activities that have been present in warfare for centuries: subversion, espionage, and sabotage (Rid 2013, 5).

Mahnken (2011) gives a similar analysis as Rid on actions in cyberspace, drawing on the same elements. He states that cyber-attacks will not result in direct fatalities, and their capacity to cause damage on a larger scale is limited (Mahnken 2011, 58). Thus, he concludes that cyber operations *alone* will not deliver victories in future conflicts. However, in conjunction with other means of violent action, he points out that cyberspace should be regarded as an important enabler of more lethal forms of warfare (Mahnken 2011, 61).

In a similar vein as Mahnken, Libicki (2009) notes that cyberattacks that support a conventional operation may be of limited significance for the success of that operation. He strongly argues that cyber war will not occur in the future. This argument is supported by comparing cyber-attacks to airstrikes. Airpower is often successful when societies believe the situation can only get worse. With cyberattacks, the opposite effect may occur. As systems are attacked, vulnerabilities are exposed and subsequently repaired or routed around. However, as systems become more resilient, societies become less vulnerable and are more likely to resist further coercion (Libicki 2009, xv).

In the aftermath of the detection of the Stuxnet operation against a nuclear uranium enrichment facility in Natanz in Iran, several articles argued more specifically against the plausibility of a cyber revolution in warfare. The worm installed in the systems managed to speed up the centrifuges, and the fast-spinning motion caused them to burn themselves out. In light of Stuxnet, Liff (2012) sets up a different framework for assessing cyberwar as Rid (2013) and Gartzke (2013), but arrives, to a large extent, at the same conclusion: it is unlikely

that cyberwarfare is the new "absolute weapon". Instead, he contends that there are very limited circumstances under which cyber operations could be used as an efficient tool for states to pursue political and military objectives. He concludes that while Stuxnet demonstrated the potential of cyber operations as a brute force measure, there is no clear example of effective and indisputable coercive or destructive cyber operations (Liff 2012, 426).

Stuxnet is also used by Lindsay (2013) as an analytical point of departure. He argues that Stuxnet provides evidence for an alternative viewpoint on cyber operations, where militarily weaker actors can gain an asymmetric advantage. Additionally, the complexity of weaponisation of cyber operations makes cyber offence less easy and defence more feasible than what was commonly believed at the time (Lindsay 2013, 365). He concludes that just because minor attacks are easy to mount in cyberspace does not mean that attacks on critical infrastructure are also easy (Lindsay 2013, 402). In a later article, Lindsay repeats his argument – that the empirical record of cyberattacks features no major damage (Lindsay 2017).

Parts of the literature argue against the perception that cyberspace is an environment where the offence has the advantage of the defence and that this – coupled with aspects such as the attribution problem – generates risks for inadvertent escalation. For instance, Borghard and Lonergan (2019) highlight mechanisms that limit escalation. One mechanism is that the option for retaliatory offensive cyber operations may not exist at the desired time of employment, and even under conditions where they may exist, their effects are uncertain and often relatively limited. Another mechanism is that the option for cross-domain escalation – responding to cyber operations with conventional capabilities – is unlikely to be chosen except in rare circumstances. The reason, they highlight, is the limited potential for applying severe costs through offensive cyber operations. Therefore, the operation's cost will not justify retaliation through conventional capabilities.

This unlikelihood of escalation after a cyber operations is echoed in the main findings of Valeriano et al (2018). In a study of cyber operations and responses between 2000 and 2014, they find that rivalling states typically react to lower-level cyber incidents, and the response usually tends to contain the intrusion instead of seeking escalation dominance. Most instances of cyber escalation are at a relatively low level of severity and do not lead to escalation

(Valeriano, Jensen, and Maness 2018, 76). Arguing for more nuance in the offence-defence calculus of cyberspace, Slayton (2017) contends that the claims that cyberspace heralds an offensive advantage are misguided. Slayton concedes that the complexity of information technology offers the offence advantages over the defence. However, she argues that the offence-defence balance in cyberspace is a result of a dyadic balance, not a systemic balance. It is, therefore, not a result of the technical characteristics of cyberspace but rather the relative skill of adversaries and the relative complexity of their goals (Slayton 2017, 74).

Furthermore, empirical studies have documented the insignificant influence of cyber operations in conventional warfare. In a study of the wars in Ukraine in 2014 and Syria in 2011, Kostyuk and Zhukov (2019) found that in Ukraine, which is one of the first armed conflicts where both sides incorporated cyber tools, cyber activities failed to create visible changes in battlefield behaviour (2019, 317). They concluded that cyber-attacks are an ineffective tool of coercion in conventional warfare. They argued that the findings showed that the "cyber war" had unfolded in isolation from the rest of the conflict (Kostyuk and Zhukov 2019, 74).

3.4 The Strategic Utility

In recent years parts of the literature have circled what I term the strategic utility of cyber operations. Parts of this literature (Egloff and Shires 2021; Smeets 2018) argue that strategic aims that were previously achieved through violent state actions can be achieved more efficiently by integrating cyber capabilities. The main idea is that cyber operations could complement force, increasing its effectiveness. A different section of this literature argues that cyber operations are an effective instrument in conflicts short of war, changing the structure of conflicts between states (Buchanan 2020; Harknett and Smeets 2020b; Harknett and Fischerkeller 2019; Kello 2017; Warner 2019). While this literature focuses on the disruptive and destructive elements of cyber operations, they do not deem it to be able to, for example, cripple the entire critical infrastructure of a country. Hence the focus is on cyber operations as a compliment to force and as an instrument in conflict short of war rather than as an instrument of war directly.

Egloff and Shires (2021) propose two ways states could integrate cyber operations into violent state action: as instead of and as a substitute for violence. They argue against the

conception that a state's offensive cyber capabilities can reduce state violence. Rather, due to an expanded definition of violence away from lethal bodily harms toward social and community harms, the authors argue that offensive cyber capabilities relocate, rather than reduce, state violence toward non-bodily harms (Egloff and Shires 2021, 19). The authors argue against parts of the literature that regard cyber operations as non-violent according to a physical definition of violence. Expanding the concept of violence, they argue, adds analytical value by providing a way to describe different forms of behaviour, both violent in a traditional sense and non-violent. In short, they expand the scope of harm that could be realised through cyber operations by deepening the analytical concept of violence (Egloff and Shires 2021).

The main argument of Smeets (2018) is that cyber operations could provide significant strategic value to states. Smeets does not try to describe or explain past cyber operations but aims to provide the conditions under which cyber operations can be effectively conducted. These conditions are threefold: (i) as an extra option for state leaders, (ii) effectiveness will be increased if it is used in conjunction with conventional military capabilities, and (iii) offensive cyber operations can be used to achieve some form of psychological ascendancy. The core of the argument is that cyber operations can be used to achieve strategic aims without the use of military violence (Smeets 2018).

Furthermore, contributions to the literature have highlighted that the strategy of deterrence falls short of its promise in cyberspace. Rather, states should persistently employ cyber operations against adversaries. The assumption is that this strategy could result in a shift in the balance of power without having to resort to the use of force. Fischerkeller and Harknett (2019) argue along these lines when they argue for a shift from a focus on cyber operations that threatens to cause physical damage to more continuous strategic competition without the resort to an armed attack. The authors introduce two concepts to explain the dynamics of state activity in cyberspace: persistent engagement and agreed competition. They assume that the central characteristic of cyberspace is constant contact, which entails that actors in cyberspace can only defend systems in the moment. Consequently, you cannot undermine future attacks through a constant defensive structure, compared to defence against traditional threats, such as nuclear weapons. The consequence of the assumption of constant contact is that actors in cyberspace must aim to hold a persistent initiative through continuous operations. A consequence of this situation is that persistence is the central dynamic in cyberspace. The authors argue that the dynamic of persistent engagement foresters an additional dynamic of

agreed competition, where adversaries continuously launch operations on each other to achieve a persistent initiative. The authors conclude that this dynamic best explains the situation in cyberspace rather than spiralling escalation. The central conclusion is, therefore, that the central dynamic of interaction in cyberspace does not warrant concern over escalation (Harknett and Fischerkeller 2019).

The same view is echoed in Harknett and Smeets (2020b). They argue that cyberspace has opened a new dimension of power politics in which cyber campaigns could become significant means for achieving strategic advantage without the resort to war (2020b, 2). Their main argument is that strategy must be separated from the presumption that it deals only with coercion, militarised crisis, and war in cyberspace. Cyber competition is strategic because of an underlying intent to shift the relative balance of power between states (2020b, 2). Therefore, the article argues that instead of focusing on whether a cyber operation can constitute warfare, research should move attention to cyber operations as part of a coherent cyber campaigns. They define such campaigns as "a series of coordinated cyber operations, which takes place over time, to achieve a cumulative outcome leading to a strategic advantage" (Harknett and Smeets 2020b, 8).

3.5 A New Theoretical Turn

The literature up until this point has focused on cyber operations as means to disrupt the functionality of systems, delete files, or deny access to systems. The discussion has circled how these detrimental effects on computers and systems can affect relations between states. In recent years, however, a part of the literature has shifted from a focus on concepts of strategic theory towards an understanding of cyber operations as intelligence operations and covert action. I consider the main perspective in this literature to be that cyber operations mainly constitute covert meddling in adversaries' affairs to achieve a desired outcome directly (see Devanny, Martin, and Stevens 2021; Gartzke and Lindsay 2015; Rovner 2019; Stout and Warner 2018; Warner 2019; Maschmeyer 2021). In this literature, a specific focus on China is introduced. The reason for this is that Chinese actions deviate from expectations developed through research on other state actors and have therefore been deemed an ideal case for studying this perspective of cyber operations.

According to Maschmeyer (2021) cyber operations are considered subversive actions. This entails covert intervention in the affairs of adversaries, with the objective of achieving specific goals directly. The main characteristic of subversion is its secretive and indirect nature. As a result, Maschmeyer argues that cyber operations are limited in their effectiveness across three key variables. Firstly, cyber operations are characterised by slow operational speed. This is the time required from starting an operation until it produces effects (Maschmeyer 2021, 67). Secondly, the secret and indirect nature of cyber operations constrains the intensity of effects, which is considered to be the severity of effects towards an individual target and the number of targets that are affected (Maschmeyer 2021, 55). Lastly, efforts to maintain secrecy and exploit systems, limit control. This effort is described as the extent of control an intruder can achieve over a targeted system and the effects it can produce through a system (Maschmeyer 2021, 64). These effects pose a trilemma for actors because the three variables are negatively correlated, which means that a gain in one variable tends to result in losses across the other two (Maschmeyer 2021, 51).

Rovner (2019) argues that most activities in cyberspace have little to do with the use of force. Rather, they are characterised as an intelligence contest. He emphasises five aspects of an intelligence contest to draw connections to cyber operations. Firstly, it is a race among adversaries to collect more and better information. Secondly, it is a contest to improve the state's relative position. Thirdly, it is an effort to undermine the adversary's morale and institutions. Fourthly, it is an effort to disable adversaries' capabilities through sabotage. And lastly, it is a campaign to prepare assets for intelligence collection in the event of a conflict. Rovner highlights that China is especially active in what he describes as "the race for information". He understands China's main effort to concern the theft of intellectual property, with an additional focus on other kinds of political and military information. Rovner does not complement this perspective with any theoretical development on the utility of cyber operations in international relations.

Other scholars have echoed the same perspective on Chinese activity in cyberspace (Cunningham 2022; Gilli and Gilli 2019; Lindsay 2015a; Lindsay, Cheung, and Reveron 2015; Valeriano, Jensen, and Maness 2018). Cunningham's (2022) analysis circles how China gathers information through espionage, seeking to substitute its technology and information systems with those of foreign countries. The analysis concludes China aims to enhance its power and control by stealing information, and emphasises that this activity represents a

significant challenge to the domination of the United States and Western countries in technological development. Gilli and Gilli (2019) have the same point of departure, highlighting that China is conducting large-scale espionage operations in the quest for intellectual property. The conclusion on the strategic effects of the espionage operations differs from Cunningham's. They argue that the complexity of modern military technology creates severe organizational restraints, making it difficult to imitate weapons systems. Consequently, free riding on research and development in other states is difficult, limiting the ability to overcome the technology gap through method of stealing intellectual property.

A similar argument is presented by Lindsay et.al (2015). The main argument is that China is running what they describe as an “aggressive industrial espionage campaign”. The conclusion is it is difficult to transfer the technology from its localised context, despite the access to information. The implication is that it is challenging to absorb the technology, leading to imitation rather than innovation. Similarly, Valeriano (2018) argues that China’s approach to cyberspace is closely linked to its technology gap strategy, with China using cyberspace to acquire foreign technology and intellectual property. The theft of intellectual property has implications for global power dynamics, with China challenging the dominance of Western countries in this area.

3.6 Research Gap

This thesis will answer the following question: To what extent do Chinese cyber operations in the context of the South China Sea region align with the Chinese government’s publicly stated policy objectives? The analysis of this question will contribute to the literature in four novel ways.

Firstly, the research question asks for alignment between policy and practice. Despite 30 years of debate on the utility of cyber operations in international politics, there is a gap in the literature on how cyber operations align with a state’s foreign policy objectives. As the literature review showed, the academic debate has discussed the value of cyber operations in warfare, whether cyber operations can be used as coercion or deterrence, or how cyber operations can be used to achieve strategic objectives of warfare without violent state action. This thesis seeks to evolve our understanding of the utility of cyber operations in international

politics by exploring the extent to which Chinese cyber operations align with publicly stated foreign policy goals.

Secondly, building on the new theoretical turn described above, the thesis will incorporate perspectives from intelligence studies. Most of the existing literature has been based on security and war studies, as highlighted by the strong focus on strategic concepts and strategic feasibility. However, I find that to study cyber operations we need to incorporate perspectives from both intelligence and security studies. This approach is based on two findings in the literature. Firstly, the existing perspectives cannot fully describe China's activity through cyber operations. Secondly, according to the findings of Maschmeyer (2021), the effectiveness of destructive or disruptive operations on systems is limited. The contribution of Maschmeyer is important because it illuminates the need to widen the focus from the disruptive and destructive aspects of cyber operations.

Consequently, there is a need to adopt a new perspective on cyber operations, prioritising the extraction of information over disruption or destruction. Malware customised to steal information, so-called “infostealers”, accounted for 21 percent of global cyber operations in 2021, and 30 per cent in of the cyber operations in the South China Sea region, according to the cyber security company Check Point Research (2022, 35–36). The high usage of infostealers shows that information extraction is a central aspect of state activity in cyberspace, yet the literature on cyber operations has largely overlooked this activity. Therefore, in this thesis I will add new understanding to information extraction in cyberspace by building on the perspective of cyber operations as intelligence. This perspective will be introduced including the decision advantage in the theoretical framework (see Sims 2022).

Nevertheless, achieving disruptive or destructive effects through cyber operations is possible. Therefore, to understand state activity in cyberspace more comprehensively, I will build on a dual understanding of activity in cyberspace. On the one hand, the extraction of information, and on the other hand, the potential of disrupting the functionality of systems, the destruction of files, or the denial of access by blocking or shutting down the system. Limiting the analysis to one of these perspectives presents a danger of limiting the capacity to explain the phenomenon of cyber operations. The disruptive and destructive activity is understood as either compellence or brute force, which will be introduced in the theoretical framework.

Thirdly, the analysis transfers the empirical emphasis toward cyber unit activity. The empirical emphasis in previous research has been on specific incidents of cyber operations (i.e., Lindsay and Gartzke 2018; Smeets 2018) and technical characteristics of cyber intrusions and systems (i.e., Borghard and Lonergan 2019; Gartzke and Lindsay 2015; Nye Jr. 2016). As will be argued later in the thesis, incorporating cyber unit activity will increase the amount of available information in a field of research plagued by a limited amount of openly available information. Chinese cyber units will be included as units of analysis. The combined incidents of cyber operations of these actors are referred to as cyber unit activity. The choice of this unit of analysis will be elaborated on in the research design.

Lastly, the thesis broadens the analytical scope to encompass China and the neighbouring states in the South China Sea. The existing literature on Chinese activity has mainly focused on the transfer of information on the development of technology to China, with a specific focus on intrusions into the systems of US-based companies and research institutes. This approach overshadows Chinese cyber units' activity in neighbouring countries, where the state holds a strong strategic interest. The South China Sea has been characterised as a region with a heightened level of conflict (i.e., McGregor 1993; Valencia 1988). My choice of focusing the analysis on the South China Sea region enables the thesis to analyse how Chinese cyber units act in the context of heightened territorial conflict. Consequently, this introduces an alternative perspective to the research on Chinese cyber unit activity.

4 Theoretical Framework: Cyber Operations as a Source of Influence

As highlighted in the research gap section, there is a need to introduce perspectives on information extraction to cover a broader range of cyber activity. By concentrating solely on one aspect of strategic theory, such as coercion, there is a danger of neglecting a significant portion of the activity. By developing a theoretical framework based on two categories of common effects from malware infection on systems, this thesis aims to introduce a framework that considers the range of cyber activity. As was highlighted above, the two common categories of effects involve either disruption of the functionality of a system, destruction or modification of files or denial of access, *or* extraction of information by exfiltrating data or conducting surveillance of the system.

This chapter is divided into the following sections. First, building on intelligence literature, a perspective of cyber operations as a means to achieve a decision advantage is developed. Second, a perspective of cyber operations as economic espionage is incorporated, which also builds on the extraction of information from a system. Third, a perspective of cyber operations as a means to achieve a compellent effect, meaning to make the adversary change its course of action, is detailed. Lastly, I detail a perspective of cyber operations as an instrument of brute force applied to achieve direct consequences. Compellence and brute force are assumed to be the intent behind more disruptive or destructive effects on systems.

This thesis will understand cyber operations as a means of exercising influence in international politics. Summarising the chapter, decision advantage denotes a situation where a state has achieved a reduced level of uncertainty about other states' intentions and capabilities because it has access to private information about these aspects through the exfiltration of information. The reduced level of uncertainty could lend a hand in developing more efficient policies toward other states, resulting in a higher degree of outcomes in line with the state's policy objectives. Compellence exerts influence through the threat of pain or harm on an opponent to redirect their current course of action or to take an action that the initiator regards as desired. Brute force exerts influence by creating effects in a system to achieve a desired outcome directly. Combined, these approaches understand cyber operations a source of influential power, where influence is understood as a means to control or shape outcomes in your favour.

4.1 Decision Advantage through the Extraction of Information

Building on intelligence literature, I develop a novel understanding of the intentions behind the extraction of information from systems. The literature has stated that this activity takes the shape of intelligence. However, this thesis contributes to this literature by incorporating concrete theoretical perspectives from the broader intelligence literature. The extraction could take the shape of intelligence, surveillance, or industrial espionage. The aim of information extraction could be to alleviate the uncertainty related to other states' actions. By alleviating the uncertainty inherent in state relations, the actor can achieve a decision advantage. Therefore, the descriptive activity of information extraction is analysed through the theoretical perspective of decision advantage.

Even though intelligence activity spans several hundred centuries, a clear definition has been lacking. Michael Warner offers the following definition: "Intelligence is secret, state activity to understand or influence foreign entities." (2002, 7). He elaborates this approach by stating that intelligence has the following four characteristics. Firstly, it is dependent upon confidential sources and methods for full effectiveness. Secondly, it is performed by state officers for state purposes, which implies that those officers receive direction from the state's civilian and military leaders. Thirdly, it is focused on foreigners—usually other states, but often foreign subjects, corporations, or groups. Lastly, it is involved in influencing foreign entities by means that are unattributable to the acting government. If the activities are open and declared, they are the sphere of diplomacy; if they utilise uniformed members of the armed forces, they belong to the military (Warner 2002, 7).

Intelligence gathering could create a situation in which one state possesses more information than the adversary. More specifically, the state knows more about the adversary's decision-making than the adversary knows about the state's decision-making. This asymmetry in knowledge leads to a situation where the state with most knowledge has less uncertainty in decision-making processes relative to the opponent. This situation means that the state has more options than the opponent and the capacity to choose among them with greater certainty, timeliness, and impact. This dynamic has been described as a decision advantage. By having a decision advantage, decision-makers are able to anticipate and respond to threats and opportunities more effectively and gain an edge over their adversaries in various domains (Sims 2022).

The same insights have been mirrored in other contributions. Wheaton and Beerbower (2006, 329) regard intelligence as "a process, focused externally and using information from all available sources, that is designed to reduce the level of uncertainty for a decision". The purpose of intelligence is, therefore, to reduce the level of uncertainty to the minimum possible. Betts (1978, 69) echoes this notion when by stating that it is the role of intelligence to extract certainty from uncertainty and to facilitate coherent decisions in an incoherent environment. Furthermore, the same observation is also maintained by Lowenthal (2017, 4, 7). He holds that intelligence exists to support the policy-making process by providing background, context, and assessment of actors' intentions, their likely action, and their capabilities in various areas.

The position that information will reduce uncertainty is mirrored in theoretical perspectives on international relations. The central implication of a lack of information is uncertainty. Specifically, this uncertainty arises from a lack of access to private information. Private information has two facets influencing state relations: the intentions and capabilities of other states (de Mesquita, Morrow, and Zorick 1997). Intentions have been understood as the willingness to use force. States have incentives to misrepresent this information to gain better deals, and states are not privy to information about the concessions adversaries are willing to make (Fearon 1994, 586). Turning the logic of Fearon, access to private information could – theoretically – reduce the need for states to communicate their intentions through public actions such as troop mobilisation and threats (Fearon 1994, 586).

Furthermore, information extraction could alleviate the uncertainty of other states' capabilities and aid in strengthening the state's capabilities by extracting information on technology development. The latter could be achieved through economic espionage, which is a government's effort to steal knowledge and appropriate trade secrets with the interest of protecting or expanding their national economies. Economic espionage could involve extracting information on other states' businesses or technological development programs, usually those of critical industries such as electronics, aerospace, defence, or biotechnology (Nasheri 2004, 12, 17). Drawing on the Correlates of War project (Singer 1988; Singer, Stuart, and Stuckey 1972) capabilities could be understood as resources in the military, economy, and population. These resources could be turned into a threat to other states or used to defend the state. Economic espionage could therefore be regarded as an effort to retrieve knowledge on other states' capabilities and, more broadly, to strengthen the capabilities of the

state relative to other states.

Overall, the thesis will understand the aim of intelligence activity as achieving a decision advantage. This advantage could aid in developing policies and actions that strengthen the state's ability to influence situations to its own advantage. These actions and policies could be military, political, or social. Decision advantage is achieved by retrieving private information on the capabilities and intentions of other states. Access to this information could have two effects. Firstly, to aid in strengthening the state's position relative to other states by improving the state's capabilities. This advantage would be achieved through information extraction from foreign companies and states to increase knowledge about their capabilities and also to facilitate technology transfer to aid in strengthening relative to others. Secondly, to reduce the uncertainty following unknown intentions and capabilities of other states, aiding in developing a future course of action towards the same states.

4.2 Disruption, Destruction, and Denial

An intrusion into a system can disrupt the system's functionality, cause destructive effects through the deletion of files or the shutdown of the entire system, or denial of access. In direct terms of the system, these effects can be regarded as more detrimental than the extraction of information. This thesis incorporates a perspective of disruption, destruction, and denial to achieve compellent effects or brute through cyber operations. The descriptive activity of disruption, destruction, and denial is therefore analysed through the analytical perspectives of compellence and brute force. In summary, compellence is a threat of harm to force the adversary to change its course of action, while brute force is understood as a means to achieve an objective directly, by shutting down or blocking access to a system.

4.2.1 Compellence

Compellence is one part of Schelling's (2008) concept of coercion. The second aspect is deterrence. The discussion on the potential of deterrence using cyber operations has been comprehensively discussed in the literature. Deterrence is understood as a threat to keep an adversary from starting an action by fear of harmful consequences (Schelling 2008, 69). However, a wide-ranging conclusion has been that deterrence is not a feasible approach in cyberspace (i.e., Borghard and Lonergan 2021; Fischerkeller and Harknett 2017; Lindsay

2015b; Nye 2017; Soesanto and Smeets 2021). Consequently, this thesis will focus solely on the potential for compellence through cyber operations.

Compellence is a threat intended to make an adversary do something or change a course of action it has already started. The success of compellence relies on three conditions. Firstly, for compellence to be successful, it depends on the cooperation of the party receiving the threat. The actor must actively decide to change a source of action due to the threat (Biddle 2020, 98). Secondly, compellence must be definite. Without a set timeline, the party receiving the threat will have no incentive to change how it acts (Biddle 2020, 102). The third condition relates to communication of the intent to inflict damage or pain. Commonly, communication appears through an action itself. Successful communication of a threat is a core condition for compellence. Without communication, the central mechanism of influencing the other party's behaviour cannot be achieved (Biddle 2020, 103).

An objection to the feasibility of coercion through cyber operations has been the difficulty of credible signalling of harm. This difficulty has been connected to the timeline for conceding to demands, clear communication (Lindsay and Gartzke 2018, 25), and the difficulty of causing sufficiently severe consequences through cyber operations (Siedler 2016, 33–34). The conclusion on the first two limitations – the timeline and communication – is connected to the secret nature of cyber operations. This characteristic of cyber operations has been emphasised as creating difficulty in clearly attributing cyber operations. The consequence is that conditions cannot be legitimately put forward in the action because the target is not supposed to know who was responsible for the incident (Lindsay and Gartzke 2018, 17).

However, the attribution problem– knowing who did it – is not as severe as some scholars have feared (i.e., Rid and Buchanan 2015). Consequently, attributing cyber operations to specific states could lead to increased credibility of threats. The main reason is that the target will know which state was behind an incident, increasing the perception of the potential for future harm. Therefore, attribution increases the awareness of the initiator's intentions toward the target by accumulating knowledge on the systems the initiator is interested in targeting. This awareness could strengthen the compellent effect by creating a perception of threat with the target (i.e., Singer 1958, 94).

The main reason for the limitation of causing sufficiently severe consequences is related to the process of achieving a successful intrusion in a cyber operation. The process of intrusion circles the exploitation of vulnerabilities in a system. When a vulnerability has been exploited, it alerts the victim to that vulnerability, consequently giving time to improve the defence of the system. Consequently, the credibility of future harm could be reduced because the same vulnerability cannot be exploited in several incidents (Siedler 2016, 31). However, there is uncertainty connected to the level of knowledge that an intruder could possess on potential vulnerabilities in a system. Cyber operations are appearing in large quantity, despite potential vulnerabilities being uncovered at a high pace. This implies that sophisticated cyber powers are applying large resources to uncover vulnerabilities in systems that could be applied in a successful intrusion into a system. Identifying and exploiting previously unknown vulnerabilities – so-called zero-day vulnerabilities – is a key tactic in this effort. Cyber units are adept at leveraging these vulnerabilities, and the implication of this is that cyber operations are still occurring at a high rate (Microsoft 2022, 39).

The capability for exploiting vulnerabilities is a part of private information in international relations. This means that the information is kept secret from other states. This could create a high level of uncertainty about how much harm this capability could create in the future, which subsequently could strengthen the credibility of future harm. Accordingly, Schelling's assumptions of credibility could be regarded as valid in and through cyber operations. The uncertainty of the capability of exploiting vulnerabilities could make the target expect that there is more harm to follow. This increases the insecurity of the potential harm the initiator could create, increasing the perception of the threat it imposes on the target's digital systems.

Furthermore, the compellent potential of action should be analysed considering the context in which it occurs. For example, at the time of the discovery of Stuxnet in 2010, which involved sabotaging a nuclear reactor in Iran, there was a perception that cyber operations could cause significant harm to critical infrastructure (i.e., Clarke and Knake 2010). The Iranian government could not know if it was the beginning or the end of a string of cyber operations and how much potential it hurt central elements of critical infrastructure. This perception of threat could have caused a compellent effect. The perception of threat leads to an argument on the credibility of the threat tied to the context. According to Schelling, credibility depends on the target's expectations (Schelling 2008). Adapting Schelling, this should be understood as

contextual credibility. This entails that the promise of coercion must always be analysed from the perspective of the relationship between the initiator and the target at a given time.

In summary, compellence through disruptive or destructive cyber operations could be understood from the following assumptions. The core of compellence is a threat to inflict harm. The fundamental idea is that this threat will induce the target to change its course of action. One source of credibility for this threat is an uncertainty of the knowledge of vulnerabilities that the initiator possesses. This uncertainty creates credibility of future harm. Furthermore, attributing cyber operations to states could strengthen the perception of future harm, increasing the credibility of the threat. This is especially important when numerous cyber operations against a target are attributed to a specific state.

Additionally, the compellent threat should be analysed in the context in which it is occurring. The perception of threat will be stronger in one context compared to another. This is understood as contextual credibility. Overall, the central assumption of compellence through cyber operations is connected to the uncertainty of future harm. The target cannot know when and where it will occur and how severe the consequences will be. This creates credibility of a threat to inflict pain.

4.2.2 Brute Force

Brute force, or forcible action, concerns the adversary's strength, not its interests. More specifically, brute force is concerned with overcoming the adversary's strength (Schelling 2008, 3). In contrast to compellence, brute force requires no cooperation. More precisely, it is limited to actions that can be accomplished without adversary collaboration (Schelling 2008, 80). Instead, the actor simply takes what he wants. Shelling compared this to a tank or bulldozer, which can simply "Force its way, regardless of others' interests" (Schelling 2008, 3). Schelling wrote that the actions an actor can take without adversary cooperation are constricted to "repel and expel, penetrate and occupy, seize, exterminate, disarm, and disable, confine, deny access, and directly frustrate intrusion or attack" (Schelling 2008, 1).

Siedler (2016) adapts these assumptions to cyber operations. The analysis interprets brute force as a direct reduction of the adversary's strength, achieved by seizing or holding by force. This approach is seen as a way to impose limitations, restricting the target's capabilities to a

greater or lesser extent. Such limitations may involve disabling or denying access to valuable data, temporarily impeding the target's ability to access critical information. Additionally, it could entail the complete takedown of systems, not only temporarily restricting access to information but also causing confusion and potentially inducing panic within the targeted entity. Particularly in situations of heightened conflict, this effect alone may interest the intruder. From this perspective, cyber operations can be seen as a means for an actor to achieve their objectives directly without necessarily considering the actions of the target (Siedler 2016, 25).

Compared to compellence through cyber operations, brute force could be understood as more relevant as preparation for an increased level of conflict or as preparation for war. The main reason is that it focuses on reducing the adversary's strength, which could directly aid in a situation of increased conflict. For example, denying access to information at a crucial time could give the intruder valuable time for starting other courses of action toward the adversary. In this situation, the main interest of the intruder is to confuse or create panic, thereby creating an upper hand as the conflict situation is initiated. Therefore, the thesis will understand brute force as especially relevant in situations of increased conflict.

5 Research Design and Case Selection

This thesis asks the following research question: To what extent do Chinese cyber operations in the context of the South China Sea region align with the Chinese government's publicly stated policy objectives? To better understand how Chinese cyber operations align with their policy objectives, I combine the theoretical framework developed in the previous chapter with an original dataset on cyber operations. This, in turn, is discussed against the contextual backdrop of Chinese policy in the same time frame.

The chapter is divided into three sections. First, I present the overall research design, which consists of an embedded case study and the case selection. The embedded case study consists of a context, case, and units of analysis. The chosen context is the South China Sea region, the case is China, and the units of analysis are cyber units conducting cyber operations. Second, I explain in detail how I gather, analyse, and interpret empirical data of various kinds to conduct the analysis. As described above, the empirical information consists of the cyber activity of Chinese cyber units and Chinese policy objectives in the South China Sea. Third, I present some reflection on issues with drawing inferences based on likely biased empirical material.

5.1 Research Design

I infer (dis)alignment between policy objectives and cyber operations by comparing observations of cyber operations to publicly available policy objectives by establishing the context in which the cyber operations occur. If Chinese cyber operations in the South China Sea region align with their publicly available policy objectives, then the activity could be understood as a method of influencing the outcome in favour of Chinese objectives. Whether the cyber activity aligns with policy objectives is established by placing a specific cyber operation in the context in which it occurred. This is achieved by highlighting the target chosen for intrusion (i.e., a government entity or a company) and the specific time of the intrusion. Based on these contextual conditions, the analysis will infer whether the specific cyber operation is aligned with Chinese policy objectives. The empirical material ranges from 2005 to 2023. However, the range of more detailed empirical material is from 2014 to 2023. Consequently, the analysis will focus on this period.

Effects of cyber operations are classified as either information extraction, disruption, or destruction based on information on how the implanted malware functions in the system. If the incident of a cyber operation is classified as information extraction and the target is aligned with policy objective, then the theoretical analysis will understand this activity as a method to achieve a decision advantage in relation to the targeted state. If the activity is classified as disruption or destruction and the target is aligned with policy objectives, then the theoretical analysis will infer the motive to be either brute force or compellence based on the context in which the operation occurs. The reasoning behind this is that the observed effect is similar and must be compared to the context in which it occurs to be established. If a pattern between observations of cyber operations and observation of policy objectives is established, it could support an understanding of cyber operations as a source of influential power, where influence is understood as a means to control or shape outcomes in your favour, irrespective of the wishes of the opponent. This would be regarded as a positive finding in the analysis.

Conversely, a negative finding would be that cyber operations do not align with Chinese publicly stated policy objectives. In a study of cyber operations in Ukraine and Syria, Kostuyk and Zhukov (2019), found that cyber activity from both sides was used in isolation from the overarching warfare. Negative findings could be regarded as plausible when transferring this finding to activity conducted by Chinese cyber units. In practical terms, a negative finding would mean that cyber activity is not occurring in step with policy objectives. For example, if there is a period of heightened tension or conflict, I would expect cyber operations to mirror the policy objectives of that period for it to be regarded as a positive finding. Undoubtedly, there is a danger of confirmation bias in relation to this, meaning that I interpret findings consistent with pre-existing beliefs. The pre-existing beliefs would, in this case, be the Chinese policy objectives that I will establish.

However, exactly because of the danger of confirmation bias, I will highlight the importance of contextualising observations – of placing a specific incident in the context in which it occurs. Contextualisation could provide the circumstantial information needed to understand observations more accurately. This could result in the ability to capture more nuance, and aid in correct interpretations of the observations. This will help in the prevention of confirmation bias by highlighting information that could serve to contradict pre-existing beliefs. The contextualisation of observations will be achieved through a strategy triangulation of sources. This approach will be explained in detail in a later section.

To capture contextual conditions, this thesis will apply an embedded case study research design. Regarding the *case*, Yin (2009, 18) has described the case study as an inquiry that investigates a contemporary phenomenon within its context, especially when the boundaries between the phenomenon and context are not clearly evident. This means that the case study should be chosen when the analysis aims to uncover contextual conditions, under the assumption that these conditions will be highly relevant to understand the phenomenon under scrutiny (Yin 2009, 18). The research question is of a descriptive kind, aiming to explore if there is an association between cyber units' activity through cyber operations and the Chinese government's policy objectives in the context of the South China Sea. The (dis)alignment between policy and practice is inferred by establishing the context in which the cyber operations occur.

Concerning the *embedded* aspect of the embedded case study design, the thesis will include a single case but multiple units of analysis (Yin 2009, 50). The units of analysis in this thesis are "cyber units", signifying the actors conducting cyber operations. The main consideration behind this choice is to establish a foundation for a systematic analysis of the activity conducted by cyber units. The choice of this unit of analysis will be elaborated in the next section.

As a final point, negative findings could serve to develop our understanding of Chinese cyber operations in two ways. Firstly, the analysis could uncover a pattern of interest in the targets chosen for intrusion. This knowledge could aid in future research on Chinese cyber operations. Secondly, it would find that Chinese cyber operations are not clearly connected to general foreign policy. This finding would show a need for future research on Chinese cyber operations as an isolated tool of state activity.

5.2 Case Selection

The case chosen for analysis in this thesis is China. Ideally, cases should be chosen through formal case selection methods to increase the potential of contributing to theory development or illuminating a phenomenon in general. However, formal case selection methods assume that cases can be selected from a large universe (i.e., Seawright and Gerring 2008). The number of cases within the research area of cyber operations with available empirical material that allows for in-depth analysis is limited. The population of analytically feasible cases

consists of China, Russia, Iran, and North Korea. This means that a formal case selection strategy is not a viable approach.

By analytically feasible, I mean cases with a sufficient level of openly available information on how cyber units operate. It does not imply that these states are the only actors conducting cyber operations. According to the 2022 National Cyber Power Index, the US, UK, Australia, Netherlands, France, and Vietnam all rank among the top ten most powerful cyber actors, along with the states listed above (Voo, Hemani, and Cassidy 2022, 9) However, the national cyber power index maps the states that are considered to have the capabilities to pursue national objectives through cyber means, and the intent to achieve a range of objectives through these means (Voo, Hemani, and Cassidy 2022, 7). The index does not, however, map the activities of these states in cyberspace. The US is listed as the most powerful cyber actor. Despite this, information on US cyber activity is insufficient to conduct a detailed analysis of the state's cyber operations (see EuRepoC 2023). Consequently, to answer the specific research question related to conducting cyber operations, the universe of analytically feasible cases is limited to China, Russia, Iran, and North Korea.

Based on this limitation, this thesis will argue that the case of Chinese cyber operations in the context of the South China Sea region is of intrinsic value to increase our knowledge of state cyber activity. There are several reasons for this. Firstly, China has been characterized as the second most powerful cyber power (Voo, Hemani, and Cassidy 2022). If we assume that cyber operations are a source of power through increased influence, it is important to increase our understanding of how China is using this source of power toward other countries. Secondly, South-East Asia has been characterised as the most targeted region for cyber operations in 2022, accounting for 31 % of all incident of cyber operations (IBM Security X-Force 2023, 7).

The South China Sea region is also described as a region of heightened conflict. An analysis of Chinese cyber activity in the region can therefore serve to illustrate how cyber operations are applied toward countries with which a state has an antagonistic relationship. However, despite these two features, there is a research gap on the activity of China through cyberspace in this region. As the literature review illuminated, the focus on China has mainly been on Chinese cyber operations as a tool to reduce the technology gap between China and other states, specifically the United States. Consequently, to understand the potential of cyber

operations as a means of influence in international relations, it is important to broaden the scope of the research on cyber operations to encompass this region.

Consequently, the analysis will study cyber operations occurring in the littoral states in the South China Sea. These states are Taiwan, the Philippines, Brunei, Malaysia, and Vietnam. Additionally, the analysis will consider cyber operations occurring in the US that can be plausibly linked to the context of the South China Sea. The reason behind this is that the US has a strong presence in the region, which the Chinese government has strongly opposed (Yang 2021, 65).

Furthermore, openly available information from private security companies shows that Chinese cyber activity diverges from the general perception of how cyber operations are applied in the majority of the literature (see i.e., Bermejo, Huang, and Lei 2017; Check Point Research 2020; Fraser et al. 2019; Insikt Group 2021; Symantec 2023). These companies describe the activity as espionage or intelligence, based on a high level of information extraction through the exfiltration of files or surveillance of systems. Consequently, research on the analytical case of Chinese cyber operations in the context of the South China Sea could serve to illuminate an alternative perspective on how states act through cyberspace.

The need to research information extraction strengthened by the fact that previous research has shown that the destructive potential of cyber operations is limited. For example, if the level of effectiveness is increased, stealth will decrease (see Maschmeyer 2021). This illustrates a need to illuminate alternative state activity in cyberspace, encompassing the elements of information extraction. Concerning this, however, it is important to highlight that the aim of this case selection is not to contribute to a general understanding of the cyber phenomenon that can be applied to all cases but rather to deepen and broaden our knowledge of the range of which cyber operations may be applied as a tool of state foreign relations. The case should therefore be understood as serving to exemplify one aspect of the phenomenon. This understanding might not apply to Russia, North Korea, or Iran, but it will increase our understanding of how China employs these tools in a region on which it holds a strong strategic focus.

For this thesis, the chosen unit of analysis is termed “cyber units”. This term signifies an actor conducting cyber operations, the choice of this unit of analysis focuses the inquiry on the

activity of specific actors. This is a novel understanding of the unit of analysis in the cyber operations literature. The literature on the topic has mainly focused on three analytical units. Firstly, the technical characteristics of cyber operations (i.e., Borghard and Lonergan 2019; Gartzke and Lindsay 2015; Nye Jr. 2016). And secondly, specific cyber operations that have occurred (i.e., Lindsay and Gartzke 2018; Smeets 2018). Concerning the units of analysis applied to previous research, the thesis will incorporate these perspectives by utilizing the technical characteristics as a foundation for the theoretical framework. Furthermore, specific cyber operations will be included as part of the activity of the cyber units.

A third unit of analysis in previous research has been a campaign perspective, where a string of incidents of cyber operations likely conducted by the same nation-state are connected to analyse the strategic significance of the campaign. Incidents are therefore aggregated by an assumed common objective (Harknett and Smeets 2022). Private security companies commonly present their data in this perspective (see i.e., Baumgartner and Golovkin 2015; Bermejo, Huang, and Lei 2017; Glyer et al. 2020a; Kaspersky 2021; Raggi and Scenarelli 2022). The main problem is that these companies rarely unveil exactly how these incidents were aggregated to an assumed common objective. These conclusions are likely drawn from data that is not openly available but rather something they have access to owing to having customers across various sectors in multiple countries. Accordingly, I will argue in the following that cyber units are a better choice for units of analysis when conducting research into cyber operations conducted by states.

The chosen unit of analysis opens a need for a note on attribution. This term denotes how specific actors are connected to a specific state. For a long time, there was an impression of the impossibility of attributing actors in cyberspace. In some cases, this served as an important empirical characteristic of cyberspace to underscore specific theoretical argument (see i.e., Borghard and Lonergan 2017). Attribution is, however, not impossible (Rid and Buchanan 2015). Attributions of specific cyber units to states often occur, and the range of sources that will be applied in the analysis is a testament to this. These attributions are often based on four parameters: (i) the infrastructure of the intruder, as in the communication structures they are using, (ii) the malware employed in the intrusion, (iii) the target of the intrusion, (iv) and the date and /or time at which the intrusion occurred (Caltagirone, Pendergast, and Betz 2013). When following attributions of cyber units, I give direct credence to the sources with direct access to information instead of sources reporting on the analysis.

These sources are security companies with customers among the targets and state intelligence services which we can assume have access to varied information on the topic. Giving direct credence to these sources involves discounting information that states something different from the statements of the primary sources.

Private security companies use different names for what is likely the same actor. This naming convention offers an obstacle to gathering information on cyber units' activity in the region. However, it is possible to merge information. This is done from known associations in the literature and by security companies, who present aliases of the name they use when referring to the cyber units. To illustrate this point, we can take an alleged Chinese threat group known under one name as APT41 as an example. APT41 is the name given by the American security company Mandiant (Fraser et al. 2019). This company has developed a naming convention where APT stands for Advanced Persistent Threat, followed by a number for when it was discovered relative to other APT groups. Aliases of the APT41 group are BARIUM by Microsoft (McConkey et al. 2022, 29; Secureworks Counter Threat Unit 2023a), Blackfly by Symantec (Symantec 2023), Group 72 Cisco Talos (Willams, Lee, and Esler 2014), Red Kelpie by PwC (McConkey et al. 2022, 29), Wicked Panda/Spider by CrowdStrike (Meyers 2018), Bronze Atlas by Secureworks (Secureworks Counter Threat Unit 2023a) and Axiom by Novetta (Novetta Threat Research Group 2014). This group is also known as Winnti in public reporting based on the name of the malware they frequently use to infiltrate systems (Meyers 2018; Secureworks Counter Threat Unit 2023a).

By merging information on aliases, the aggregated level of empirical information increases. This creates an improved ability to analyse threat group activity over time and draw more coherent inferences on what targets and sectors they are interested in. Connecting this information to the context in which it appears, and public documents on foreign policy interests could allow for drawing valid inferences on how the Chinese government applies these cyber operations as a foreign policy tool. Some of these actors are attributed directly to Chinese government agencies. Others are assumed to be based in China. Considering the strict laws governing the use of the Internet in China and the laws that any actor must disclose information to the government on request (Creemers 2022), it is safe to assume that the government knows what is going on. This could mean that groups not directly linked to the government are used as contractors and may therefore aid in achieving government objectives. The cyber units listed in the table below will be emphasized to allow for this

analysis. These actors are chosen based on the active cyber units in the region, which is information drawn from openly available information. The character of this information is elaborated on below. The main name will refer to the cyber unit in this thesis. The aliases will be used to search for information on the activity of the cyber unit as a unified actor.

Table II

Main name	Aliases
APT41	BARIUM by Microsoft (McConkey et al. 2022, 29; Secureworks Counter Threat Unit 2023a), Blackfly by Symantec (Symantec 2023), Group 72 Cisco Talos (Willams, Lee, and Esler 2014), Red Kelpie by PwC (McConkey et al. 2022, 29), Wicked Panda/Spider by CrowdStrike (Meyers 2018), Bronze Atlas by Secureworks (Secureworks Counter Threat Unit 2023a), Axiom by Novetta (Novetta Threat Research Group 2014) and Winnti (Meyers 2018; Secureworks Counter Threat Unit 2023a).
APT10	Red Apollo by PwC (McConkey et al. 2022), MenuPass by TrendMicro (Benson and Kohei 2017), Stone Panda by CrowdStrike (Kozy 2018), POTASSIUM (Benson and Kohei 2017; Secureworks Counter Threat Unit 2023f), CVNX by BAE Applied Intelligence (Benson and Kohei 2017), Bronze Riverside by Secureworks (Secureworks Counter Threat Unit 2023f), Hogfish by iDefense (Secureworks Counter Threat Unit 2023f), Tianjin State Security Bureau (Department of Justice 2018). 22/05/2023 16:35:00
APT30	Naikon by Kaspersky (Secureworks Counter Threat Unit 2023c), Bronze Sterling/Bronze Geneva by Secureworks and Override panda by Crowdstrike (Secureworks Counter Threat Unit 2023c). 22/05/2023 16:35:00
BlackTech (Bermejo, Huang, and Lei 2017)	Bronze Canal/CTG-6177 (Secureworks Counter Threat Unit 2023b), Palmerworm by Symantec (Symantec 2020) and Shrouded Crossbow (Bermejo, Huang, and Lei 2017). 22/05/2023 16:35:00
APT27	APT27 by Mandiant, Budworm by Symantec, Emissary Panda by CrowdStrike, Iron Tiger by Trend Micro, Lucky Mouse by Kaspersky, Temp.Hippo by FireEye and Bronze Union by Secureworks (Secureworks Counter Threat Unit 2017b).

Mustang Panda	Red Lich by PwC (McConkey et al. 2022, 28), Bronze President by Secureworks, and HoneyMyte by Kaspersky (Secureworks Counter Threat Unit 2019).
Goblin Panda	Cycldek by Kaspersky (Kaspersky 2021)
APT40	Bronze Mohawk by Secureworks (Secureworks Counter Threat Unit 2023e), FEVERDREAM, GADOLINIUM by Microsoft, Hellsing by Kapersky, Kryptonite Panda by Crowdstrike, Leviathan by ProofPoint, Pickleworkm by Symantec and Periscope, Temp.Periscope and Temp.Jumper by Mandiant (CISA 2021).
APT17	Deputy Dog by Mandiant, Aurora Panda by CrowdStrike, Hidden Lynx by Symantec, Shell Crew, Tailgater Team, Bronze Keystone/TG-8153 (Secureworks Counter Threat Unit 2023d).
Chimera	Referred to Chimera in open-source information by Taiwanese company CyCraft (CyCraft Research Team 2020). Same name used in other reports on the cyber unit (Jansen 2021).
APT3	Gothic Panda by CrowdStrike (Kozy 2018), Buckeye, Pirpi, UPS Team, TG-0110/Bronze Mayfair by Secureworks (Sungbahadoor 2017).
Bronze Butler	CTG-2006/Bronze Butler by Secureworks, Stalker Panda by CrowdStrike (Secureworks Counter Threat Unit 2017a), Tick and RedBaldKnight by Trend Micro (Chen, Kakara, and Shoji 2019).
APT1	Comment Crew by Symantec (Chantzos 2010), Numbered Panda, Bronze Globe/TG-8223 by Secureworks and Byzantine Candor.

In merging information on cyber units, I have chosen a majority-based understanding of attributions. If several sources agree that one actor is the same, I follow this conclusion. The rationale behind this is that if several sources agree, it could indicate that the conclusion is based on a higher level of information, as these companies are in charge of the security solutions of separate systems. I highlight this because reports suggest an overlap between APT17 and APT41 (Hegel 2018). This means that there are indications that these actors could be the same. The reason for this is based on how attribution is conducted. If they find similarities in infrastructure or the malware employed in the intrusion, it might suggest that two cyber units are the same. However, in this case, I could not find any sources

corroborating that APT17 and APT41 are the same, and therefore I have chosen to treat them as separate units.

5.3 Empirical Information and Triangulation of Sources

As has been made evident in the section above, private security companies are one of the most important sources of information into the activity of states through cyber operations. These companies offer security solutions (e.g., antivirus protection, intrusion detection, incident management, threat intelligence) to government entities, the private sector, and businesses in various countries. Therefore, they often hold direct access to empirical information that is not available anywhere else. The analysis of Chinese cyber units' activity will therefore be based on available information on cyber operations from private security companies, combined with reports from the media in the region. This will, however, present itself with some issues, which will be highlighted below.

Whether a cyber operation is initiated for information extraction, surveillance, or more destructive purposes, such as systems take-down, or deletion or modification of files, will be based on how the implant (i.e., malware) functions within the systems. Private security companies attributing incidents of cyber operations are experts in IT security. Consequently, information on how malware functions is extensive relative to other types of information on this topic. It is, therefore, possible to classify the activity of cyber units into the specific categories of information extraction or disruption, destruction, and denial.

Classifying cyber unit activity in this way involves collecting information for an original dataset on activity by the cyber units listed above in the region (see appendix). When establishing whether an actor is active in the region, I have used the list of actors in the MITRE ATT&CK framework as a point of departure. This is a comprehensive list of all active cyber units and includes "China-based" listings (MITRE ATT&CK 2023). MITRE ATT&CK is an industry-leading framework mainly known for detailing the tactics and techniques cyber units use to infiltrate systems. Additionally, MITRE offers a page for every cyber unit, which gives access to two very useful sources of information. The first is a short list of sources describing the tactics and techniques of the groups, and the second is a list of synonyms signifying one actor. Based on this information, I searched for information on the cyber units.

During this process, two additional tools were particularly helpful. The first was the cyber operations tracker from the EU Repository for Cyber Incidents (EuRepoC). This yielded access to several reports on cyber operations occurring in the region. However, the project is in its early stages and only includes incidents that have generated attention in traditional media (see Harnisch et al. 2023). Related to cyber operations, I find this is a rather high threshold for inclusion in the analysis. The main reason for this is that cyber incidents that have resulted in attention in traditional media generally create a relatively large amount of disruption. Only including these incidents could create a skewed picture of cyber activity. Therefore, this tool was supplemented with the malware tracker from the Fraunhofer Institute for Communication, Information Processing and Ergonomics (Fraunhofer FKIE 2023). This tool offers a comprehensive list of sources of malware observations, categorized based on the names of cyber units. Since it is a list based on observations of the use of specific types of malware, the number of included incidents of cyber operations is higher. This helped me overcome a central problem when collecting information from websites. Several of the sources were found on websites that are no longer maintained. This problem could be a result of mergers of companies or simply that the site has been deleted. However, with access to saved links on the Malware Tracker, I could find the deleted information through the Internet Archive.

Collecting empirical information resulted in several reports from private security companies. Reading through these reports, I could filter out the active cyber units in the region. Moreover, reading through the reports created a snow-balling effect, leading to access to more sources on the same actors. The main strategy was to look up references and search for information whenever a report stated a synonym for the cyber units. Furthermore, after establishing synonyms and connecting this to one security company, I searched for information in annual reports from companies such as Microsoft, Mandiant, TrendMicro, SecureWorks, TrendMicro, and PwC. Knowing the name security companies use to describe one actor and whether it has been known to be active in the South China Sea region allowed me to look for additional information on the activity of one actor within a given year.

All in all, my efforts yielded a dataset of 50 cyber incidents occurring in the South China Sea from 2005 until 2023 (see Appendix). While too small a sample for meaningful statistical inference, it is a significant improvement on existing peer-reviewed articles on cyber

operations. Compared to previous research on cyber operations, this original dataset provides a more comprehensive empirical foundation for analysis of cyber operations in a regional context (see i.e., Lindsay and Gartzke 2018; Nye Jr. 2016; Smeets 2018). Consequently, the original dataset will broaden the empirical scope by including all the openly available information on Chinese cyber activity in this region in a more systematic way.

An incident can include intrusions into the systems of one target or consist of targeting of several entities. Most "incidents" in the dataset are cyber operations conducted toward one entity. However, in some cases, I have not been able to separate the information of targeting towards separate entities. The reason for this is that some sources is characterised by a certain vagueness. By this I mean that they do not disclose which entity was targeted at what time. Rather, they state that entities in particular sectors of society were targeted over a longer period. One example is that entities within the government, military, health, diplomacy, education, and politics were targeted in Vietnam in 2020 and 2021 (Kaspersky 2021). This type of empirical information illuminates what targets Chinese cyber units are interested in. However, they make contextualisation difficult. Because of this, I will go in-depth in the analysis of the incidents that give more detailed information on a separate targeted entity and the time in which the incident occurred.

The limited amount of information is a central concern that any analysis of cyber operations must deal with. I present the triangulation of sources as a solution to this problem. This will involve complementing information on cyber operations with information on the context in which they occurred. The context can be established through observations of targets and the time the incidents occurred. This is a solution to the problem because it provides a deeper and more nuanced understanding of the surrounding circumstance of cyber operations. This is helpful for three of separate reasons. Firstly, by considering the broader context, the analysis can gain a more comprehensive understanding of the subject under analysis. Secondly, it provides information that helps in interpreting incidents. Without context, the meaning or significance of certain elements may be misinterpreted or misunderstood. This is especially important considering the limited amount of information on cyber activity and could aid in preventing biased inferences. Thirdly, by examining contextual conditions, the analysis may identify patterns that emerge over time. Considering that the empirical information can be rather vague, placing the incidents in their context may provide a path to identifying trends.

Central to illuminating the research objective of how Chinese cyber operations align with policy objectives is to identify the characteristics of Chinese policy objectives in the South China Sea region. Hansen (2006) has presented a perspective on what sources are authoritative in research of foreign policy. She argues that material should be chosen in accordance with two sets of considerations. Firstly, the texts should primarily be from the period under examination. Secondly, the collection of texts should encompass key texts that are frequently cited. This means that material that is widely read and receives significant attention should be emphasised (Hansen 2006, 74).

Doshi (2021) also presents an argument for what texts should be considered authoritative, particularly in relation to China. He regards the most authoritative texts to be leader-level memoirs, doctrinal texts, archival sources, official speeches, classified materials, and essays by senior leaders. According to Doshi, they better reflect Party thinking in China than more frequently cited but less reliable sources, such as Chinese journal articles (Doshi 2021, 33). The analysis will mainly focus on the year before 2014 and up until 2023, which is a period offering more detailed information on Chinese cyber operations. The relevance of archival sources and leader-level memoirs is therefore reduced. Furthermore, classified texts and essays by senior leaders are not easily available for two reasons. The first is that the classified texts rely on leaks of this information from sources within the governments, and the second – and more important - is that I cannot read sources in Chinese.

Therefore, with these considerations as a point of departure, the characteristics of Chinese policy objectives is established through a combination of official speeches, statements, and doctrinal texts, such as government White Papers stipulating Chinese foreign policy, trade policy, or security policy and the Five-Year-Plans, stipulating the overall strategy for achieving central goals. Such texts are frequently applied to analyse CCP policy objectives and are therefore often available in a translated version. Overall, this triangulation of sources makes use of a wide range of available information. This triangulation opens up to searching for regularities. This could yield a more detailed and balanced picture of the situation.

5.4 Obstacles to Valid Inferences and Solutions to These Issues

In the section above, I have detailed an approach to gathering empirical information on cyber operations and the context surrounding cyber operations. Nevertheless, this approach does not present itself without some issues. In this section, I will highlight some issues connected to this approach and how these issues might interfere with the validity of inferences in the ensuing analysis. I will also present some solutions to the weaknesses and how these solutions could aid in establishing a stronger validity of inferences.

The method of triangulation of sources introduces some issues. A central issue is the danger of confirmation bias, which entails an interpretation of information that is consistent with pre-existing beliefs. By connecting the cyber threat activity to an established context, it is quick to conclude that the interest in a specific sector is aligned with the policy objective. The main reason for this is that the activity itself is obscured, and concrete information is limited. This is a weakness of studying cyber activity – it is shrouded in vagueness and secrecy. This is one of the reasons why the thesis asks how activity "aligns" with policy objectives. It is not possible to establish a clear connection. However, despite this, the findings that could be uncovered are valuable to broaden and deepen our understanding of how cyber operations are utilised in international relations. The thesis conducts research into a phenomenon that we lack information on. This makes it important to find answers, despite the potential biases in empirical information and the issues with drawing inferences.

Furthermore, I will highlight three issues with the empirical information collected from private security companies that must be highlighted. The core consequence of these issues is that the empirical information I have collected might not give a representative picture of Chinese cyber activity. Concerning bias, the first source is that customers of private security companies are likely wary of letting them disclose information on security breaches. A result of this is that the openly available information often applies a general name for a targeted sector rather than the specific target. An example of this is using the name "military organizations" or "government organizations" instead of the specific name of the entity in these sectors. Moreover, the names "education" or "research" is used when a university or a research institute has been targeted, rather than the specific names of these organizations. This is coupled with the country of which the target is located. Consequently, it is possible to draw information on the targeted sector in a specific country. For example, it is possible to classify a specific incident as an intrusion for the purposes of information extraction from a military

entity in Vietnam. Based on these classifications, the activity will be analysed in light of the theoretical framework and the context in which it occurs.

The vagueness in the information creates a hurdle to drawing valid inferences. This is because valid inferences rely on the ability to connect the targeting to the context in which it occurs. This is a weakness of for three reasons. Firstly, it can make it difficult to interpret the empirical information accurately. Consequences of this could either be inconsistent inferences, or it could result in difficulty of understanding the meaning of an observation, thus making it challenging to draw valid conclusions. Accordingly, I will specifically focus on activities where there is information on the time the activity occurred. The reason is that it makes it possible to contextualise the activity. While not a completely failsafe solution, it makes it possible to draw inferences on how they align with policy objectives. Still, where the information is particularly vague, this will be emphasised, and inferences will be drawn cautiously. Moreover, if several interpretations of the same observation of cyber activity are possible, this will also be highlighted.

Secondly, highly sophisticated actors could succeed in keeping the operations covert, for example by employing openly available malware (which is openly available online) or by using the established infrastructure for cyber operations of an adversary (i.e., Bartholomew and Guerrero-Saade 2016). This ability could result in the most sophisticated actors not being present in the available empirical material. For instance, the US is largely absent from available empirical material, even though they take up the top spot over a ranking of the world's strongest cyber powers (Voo, Hemani, and Cassidy 2022). The result of this could be that some countries are over-represented in openly available information. Consequently, it could create the impression that these states conduct more cyber operations than other states when this might not be the case.

Thirdly, most of the industry dominating private security companies are based in Western countries. Some of the largest companies offering security solutions are Microsoft, Mandiant (a part of Google), Symantec, and CrowdStrike. These companies inflict a strong influence on how the phenomenon of cyber operations is understood because they have access to first-hand information on the state of systems. This could result in an additional bias in the data. In 2011 the US government signalled increased strategic interest in China and the Asia-Pacific Region (Clinton 2011). This opened an important new avenue in security solutions. When private

security companies choose to highlight the activity of cyber units originating from China, it could be interpreted as a result of a need to signal to potential customers that relevant threats are of the highest priority. Therefore, the strong focus on China could result from a commercial interest in gaining more customers (FireEye 2015; 2019; Glyer et al. 2020a; Hegel 2018; Insikt Group 2017).

The second and third biases present issues to valid inferences for two reasons. First, it could present a limited perspective of cyber operations, which could be an obstacle to a comprehensive understanding of Chinese cyber operations. Second, it could emphasise a particular narrative. For example, if the empirical information is biased along the lines of a strategic focus of Western countries, the data could, for instance, be biased towards a specific target, thereby creating the impression on a stronger focus on this type of target. Combined, this creates an obstacle to the validity of inferences. Nevertheless, this thesis can only rely on openly available information, including the potential biases that could be introduced in the analysis due to relying on this information.

Nevertheless, two qualities of the research design have been introduced to remedy these issues. Firstly, the chosen unit of analysis – cyber units – is chosen to ground the analysis in a broader empirical foundation. The original dataset is one of the most comprehensive empirical foundations for an analysis of state activity through cyber operations. Secondly, the strategy of triangulation of sources gives insight into the cyber activity in its broader context. This could aid in gaining a more comprehensive understanding of the topic of the research objective. It could also aid in interpreting the incidents conducted by the separate cyber units. Due to the vagueness of the sources, the contextual conditions could strengthen the understanding of the significance of incidents, which could be overlooked if cyber operations are analysed in isolation. All in all, this could create a foundation for a more nuanced understanding of Chinese cyber operations.

Additionally, more openly available information could be a positive side-effect of the biases presented above. Compared to other cyber powers, such as the US, UK and, France (Voo, Hemani, and Cassidy 2022), there is more openly available information on the activity of Chinese cyber units. The potential bias in the empirical material resulting from the strategic focus of Western states could therefore result in more available information on the activities of Chinese cyber units. This means there is more data on the means of intrusion they use, the

targets they choose, and the effects of those intrusions. If the analysis had aimed to compare the activity of China with the US, UK or France, the bias would most likely have resulted in skewed inferences. However, the research question asks for Chinese cyber unit activity in isolation. Despite the potential bias in the material, the available information could serve to illuminate how Chinese cyber units operate. In combination with information on the context, this strengthens our ability to understand how China specifically employs cyber operations as a tool of foreign relations.

Even though the empirical material might not yield a full picture of Chinese operations, I will argue that illuminating state activity in cyberspace through the research objective of this thesis is important. The field of research on cyber operations is relatively new. By combining the theoretical framework developed in this thesis with the original dataset, I will contribute to developing innovative approaches and theories to the research on how and why states conduct cyber operations. In summary, this innovative approach has three central aspects. Firstly, I ask an original question of how cyber operations align with broader foreign policy objectives. Secondly, I shed light on this research objective by developing a theoretical framework that encompasses a more nuanced understanding of cyber operations. Thirdly, I apply this to an original dataset, which is developed to open up for a more empirically grounded analysis compared to a large portion of the previous research on cyber operations.

6 Analysis and Discussion

In this chapter, I establish Chinese policy objectives in the South China Sea region. Establishing publicly stated policy objectives creates a foundation for the extent to which policy aligns with practice. In the following, I will discuss the findings of my data collection by presenting the activity of Chinese cyber units, understood as the target chosen for intrusion and the time in which the activity occurred. The activity of Chinese cyber units is then discussed against the contextual backdrop of Chinese policy in the same period, and this is combined to determine whether policy and practice align. The activity and the contextual backdrop are then combined to discusses how the findings can be interpreted in relation to the theoretical framework.

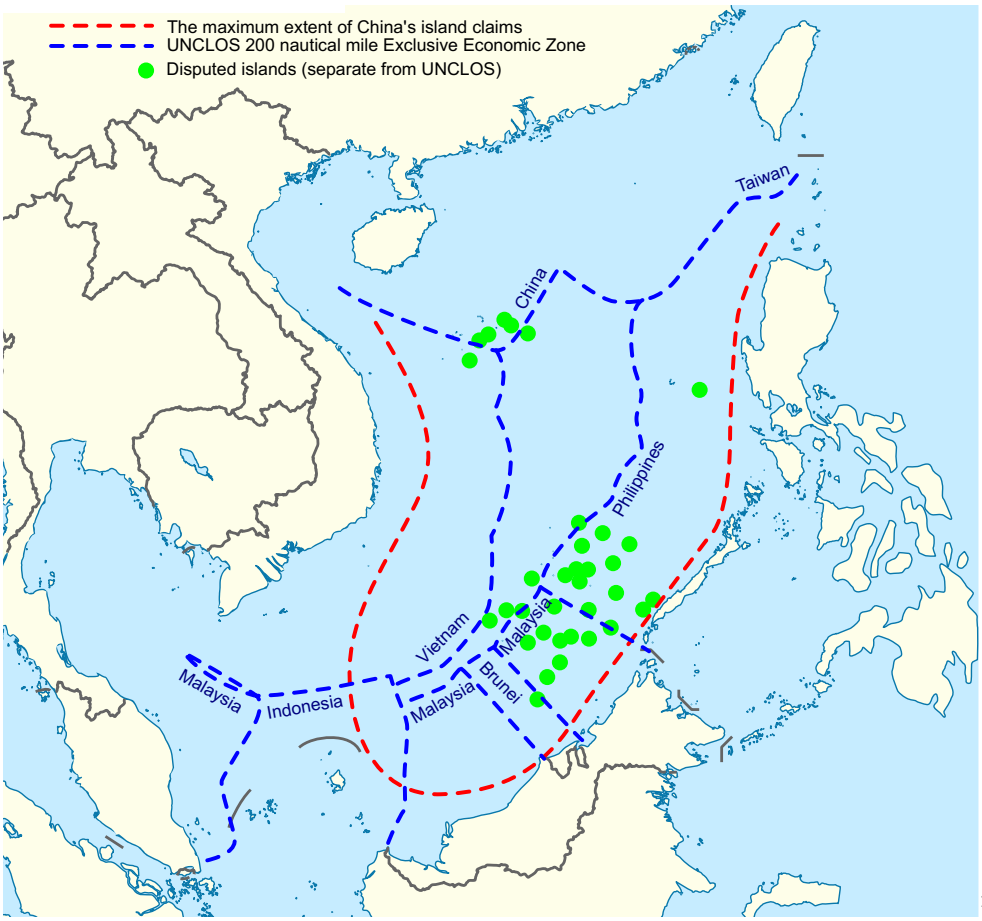
6.1 Chinese Policy Objectives in the South China Sea

To infer (dis)alignment between cyber operations and policy, it is first necessary to lay out key information on Chinese policy objectives in the context of the South China Sea region. Policy objectives of China in the region may be divided into the following three categories. Firstly, territorial questions, specifically connected to disputed islands and reefs in the South China Sea, and the question of Taiwan. The latter is related to ensuring the unity of the country, which includes safeguarding sovereignty over Tibet, Xinjiang, Hong Kong, and Taiwan. Safeguarding sovereignty over these regions is connected to safeguarding national security, which is understood as guaranteeing the safety of citizens and the stability of the political system. Lastly, economic development, specifically related to the Belt and Road Initiative and other economic development strategies stipulated in the Five-Year Plans. These policy objectives guide China's foreign policy and shape its interaction with other countries and international organizations.

Official statements from the government can give an insight into the policy objectives that the state deems particularly important. In 2011 a White Paper on ´China's Peaceful Development´ was published. This document described China´s "core interests", which were pronounced to include "state sovereignty, national security, territorial integrity, and national reunification, China's political systems established by the Constitution and overall social stability, and the basic safeguards for ensuring sustainable economic and social development" (The State Council The Peoples Republic of China 2011). This statement gives some insight into the overall focus on policy development in the past decade.

A central question is China's claim of sovereignty over territory in the South China Sea that other states have claimed as their own. The most strongly disputed islands in the South China Sea are the Spratly Islands and the Paracel Islands, both of which China has claimed sovereignty over based on historic rights (Yang 2021, 67). Specifically, the historical claim over the region is referred to as the nine-dash line. This refers to a unilateral nine-dashed line which China has used to claim the entire South China Sea basin (i.e., Permanent Mission of the People's Republic of China 2009). The nine-dash line was first published in 1948, and has been used to emphasise the sovereign claim over the waters (Yang 2021, 67), stretching along the coastline of the Philippines, Brunei, and Vietnam, the other claimants of territory in the South China Sea.

Figure I



[1]

[1] Illustration by Goran Tek-en, CC BY-SA 4.0, https://commons.wikimedia.org/wiki/File:South_China_Sea_vector.svg#/media/File:South_China_Sea_vector.svg

This conflict has roots going back several decades. In 1974, China gained full control over the Paracel Islands through naval battles with Vietnamese forces. Vietnam considers this area within its Exclusive Economic Zone (EEZ). This conflict has resurfaced in recent years (Zhang 2017, 444). In 1988, China occupied the Spratly Islands, again through a naval conflict with Vietnam (Zhang 2017, 437). In late 2013, the Chinese government started building projects on seven reefs around the Spratly Islands. By 2016, all these reefs had been turned into islets (Zhang 2017, 445). Vietnam claims sovereignty over this area (Hải and Linh 2021, 101). In 1994 China took control over Mischief Reed located within the EEZ of the Philippines (Zhang 2017, 438). The conflict over disputed territory, which has resurfaced in the last decades, has spurred China's ambition to establish itself as a maritime power (Yang 2021, 69).

The perception of a legitimate claim over territory in the South China Sea basin has been evident in official policy statements. The 2012 Defence White Paper was the first to argue that China was a major maritime country. Accordingly, a reorientation of the PLA toward maritime interests occurred (Doshi 2021, 189). The 2013 Defence White Paper had a subsection on "protecting overseas interests", defined as overseas energy resources and strategic sea lines of communication (Doshi 2021, 187–88). The 2015 White Paper echoed the same sentiment as the 2013 Whitepaper but it also noted that it was necessary for China to develop a modern maritime military force structure, including modern military equipment for fighting a maritime war (Doshi 2021, 190).

In 2019, The Chinese White Paper on national defence highlighted that national security faced threats from countries from outside the region entering what is considered China's territorial waters and the waters and airspace near what is considered Chinese islands and reefs, such as the Spratly Islands and the Paracel Islands (The State Council Information Office of the People's Republic of China 2019). Since 2015, the US has conducted Freedom of Navigation operations in the South China Sea. These operations are conducted in what is considered international waters according to the United Nations Convention on the Law of the Sea (UNCLOS). Concerning the US Freedom of Navigation Operations, the official narrative from the Chinese government is that the US is illegally entering Chinese territorial waters (Yang 2021, 65). A similar narrative on the US' role in the region is either implicitly or explicitly alluded to by Chinese academics when discussing South-East Asian matters (Zeng, Xiao, and Breslin 2015, 257). Specifically, the question of the "first island chains" forms key

element in the US strategic plans towards China in the region. The “first island chain” refer to a chain of islands along the border of the territory that China considers to be holding a legitimate claim over in the South China Sea, such as the Paracel and the Spratly Islands, but also including Taiwan.

Closely related to the question of control over the South China Sea and the relationship with the US is an interest is to gain control over Taiwan. To gain control over Taiwan, the Chinese government has perceives a need to solve three separate issues: gain control over the ‘first islands’ chain, to increase maritime security, and to strengthen control over what is regarded as a matter of undisputed unity of the mainland (Zeng, Xiao, and Breslin 2015, 260). In the category of “internal unity”, we find questions related to Tibet, Xinjiang, and Taiwan (Zeng, Xiao, and Breslin 2015, 257). The question of control over Taiwan is regarded as the largest problem in state relations with the US. China blames the US for trying to sabotage an important Chinese policy objective of achieving “internal unity” by uniting Taiwan in mainland China (Zeng, Xiao, and Breslin 2015, 262).

The question of territorial control over the South China Sea is related to the interest in energy security and economic development, which was set out in the 2011 White Paper 2011. The Chinese government views the South China Sea as home to several important sea lanes, which are among the main navigation routes for China’s foreign trade and energy imports. The United Nations Conference on Trade and Development (UNCTAD) estimates that roughly one-third of global shipping passes through the South China Sea. China is the largest importer and exporter of goods in the region (Cordesman, Burke, and Molot 2019).

Furthermore, the region is also described as a central part of the 21st Century Maritime Silk Road, one of two branches of the Belt and Road Initiative (BRI). Therefore, the security of these sea lanes is considered to be a vital objective for the Chinese government (Yang 2021, 66, 69). Concerning economic development, the BRI is a central building block. In 2013, the Central Committee of the Chinese Communist Party (CCP) decided that China should accelerate the construction of infrastructure, to connect China with neighbouring countries and regions, and promote development along the Silk Road Economic Belt and the Maritime Silk Road (Liu, 2021, p. 226).

The success or failure of this endeavour relies heavily on the participation of Southeast Asian countries. Most of the BRI projects initiated in the region since 2013 involve railway, road, and power projects. Typically, these projects are carried out through joint ventures between a Chinese entity and the host country entity, with financing from Chinese-linked financial organizations. These joint ventures operate under concessions from the local government (Suffian 2018, 11–12). Moreover, trade between China and the countries in the region has increased rapidly in recent years (Yan 2018, 5). This development mirrors the Chinese preference for a South China Sea region where the other states are dependent on China economically and divorced from US alliances. Decreasing US influence in the region was outlined in a 2011 White Paper stipulating the concept of a "Community of Common Destiny" (Doshi 2021, 169). President Xi echoed the same sentiment in a speech held at the 2014 Central Foreign Affairs Work Forum meeting. Here, Xi elevated the periphery over other focuses for Chinese strategy, thereby highlighting the central focus on the neighbouring countries from around this time (Doshi 2021, 172)

The outline for social and economic development is stipulated in the Five-year plans. The plans set goals and targets for economic growth and development, with a focus on specific industries and sectors, and outline strategies and policies to achieve these goals. The currently active 14th plan, covering 2021-2025, aims to strengthen domestic capacity for innovation in manufacturing and high technology, with the ultimate goal of reducing reliance on foreign technology. Other important goals of the plan include upgrading infrastructure and enhancing China's integration into the global economy (Xinhua News Agency 2021). The 13th plan, active from 2016 to 2020, aimed at improving the quality and efficiency of growth, transforming, and upgrading the economy, and doubling the 2010 GDP by 2020. Innovation was considered the driving force of this development (Central Committee of the Communist Party of China 2016). These goals are all emphasised in the 2015 "Made in China 2025" plan. The strategy defines industries where China wants to achieve major breakthroughs and become globally competitive. These include power equipment and next-generation information technology. To achieve this goal the government is investing heavily in research and development of advanced technology. The core aim is to initiate domestic innovation in technology (Zenglein and Holzmann 2019).

In contrast to the 13th and 14th plans, the 12th five-year plan, active from 2011 to 2015, focused on elevating the core competitiveness of the manufacturing industry, improving new

and strategic industries, and strengthening urban and rural development (China's National People's Congress 2011). The 12th to the 12th and 12th plans gradually shift towards a more pronounces emphasis on innovation. While the 12th plan prioritized increased competitiveness, the 13th and 14th plans elevated scientific progress and innovation as the primary means of transformation and rejuvenation of the country.

6.2 Cyber Unit Activity in the South China Sea

The data I have collected indicate that Chinese cyber units are interested in targeting a specific set of entities in the South China Sea region. The most prominent targets are entities connected to national governments, such as ministries or the military. In 26 out of 50 incidents, those were the target or one of the targets of the operation, as some incidents in the dataset include several targets, in line with the description of incidents given above. Additionally, seven incidents included the targeting of entities within the energy sector, while eight incidents involved the targeting of entities related to technology or technological development. Local law enforcement, telecommunications, and research (e.g., institutes and universities) were also among the targets of cyber operations conducted by Chinese cyber units. Some of the targeted research institutes are described as defence contractors. Concerning the targeting of Taiwan, the empirical information reveals an interest in advanced technology, such as superconductors, semiconductors, and other parts of the electronics industry. This was described as the target or one of the targets in five incidents in the period that the analysis covers.

One of the most important findings of my information collection is that the impact on systems is classified as information extraction in all but one incident. In the following, I will analyse a selection of these incidents to establish whether they align with China's publicly stated policy objectives. I have chosen to explore certain incidents in detail to gain a better understanding of the context in which they occurred. The common denominator between these incidents is that they yield more precise information on the targeted entity and when the intrusion occurred. The information on target and time makes it possible to place the activity in the context in which it occurred, which is important to infer (dis)alignment between policy and practice.

In my data set, the cyber unit with the highest frequency of incidents is APT40. The unit has been connected to the Hainan Province State Security Department, an arm of the Ministry of State Security (MSS) (Department of Justice Office of Public Affairs 2021). The Ministry of State Security (MSS) is responsible for overseeing Chinese intelligence operations. These intelligence efforts serve a dual purpose: carrying out internal security measures against dissidents and conducting foreign intelligence operations (Lowenthal 2017, 499). The cyber unit has been active since 2013, targeting various organizations, but with a specific focus on the South China Sea. In general, targeted organizations have included government agencies, defence contractors, manufacturers, universities, and legal firms involved in diplomatic disputes (Raggi and Scenarelli 2022). In 2019, the US Department of Justice issues an indictment that suggested that APT40 has historically targeted state-funded defence contractors across the globe to obtain intellectual property related to naval technology (United States District Court Southern District of California 2019).

Specific incidents conducted by APT40 corroborate the findings of the two reports listed above. In early August 2016 a compromise of the Secretary General of Taiwan's Government Office – the Executive Yuan – was uncovered. The Executive Yuan is the name of the executive branch of government in Taiwan. This intrusion was conducted by APT40 (Ray et al. 2016). The context of this incident was an increased uncertainty on the future of relations between China and Taiwan after elections were held in Taiwan in January 2016. Taiwan has two large political parties: the Kuomintang (KMT) and the Democratic Progressive Party (DPP). The DPP has supported the independence of Taiwan, while the KMT has been more lenient in state relations with China. In the election, Tsai Ing-wen from the Democratic Progressive Party (DPP) was elected president. For the first time, the political party Kuomintang (KMT) lost power in both legislative branches. After this election, the DPP controlled the Executive Yuan, the Legislative Yuan, and the majority of local government in Taiwan. In the aftermath of the election, China demanded that Tsai would accept the 1992 consensus, which stipulates that the two sides of the Taiwan Strait belong to one China (Tung 2016). President Tsai has subsequently refused to accept the consensus. The election, therefore, marked a deterioration of the relations between China and Taiwan. During the former president Ma of the KMT, dialogues and negotiations were more frequent, and involved tighter economic integration. This development culminated in a meeting between President Ma and President Xi in Singapore in November 2015 (Tung 2016).

The election of a DPP president created an increased situation of uncertainty regarding the future of relations between Taipei and Beijing. With this context as a point of departure, the compromise of the Legislative Yuan could be connected to an interest in gaining information on the future policy of the government of Taiwan on its relations with China. Based on the timing and the context of the incident in August I infer that this activity is in line with the Chinese policy objective of unifying China and Taiwan. Access to private information would be valuable to China at this junction. Based on the information extraction, the choice of target and the context in which the cyber operation occurred, the incident could be connected to an interest in achieving a decision advantage, to aid in developing the future strategy of incorporating Taiwan into mainland China.

APT40 has also displayed an interest in targets in the Philippines. A specific incident n occurred in 2015, where the activity was aimed at military agencies. The attackers applied social engineering tactics to breach the targeted networks. They used contextually relevant subjects, and content, and gave e-mail attachments names such as “Statement” to convince chosen recipients to download and open the files supposedly sent for review (Alintanahin 2015). Context-wise, prior years were marked by rising tensions. In 2014, the Philippine Air Force (PAF) initiated a modernization scheme known as Flight Plan 2028, prompted by the absence of up-to-date combat aircraft from 2005 to 2015. The primary objective was to acquire capabilities to combat incursions in 50% to 75% of the territory by 2020 and the complete territory, including the exclusive economic zone, by 2028. In 2013, the country also launched a program to acquire two new-build frigates. The 2013 program constituted a significant modernization of the Philippine Navy and Air Force (Vuving 2017).

The modernization process could have created an interest acquiring information on the new state of Filipino military capabilities. As with the incidents above, the intrusions in military systems in the Philippines could be connected to an interest in achieving a decision advantage. The development of capabilities is considered private information in international relations. Achieving access to this information could serve to decrease the Chinese level of uncertainty in the relationship with the Philippines, possibly aiding in the creation of more precise future policies in the relationship between the two countries. Based on the activity aimed at Filipino military entities at the given time, the incident could be aligned with territorial interests in the South China Sea, of which China and the Philippines were engaged in a long-standing dispute in the years leading up to 2015.

Furthermore, APT40 also targeted the Department of Justice in the Philippines in 2015 (Proofpoint 2017). The context of this intrusion was likely the proceedings between China and the Philippines in the Permanent Court of Arbitration under UNCLOS. The case concerned the dispute over maritime rights in the South China Sea, and what the Philippines regarded as Chinese unlawful actions in the region. China refused to take part in the proceedings, arguing that the Permanent Court of Arbitration had no jurisdiction over the case (Permanent Court of Arbitration 2016). Consequently, an intrusion into the Department of Justice during the height of the proceedings could give access to information on the Filipino government's views on the dispute and the arbitration. Despite claiming that the Court of Arbitration holds no jurisdiction over the dispute, a ruling in the Philippines' favour would serve as a blow to China's standing in international relations. Insight into the perspective of the Department of Justice would therefore be valuable, especially considering that China chose to not take part in the proceedings and would therefore not get access to information through traditional sources. Consequently, considering the context of the incident it is possible to infer that the intrusion by APT40 occurred in step with policy objectives. The objective in this case was the territorial dispute between China and the Philippines. Consequently, the intrusion could be regarded as an effort to achieve a decision advantage because it would reduce the uncertainty related to how the Philippines viewed the arbitration case. This information would be particularly valuable seeing as China did not take part in the proceedings, and therefore would not have access to sources of information on the scene.

In 2017, APT40 was observed impersonating an unmanned underwater vehicle manufacturer in phishing emails (Plan et al. 2019). This activity could indicate an interest in this specific maritime technology. Context-wise, this interest could be supported by the fact that the People Liberation Army Navy seized a United States Navy unmanned underwater vehicle (UUV) in December 2018 in international waters outside the coast of the Philippines. China was publicly called upon by the US for this incident (Cronk and US Department of Defense 2016). Furthermore, in January and February of 2018, a US Navy contractor's computer system was hacked by APT40, resulting in the theft of confidential data related to secret projects. The contractor in question collaborated with the Naval Undersea Warfare Center, a research and development facility used by the US Navy for submarine-related engineering, testing, evaluation, and fleet support activities. The stolen information included hundreds of gigabytes of data associated with undersea warfare, autonomous underwater systems, and

offensive and defensive weapons systems (Liptak 2018). According to American officials, the stolen information included secret plans to develop a supersonic anti-ship missile for use on US submarines by 2020. Additionally, the stolen information also included signals and sensor data, submarine radio information relating to cryptographic systems, and the Navy submarine development unit's electronic warfare library (Nakashima and Sonne 2018).

Also in 2018, it was uncovered that APT40 had stolen information related to maritime technology from engineering firms and defence contractors in the US. The engineering firms included research institutes and other academic institutions (FireEye 2018). According to a report in Bloomberg, APT40 collected data related to radar range and the level of precision with which a developing system could detect activity at sea (Tweed 2018). Another report stated that the same actor had targeted universities in the US, with a specific focus on maritime technology. The targeting dates back to April 2017, and the security company iDefense assessed that the group emphasised small and medium contractors, academic institutions, and think tanks (Accenture iDefence 2019). A report from Wall Street Journals corroborated that some of the universities in this specific incident had been awarded contracts with the US Navy (Volz 2019).

There are two possible interpretations possible for how these three separate incidents align with Chinese policy objectives. On the one hand, it could aid in developing new technology to modernise the PLA Navy, as per the 2013 Five-Year Plan. By acquiring information on foreign technology through cyber operations, the development of native technology could be stimulated. This would not be a novel occurrence. In 1999, the US House Select Committee on US National Security and Military/Commercial Concerns with the People's Republic of China claimed that China had stolen various pieces of information about nuclear weapons and satellite technology (Lowenthal 2017, 501). However, this assessment could be mirroring the US perception of Chinese activity, rather than the Chinese focus through the activity of APT40. An alternative interpretation is that the activity could serve to decrease uncertainty on US maritime capabilities and activities in the region by acquiring information on the technology that the US Navy is using in the region, and the character of the information that the US Navy is able to retrieve from their monitoring equipment, such as the UUV that was seized in 2016.

The context of these incidents are the Freedom of Navigation operations that the US Navy has conducted in the South China Sea since October 2015. These US Navy operations took place around the Spratly and the Paracel Islands, which China regards as its sovereign territory. The US argued that The Freedom of Navigation operations in 2015 and 2016 took place under innocent passage, which is considered a continuous transit through another state's territorial water. In 2017, however, the operation in 2017 was conducted in a manner not consistent with innocent passage, presumably to more clearly challenge what the US considers to be an illegal Chinese claim to the area in question (Freund 2017). These Freedom of Navigation operations form the context of the APT40 incidents described above, because they all occurred after the US increased it military presence in the region. Based on the targeting and the context, the activity of APT40 could therefore be inferred to be in step with the policy objective of safeguarding territorial sovereignty in the South China Sea region and reducing the US impact in the area.

The targeting of US navy contractors in the context of the Freedom of Navigation operations indicates an interest in monitoring the development of capabilities that can be deployed by the US Navy in the region. Information on capabilities is considered to be private information in international relations, and is a central source of uncertainty. However, access to this private information from systems of US navy contractors could give insight into the development of maritime capabilities. This access could result in a decision advantage, because it would alleviate the uncertainty related to US military activities in the South China Sea. This decision advantage could aid in developing future Chinese policy on how to address US military presence in the region.

Regarding the interest in safeguarding sovereignty in relation to the US in the context of the South China Sea, it is noteworthy to highlight the activity of the cyber unit RedAlpha. Between 2019 and 2022 RedAlpha targeted entities such as the American Chamber of Commerce in Taiwan and American Institute in Taiwan. The activity is classified as the extraction of information (Insikt Group 2022). The targeting could serve to illuminate an interest in acquiring information on entities central to the relationship between the US and Taiwan. The American Institute is the de facto American embassy in Taiwan, and it has functioned as the diplomatic representation in Taiwan since 1979 (Kosar 2011, 26). The same interest in US relations with Taiwan is supported by the targeting of the American Chamber of Commerce in Taiwan, which supports American companies trading in Taiwan.

Context-wise, the period that RedAlpha conducted these intrusions marked the run up to the Taiwan Policy Act, approved by the US Senate Foreign Relations Committee in September 2022. If the legislation is passed by the US Senate and House of Representatives, it will significantly enhance US military support for Taiwan, including billions in military assistance. The American Institute in Taiwan figured in the hearings leading up to the US Senate's Taiwan Policy Act. Additionally, the Taiwan Policy Act has language on strengthening trade between Taiwan and the US (Costigan 2022). Targeting these entities could therefore be an important source of private information on the relationship between the US and Taiwan and how this might change. While the information on RedAlpha cyber operations in this period is not detailed enough to find a clear link between the Foreign Relations Committee policy proposal and RedAlpha activity, a central aspect of uncertainty in the Chinese objective of uniting Taiwan in mainland China is how the relationship between the US and Taiwan develops. Targeting these US entities could reduce uncertainty in this area, thereby aiding in acquiring a decision advantage on the US stance on the independence of Taiwan and how this might develop in the future.

APT40 activity is not limited to targeting entities in the government and military sectors. In June 2021, the actor was observed targeting Malaysian entities engaged in offshore drilling and exploring deep-water energy sources, specifically companies involved in engineering, natural gas extraction, and the export of natural gas from the Kasawari Gas Project located off the coast of Malaysia (Raggi and Scenarelli 2022). As an isolated event, the intrusion could be aligned with Made in China 2025, which stipulates that the development of power equipment is a central interest. Accordingly, the targeting of the Kasawari Gas Project could be connected to an interest in developing economic capabilities relative to other states, which is regarded as an aspect of decision advantage.

However, in close proximity to this activity, the Asia Maritime Transparency Initiative reported disruption at the project site stemming from Chinese Coast Guard intervention (Asia Maritime Transparency Initiative 2021). Therefore, considering the context, the activity could signify an interest in the project related to achieving a decision advantage. The reasoning for this conclusion is that the specific targets in this incident were all related to a physical presence in the area. This targeting, in the context of the activity of the Chinese coast guard, indicates an interest in monitoring which actors conducted activity in the area. The gas field is

located close to the nine-dash line, which China has used to claim sovereignty over the South China Sea. Therefore, this cyber activity by APT40 could be understood as aligned with Chinese interests in the territorial strife with Malaysia. Based on the context and the alignment with policy, it is possible to conclude that this incident was conducted in an effort to achieve a decision advantage, where the information could assist in developing policies for how to safeguard Chinese territorial integrity in the area.

APT40 has also targeted various companies involved in the supply chain of offshore energy projects located in the South China Sea. The targeted entities comprise heavy industry and manufacturers responsible for the maintenance of offshore wind farms, producers of installation components used in offshore wind farms, exporters of energy from major energy exploration sites in the South China Sea, leading consulting firms offering specialized knowledge for projects in the area, and global construction companies accountable for installing offshore energy projects in the South China Sea (Raggi and Scenarelli 2022). An incident with more detailed information occurred in late March 2022. The incident involved phishing activity towards a key European supplier of heavy equipment for entities involved in the construction of the Yunlin Offshore Windfarm. The wind farm is located off the coast of Yunlin County in Taiwan. The incident was described as phishing, with no information on the effects of the intrusion (Raggi and Scenarelli 2022).

An explanation of these incidents is that China is interested in the technology and the strategy for developing this technology. Offshore wind farms are a technology in development. To retrieve information on these wind farms would, as suggested above, be in line with the 2021-2025 Five-Year plan emphasising innovation as a core goal, in addition to the reduction in climate emissions and energy security. It would also be aligned with the “Made in China 2025” plan, which emphasises energy equipment as a core industry of domestic innovation. Access to information on the technology used and how it is developed, could serve to support the development of Chinese wind farms, aligned with the strategic plans. Theoretically, the targeting could be understood as an effort to improve Chinese economic capabilities. The information could contribute to reducing the uncertainty of the characteristics of the economic capabilities of the other littoral states of the South China Sea and aid in the effort to strengthen Chinese economic capabilities.

However, the targeting of Yunlin Offshore Windfarm also be connected to an interest in identifying the weak spots of Taiwan, to pressure the government to be more lenient towards Beijing. Taiwan has few indigenous sources of energy. The offshore wind resources are one of the few sources of energy in the country. It has no physical power connection with neighbouring countries, and there are no domestic sources of fossil fuels. Consequently, Taiwan relies on imports of fossil fuels for 97,7 percent of its total energy supply (Kucharaski 2022). An efficient production of offshore wind in the future could therefore significantly contribute to energy security in Taiwan. Currently, Taiwan is vulnerable for disruptions. The fact that APT40 could successfully target the systems related to the windfarm, demonstrates a capability to access these systems. This demonstration could create a fear for disruptions in the future, in what could be an important part of the energy infrastructure in Taiwan. Based on the context, the incident could be described as an effort to compel the government in Taiwan. The reasoning behind this is that it demonstrates an ability to inflict pain in the future, creating an insecurity of what this actor might achieve in terms of disruptive effects in the future. This compellent effect would be aligned with the interest of uniting Taiwan in China.

Furthermore, openly available information on APT40 activity indicates an interest in projects related to the development of infrastructure under the BRI. Around December 2017, the group was observed targeting a Malaysian high-speed rail corporation and a Malaysian political party. According to a US Department of Defence Indictment, the context of these intrusions was that the China Railway Engineering Group was seeking a multi-billion-dollar contract to build a high-speed railway to Malaysia. The Indictment claimed that the intrusions occurred around the same time that the party had a role in deciding whether the Chinese state-owned enterprise would get the bid on a railway contract in Malaysia (United States District Court Southern District of California 2019). As noted above, infrastructure development under the BRI is often achieved through a contract with the local government, which requires political support. Set in its contextual circumstances, this specific incident, therefore, indicates an interest in gaining information on the political process of acquiring the contract for infrastructure development, which would aid in developing a strategy of how to act towards the political actors involved in the process. Therefore, APT40 was likely employed to retrieve information on this process, which could be used to get the bid on the railway contract. This activity is in step with the policy objective of investing in infrastructure projects in the region. Based on the timing and the context, the incidents in Malaysia could be connected to an

information advantage, where the activity aid in achieving access to private information that the actor will not gain through traditional diplomatic and corporate channels.

Another group active in the region is APT41. This cyber unit has also been connected to the Ministry of State Security in an indictment from the US Department of Justice (Department of Justice Office of Public Affairs 2020). Publicly available information suggests that the group has a particular interest in Taiwan. In April 2020, one of the largest cyber intrusions in Taiwan occurred. According to reports, the ColdLock ransomware was used during these incidents. In contrast to infostealers, ransomware encrypts both user files and databases present on local, removable, and network drives, effectively locking access to these systems (Cyberint 2020). One of the targets was the CPC Corporation, a state-owned petroleum and natural gas company and the largest supplier of petrol to Taiwan. The intrusion created a disruptive effect, with long queues at petrol stations around Taiwan for several days. CPC Corporation was not alone; ten more organizations in critical infrastructure were also targeted for intrusions that same weekend, including a large multinational semiconductor vendor. Chunghwa Telecom announced on May 6th that it had been breached. This is Taiwan's largest telecommunications company and the local exchange carrier of PSTN, Mobile, and Broadband services. (CyCraft Technology 2020b). Additionally, according to reports, the ransomware incidents also impacted Powertech Technology and other non-disclosed companies operating in Taiwan's semiconductor industry (Cyberint 2020).

As was highlighted in the section on Chinese political objectives in the region, China is interested in fully implementing Taiwan as a part of mainland China. The context of this incident could – once again – be assumed to be the presidential election in Taiwan. Tsai Ing-Wen from the DPP won the presidential seat for her second term by a strong majority. Tsai's refusal to accede to Beijing's proposal for a unification agreement was reported to have had an effect on the popular support of Tsai (L. Kuo 2020). The re-election of Tsai marked renewed support for the independence of Taiwan.

The incidents at the beginning of 2020 were targeted toward what the government in Taiwan regards as critical infrastructure, which is considered to be energy, water resource, telecommunications, transportation, banking and finance, emergency aid and hospitals, central and local governments, and high-tech parks (Administration for Cyber Security 2022). Based on the context of the incidents and the targeting, it is possible to analyse these incidents in light

of compellence. The targeting of critical infrastructure could be considered compellence by putting pressure on the DPP government. The incidents displayed the capability of several Chinese cyber units to apply potentially severe effects on systems connected to critical infrastructure. The core of this potential compellent effect is the uncertainty it generates regarding the potential for future detrimental effects on critical infrastructure. The head of Taiwan's Department of Cyber Security acknowledged that significant breaches had occurred around this time. He noted that Taiwan's critical infrastructure relies heavily on digital systems, making it vulnerable to attacks (Cheung, Ripley, and Gladys 2021). This shows that the government in Taiwan is very aware of the likelihood of cyber operations occurring in the future and regards this as a threat.

Accordingly, the effectiveness of cyber operations as a compellent threat is achieved through three factors. Firstly, through the action of targeting critical infrastructure, the willingness to impose pain is communicated. This action could be considered an effective threat because it is considered to be harmful by the government in Taiwan. Secondly, the incidents have been attributed to a Chinese cyber unit, one of which is known to be associated with the MSS. The attribution could heighten the fear of future Chinese action toward critical infrastructure. This fear could be strengthened by the capability of Chinese cyber units to exploit vulnerabilities in systems. According to Microsoft (Microsoft 2022, 39), Chinese state-sponsored actors have a high capacity for discovering and creating zero-day exploits from previously unknown vulnerabilities. Lastly, viewed in the context of statements from China on the unification of China and Taiwan, the aim of this activity could be to put pressure on the DPP government in Taiwan to change its stance on the relationship with China. Furthermore, the effect could be strengthened by undermining the confidence in the government of Taiwan’s ability to defend critical infrastructure. Taken together, these incidents could be understood as compellence towards Taiwan, aligned with the objective of incorporating Taiwan into mainland China.

Nevertheless, the targeting of entities in the critical infrastructure of Taiwan could also be understood as surveillance. If cyber units are to create more disruptive effects on critical infrastructure in the future, it could be valuable to have information on how the situation would develop. This information could for example be how fast the systems would be up and running again and how the government in Taiwan would handle the situation. The destructive element of this incident – and the information retrieved from the other targeted entities - could be understood as a decision advantage because it could aid in developing cyber operations toward

critical infrastructure in the future. Observing how the reaction spans out after a disruptive attack could aid in modelling future disruption. Therefore, the information from the incidents in 2020 could be used to develop means of brute force in a situation of increased conflict in the future.

A situation in which brute force could be expected occurred in 2022. In August of 2022, there was an increase in tensions across the Taiwan Strait. From the Chinese side, this was signalled through military demonstrations. These military demonstrations were reported to be the largest in 26 years and included numerous incursions into Taiwan's air defence identification zone and four missiles evidently fired over the country (U-Jin and Suorsa 2022). A reason for this situation was the visit made by the Speaker of the US House of Representatives, Nancy Pelosi, in August 2022. Beijing regarded these steps as a de facto recognition of the independence of Taiwan, where each US action is part of a larger campaign to change the status quo (M. A. Kuo 2022). In a situation of increased tension, the existing literature on cyber operations would expect cyber activity to complement force to increase its effectiveness (see i.e., Egloff and Shires 2021; Smeets 2018). However, around this point in time, the only reported disruption was a Denial-of-Service incident against government websites. Among them was the website of the president of Taiwan (Miller 2022). Denial-of-Service is conducted by overloading a website with traffic, subsequently rendering it inaccessible, and this type of incident is regarded as a less sophisticated method of creating effects on a system. Furthermore, the incident was not attributed to any of the active cyber units in the region. Rather, security experts were wary of connecting the incident to China (Miller 2022).

This leads to the conclusion that there is no publicly available information of a more advanced intrusion into systems of critical infrastructure during this period of increased tension, as it would be plausible to expect. The reason for the lack of information on incidents could either be that the government of Taiwan or entities within Taiwan chose not to publicly disclose incidents, or it could be that no disruptive activity took place around this point in time. Considering that the intrusions to entities in critical infrastructure in 2020 were disclosed, the assumption that any severe intrusions occurring in 2022 would have been publicly disclosed is plausible. The result is a lack of severe disruptive activity during a period of heightened tensions. A possible interpretation could be that China regarded the military exercises as a clear signal of discontent with how the situation developed. China did

not, however, plan to invade Taiwan at this point. Theoretically, brute force would function well in preparation for increased conflict. For example, in combination with an invasion the effect could be used to deny access to information at a crucial time. Because China did not plan to invade Taiwan at this point, brute force could be regarded as not suitable under these circumstances.

Other cyber units have also shown a specific interest in Taiwan. One of these is BlackTech. The unit has not been specifically connected to an intelligence or military bureau within China but has been described as well-funded and organized (Huang 2016). In April 2020, malicious activity was discovered in the systems of Taiwanese government agencies (CyCraft Technology 2020c). Additionally, targets across media, electronics, and finance were uncovered around this time. The targeting of a media company lasted from August 2019 to June 2020. The finance company was targeted from August 2019 to March 2020, and the finance company was targeted for a briefer period in March 2020. In contrast to the April 2020 targeting of critical infrastructure, these incidents involved malware designed to enable information extraction (Symantec 2020).

The aim of BlackTech in the incidents described above could be understood in multiple ways. The targeting of the media company could be understood in the context of the election in Taiwan. Exfiltration of information from a media company could increase knowledge on how the situation developed in the aftermath of the DPP election win. Theoretically, this activity could be understood as an effort to achieve a decision advantage, where the information retrieved could be an extra source of private information on how the political situation in Taiwan developed in the first half of 2020. Furthermore, a finance company was targeted in March 2020. Context-wise, retrieving information from a finance company in this period could serve to increase knowledge on the financial effects of the first measures of the Covid-19 pandemic. The stability of the financial situation is vital for continued trade between China and countries in the region, which is an economic objective of China. The early stages of the Covid-19 pandemic induced a high level of uncertainty about how the measures following the pandemic would impact the financial situation. China is the largest trading partner of Taiwan (Maizland 2023). Additionally, Taiwan produces important components in Chinese advanced technology manufacturing, with companies in Taiwan producing around 68 percent of the world's semiconductors and over 90 percent of the most advanced ones (Sacks 2023). Access to information that could reduce the uncertainty connected to the state of the financial situation

in Taiwan during this period would be attractive to the government of China. Therefore, it is possible to understand this activity in line with an effort to achieve a decision advantage to aid in developing future trade policy towards Taiwan.

The electronics manufacturing industry in Taiwan was also targeted by both BlackTech and APT41 in 2020. Semiconductors are important components in every networked device, form mobile phones to electric cars. With the increased level of digitalization in societies worldwide, semiconductors will be increasingly important. Considering the existing literature on Chinese cyber operations (Gilli and Gilli 2019; Lindsay, Cheung, and Reveron 2015; Valeriano 2018), it is plausible to conclude that the active cyber units in the 2020 incident targeted the electronics industry in Taiwan for the purpose of stealing intellectual property. This information could aid in developing the same technology, consequently strengthening China's position as a manufacturer of advanced technology. Theoretically, targeting high-tech manufacturing in Taiwan could aid in improving Chinese capabilities through the extraction of information on technology development. The capabilities in this case would be the resources in the economy, understood as one aspect state's capabilities (Singer 1988; Singer, Stuart, and Stuckey 1972). In the context of the Taiwan-China relationship, semiconductors could be understood as a central element of leverage for Taiwan in preventing the Chinese government's objectives of unifying the two countries. According to the "Made in China 2025" plan, China aims to meet the domestic demand for semiconductors by 2025, which means that domestic innovation on this technology is necessary (Zenglein and Holzmann 2019). Accordingly, the targeting of semiconductor manufacturers in Taiwan could be understood as aligned with the objective of improving domestic innovation in advanced technology.

There is an active cyber unit that is seemingly focusing on Vietnam. In June 2020, it was uncovered that entities in the government and military sectors in Vietnam were targeted by the cyber unit called APT27. In the incident in Vietnam, the final payload was a remote administration tool that provided full control over the infected device. The analysis suggested that the activity was conducted by a group related to Cycldek, a Chinese-speaking group active since at least 2013. Dozens of computers were affected, with 80 % of them based in Vietnam. Most belonged to the government of the military sector; however, other targets were related to health, diplomacy, education, or politics (Kaspersky 2021).

The context of this activity is several maritime stands-offs between Vietnam and China in 2020. Throughout the year, this included two missile tests near the Paracel Islands and sending a survey ship into the EEZ of Vietnam (Jennings 2020). Furthermore, in April 2020, China announced the establishment of two new administrative structures in the South China Sea. The first was the Xisha district, covering the Paracel Islands and Macclesfield Bank, and the second was the Nansha district, covering the Spratly Islands. Vietnam also claims both of these areas. The official motivation behind the move was to make administrative control more effective but it was read as a move to strengthen the grip over the area through a formalization of control with more lasting effects (Huong 2020). The government of Vietnam publicly disputed the announcement (Reuters 2020). Also in April, a Chinese coast guard ship sunk a Vietnamese fishing boat near the Paracel Islands. Vietnam answered by sending a note verbale to the United Nations rebutting Beijing's claim to the maritime area. The maritime tension was resolved through a meeting between Chinese Defence Minister Wei Fenghe and Vietnam's Ambassador to China Phạm Sao Mai, in September 2020 (Jennings 2020). Based on this, the activity would be aligned with Chinese territorial interests, specifically related to the dispute over the Spratly Islands with Vietnam.

Establishing permanent administrative districts in a disputed area was an audacious move by China. Compared to maritime skirmished, it creates a more permanent effect. The move could potentially lead to escalating actions from Vietnam. However, access to military systems could give insight into how Vietnam would respond to these actions, potentially reducing the Chinese uncertainty on whether the situation would spiral into a more violent level of conflict. It is not possible to know at what specific time APT27 was active in retrieving information from military systems. However, based on the activity of the cyber units, the systems it was interested in, and the general context of this incidents, it is possible to infer that the aim was to achieve a decision advantage. The alleviated uncertainty of how Vietnam would respond to Chinese actions, thereby giving China an advantage in taking more precise and timely policy actions in the tense situation.

Following parts of the literature on cyber operations, it would have been reasonable to expect a destructive or disruptive cyber effect to military systems in Vietnam following the June 2020 Cycldek incident. This section of the literature argues that cyber operations are an effective instrument in conflict short of war (Buchanan 2020; Harknett and Smeets 2020b; Harknett and Fischerkeller 2019; Kello 2017; Warner 2019). In the context of increased

maritime tension between the countries, this would be a situation where it would be plausible expect a disruptive cyber operation. However, despite taking administrative control over territory that Vietnam has claimed sovereignty over, China was seemingly not interested in escalating the situation, which the meeting between the Chinese Defence Minister and the Ambassador of Vietnam to China could be an indication of. Implementing disruptive effects on the military systems in Vietnam could have been understood as an act of escalation in a situation that was already tense. Accordingly, the use of disruptive effects could be regarded as counter-productive to the aim of increasing control over the region while at the same time holding tensions at a level of control. Military conflict in the region would disrupt Sea Lines of Communication, which would countervail several of the Chinese objectives in the region. Therefore, an escalated conflict with Vietnam is likely not China's wish in the situation. Rather, the extraction of information would have aided the effort of controlling tensions in line with Chinese objectives through a decision advantage.

Mustang Panda is another actor that has been active in Vietnam. The cyber unit has mainly been observed targeting government entities and politically oriented NGOs (Côté Cyr 2022). A specific incident was aimed at political entities in Vietnam. The lure documents used in targeting dates the activity between November 2018 and August 2019. Based on these documents, one report assessed that the Communist Party of Vietnam (CVP) was the primary target. Other targets included the CVP of Lang Song Province in Vietnam, the CVP of Lao Cai Province in Vietnam and the Embassy of Vietnam in China. The lure document sent to the Vietnam embassy in China had a military theme and highlighted that no civilian ships were allowed within the area of the exercise (Anomali Threat Research 2019).

The context of these incidents has several aspects. Firstly, Vietnamese diplomacy has been described as historically unobtrusive towards China, preferring not to increase tension between the countries. In the context of these incidents, the beginning of 2018 marked a change in this preference. In March, the president of Vietnam Tran Dai Quang, met with Indian Prime Minister Narendra Modi and issued a joint statement to continue defence collaboration. They also pledged to uphold freedom of navigation and overflight in the South China Sea. Secondly, at the beginning of March, the CVP allowed a US aircraft carrier access to Vietnam for the first time since the Vietnam War. This signalled a closer military partnership between the US and Vietnam (Grossman 2018). Lastly, this period marked the preparation to a summit between US President Donald Trump and North Korean leader Kim

Jong Un, which was hosted in Hanoi, Vietnam. Reports stated that Kim arrived in the border province of Lang Song ahead of the summit (Regan 2019). The meeting marked a possible change in the hostile relationship between the US and North Korea, which would be development that China would be interested in monitoring, as it could influence the existing power dynamics in the region. Overall, this targeting illuminates a specific interest in political targets in Vietnam. Taking the targeting and context into consideration, the intrusions could give access to private information on how the diplomatic and military relationship between other states with a presence in the region developed. Particularly, closer military cooperation between the Vietnam and the US and India could be a source of uncertainty for China, particularly in relation to the territorial disputes between the two neighbouring countries. Consequently, by alleviating this uncertainty the information extraction in this period could be connected to an interest in gaining a decision advantage.

Mustang Panda has been known to use the ASEAN summit as a bait to infect individuals who are attending the summit. This tactic has allowed the cyber unit to target a broad range of individuals, as the ASEAN association comprises ten member countries in Southeast Asia. (Malhotra, An, and McKay 2022). ASEAN has also been a target of the cyber unit APT30. A report from 2015 revealed a decade-long operation focused on targets – government and commercial – who hold key political, economic, and military information about the region. Most of the social engineering efforts suggest the group is particularly interested in regional, political, military, and economic issues, disputed territories, and media organizations and journalists who report on topics related to China and the government's legitimacy. Entities in Vietnam and Malaysia had been targeted, in addition to Thailand, South Korea and India. The actors have also been particularly interested in governments associated with ASEAN, especially around official meetings in ASEAN (FireEye 2015).

Furthermore, in 2020 APT30, several national government entities in the Asia Pacific (APAC) region were targeted. A report named national governments in Vietnam and the Philippines as targets, in addition to the governments of Australia, Indonesia, Thailand, Myanmar and Brunei. The targeted government entities include ministries of foreign affairs, science and technology ministries, as well as government-owned companies (Check Point Research 2020). While lacking detailed information, which inhibits clear contextualisation of these incidents, these reports are included because they emphasise an important aspect of Chinese cyber units' activity in the region: the targeting of political entities. The government's

publicly stated policy objectives range from military, political, and economic interests. The targeting of government entities could underscore an interest in achieving a decision advantage within these more general areas through cyber operations because it could give access to the private information these entities and government representatives have access to on relations to China in various policy areas. Overall, this could reduce uncertainty and thus aid in developing more efficient policies in central areas of interest for the Chinese government towards the government in the South China Sea and the broader region of Southeast Asia.

Comparing openly available information on targeting in Taiwan, Vietnam, Malaysia, and the Philippines results in some patterns of interest. Concerning targeting in Taiwan, incidents are aimed at the government or critical infrastructure. This activity could be understood in two ways. Firstly, it could be a means of signalling a compellent threat in an effort to force the government in Taiwan to change its stance on relations with mainland China. Secondly, extracting information from these targets could be understood as an effort to achieve a decision advantage, which could aid in developing the next policy steps to incorporate Taiwan into mainland China. Accordingly, the cyber unit activity in Taiwan is mainly aligned with the policy objective of the unification of Taiwan in China.

Furthermore, publicly available information on the targeting of Vietnam shows that cyber unit intrusions is aligned with political and military disputes. Specifically, the territorial disputes in the South China Sea are a prominent context for intrusions. The effect in targeted systems in Taiwan is classified as information extraction. Therefore, the activity can be described as an effort to achieve a decision advantage to develop future policy in relations to Vietnam.

Related to the Philippines, the intrusions are also aligned with policy objectives related to territorial disputes. However, this conflict has been conducted more clearly through legal platforms, which is mirrored in the targets chosen for intrusion, among them the Department of Justice in the Philippines. In the case of the Philippines, the goal of the intrusions has been information extraction, indicating an effort to achieve a decision advantage in these areas of central interest.

Targeting in Malaysia has seemingly less of a military or legal dimension. Rather, the targeting could be regarded as aligned with economic interests in the region, especially related

to the BRI. One intrusion at an offshore energy company could, however, be said to be aligned with territorial interests, specifically when considering the intrusion's context. Concerning the incidents in Malaysia, they are all classified as information extraction. Therefore, the activity could be understood as an effort to achieve a decision advantage, either to reduce uncertainty on territorial issues or to improve domestic economic capabilities.

The conclusion that this activity could be described as a decision advantage is supported by the fact that some of the cyber units that have been analysed in-depth in this chapter have been attributed to the Chinese Ministry of State Security (MSS), which is the organization responsible for coordination Chinese foreign intelligence operations (Lowenthal 2017, 499). APT41 was connected to MSS in an indictment from the US Department of Justice (Department of Justice Office of Public Affairs 2020), while APT40 has been connected to the Hainan Province State Security Department, an arm of the Ministry of State Security (MSS) (Department of Justice Office of Public Affairs 2021).

When Chinese cyber units actively conduct information extraction aligned with the state's foreign policy objectives, this could create a situation in which the Chinese government possesses more information than the adversary. Specifically, the state possesses greater knowledge about the adversary's decision-making compared to what the adversary knows about the state's decision-making. This is especially relevant considering the high number of government and military targets listed in my dataset. As a result, China could experience reduced uncertainty in its decision-making processes relative to its adversaries in the South China Sea region. This situation translates into having more options and the ability to choose among them with enhanced certainty, timeliness, and impact. Consequently, Chinese decision-makers are able to anticipate and respond to threats and opportunities more effectively and gain an edge over their adversaries in various domains (as per Sims 2022). Related to this, a Chinese decision advantage in the South China Sea region could be understood as a source of power because support in developing policies which shape circumstances to the advantage of China. Consequently, this could result in a higher degree of outcomes in line with the states policy objectives.

7 Suggestions for Future Research

The analysis established that Chinese cyber units have been active in retrieving information from systems related to the South China Sea and that the targets chosen for this activity align with political objectives in the region through the context in which they occur. The analysis yields two separate implications. Firstly, it is important to broaden the empirical scope toward activity described as information extraction. Secondly, it is valuable to research the alignment between policy objectives and cyber operations. In the following, I will detail other potential avenues for future research on cyber operations and the phenomenon's impact on international relations.

The analysis described APT30's activities toward governments in the ASEAN region. A suggestion for future research following this would be to include other states with interests in the region. This research could further aid in understanding how China applies cyber operations in general in the region – seeing as this thesis has established that Chinese cyber operations and policy objectives are indeed aligned. Furthermore, this research could use the methods developed in this thesis to conduct the analysis. It could further serve to develop an understanding of how China is utilizing cyber operations as a source of influential power in its international relations.

The analysis also illuminated a Chinese interest in targets in the US, in this case, related to territorial strife in the South China Sea. Therefore, a suggestion for future research would be a structured analysis of all the publicly available incidents in the US that have been attributed to China. The research would likely require significant data collection. However, using the steps for data collection developed in this thesis, it could serve to significantly develop the understanding of Chinese cyber operations toward entities in the US. The existing literature focuses strongly on the theft of intellectual property, and this has been regarded as a danger to national security in the US. Structured research into Chinese cyber operations in the US and how it is aligned with policy through the context in which it occurs could serve to broaden the perspective away from intellectual property, alternatively to confirm the Chinese cyber unit activity towards the US mainly consist of theft of intellectual property.

Another interesting avenue for future research is Russian cyber unit activity leading up to and during the war in Ukraine. In a report from the Ukrainian government, it was stated that 70

percent of incidents were likely for the purpose of gathering intelligence (State Service of Special Communication and Information Protection of Ukraine 2023). Microsoft has corroborated these findings, stating that the Federal Security Service (FSB), was particularly active in retrieving information from political targets, such as national and local governments in Ukraine in the first months of the war (Microsoft Digital Security Unit 2022). As the theoretical framework in this thesis stipulated, cyber operations could serve a dual purpose – both as disruption or destruction and to gather information that could be relevant to more traditional aspects of warfare. An analysis of the activity in Ukraine could serve to illuminate this further. Additionally, a structured analysis of how Russian cyber units' cyber operations are aligned with policy objectives could aid in understanding how Russia is utilizing cyber operations in the larger context of warfare in Ukraine.

Another option is to conduct a comparative study of at least two central cyber powers of which there exists a feasible amount of empirical information on cyber operations. One option would be China and Russia. The fact that there exists a feasible amount of information on these states' activities opens for comparison, while also limiting the dangers of biased or skewed inferences. An analysis comparing cases – such as China and Russia – would increase our understanding of the (dis)alignment of cyber operations and foreign policy. The novel theoretical framework and methodological approach that I have developed in this thesis could support this effort of acquiring a more nuanced understanding of the impact of cyber operations on international relations in future research.

The literature review indirectly illuminated a central characteristic of the academic debate in the West: Most of the discussion has been based in US academic circles. However, there has been little focus on how the US perceives this threat. The reason seems to be the lack of openly available information on the concrete activity by the US. The main point is that understanding how the US perceived the threat could aid in distinguishing between analytical assessments that are a result of a perceived threat rather than actual activity. The field of research on cyber operations is in an early stage of development. Accordingly, it could be valuable to establish a what assessments are likely a result of a perceived threat. As the literature review showed, parts of the literature have been heavily focused on theoretical concepts, at times without grounding these in structured empirical analysis. Furthermore, changing perceptions is difficult, despite information to the contrary being presented. To achieve this research objective, it could be helpful to analyse a combination of US doctrinal

texts and the academic debate. The methods applied to this analysis could be a textual analysis, such as a discourse analysis, to identify the common representations of the cyber threat appearing in this material. This research strategy would be feasible because through a discourse analysis it is possible to establish how actors perceive the world, which would aid in defining how a threat is perceived (Bratberg 2021).

If future research were to corroborate the findings of this thesis – that information advantage serves to describe some of the activity – a potential path for future research could be to analyse the relationship between decision advantage and the security dilemma. The security dilemma assumes that a central dynamic of conflict in state relations is uncertainty over others' intentions (Jervis 1978, 62). The dilemma has held an important position in the analysis of international relations for decades. The continued relevance of this concept would therefore be interesting to explore. The assumption would be that if cyber operations are developed to gain access more efficiently to private information and therefore reduce uncertainty on other states' intentions, the central dynamic of this dilemma could be impacted. For example, Jervis (1978, 199) states that the security dilemma could be ameliorated if states are able to distinguish between offensive and defensive capabilities. Therefore, if states have access to private information on the characteristics of capabilities, the security dilemma could be ameliorated. A potential strategy for achieving this analytical objective could be to develop game theoretical models incorporating a change in this assumption of the concept of the security dilemma. This research could build on already existing models.

8 Conclusion

My analysis of likely Chinese cyber operations indicates that the activity of Chinese cyber units is aligned with policy objectives. Specifically, I argue that they align in three areas. The first is the objective of safeguarding national sovereignty and territorial integrity in the South China Sea. This objective becomes apparent through several intrusions targeted at entities, such as the military, in the context of increased tension in territorial disputes. This finding is especially apparent in Chinese relations with Vietnam and the Philippines, of which there is a long-standing dispute over the Spratly Islands and the Paracel Islands, respectively. The activity conducted by Chinese cyber units to targets in Vietnam and the Philippines has exclusively been described as information extraction. The alignment between cyber operations and policy objectives opens up to an interpretation of this cyber activity as a Chinese effort to achieve a decision advantage in relations with Vietnam and the Philippines.

A second objective is a commercial interest through the Belt and Road Initiative (BRI). The alignment between this objective and cyber unit activity has been made evident through the targeting of a Malaysian political party and railway construction company in the context of a potential contract of developing infrastructure in the country. The activity was described as information extraction. As highlighted, infrastructure development is achieved through a contract with the local government. In this process, private information is important to gain an advantage compared to other contestants for the contract. Therefore, the activity could be described as decision advantage.

The third policy objective is to unite Taiwan in mainland China. Cyber operations against targets in Taiwan had in one incident a disruptive character, while the rest is classified as information extraction. Most of the targets chosen for intrusions have been part of what the government in Taiwan regards as critical infrastructure, such as energy, telecommunications, banking and finance, central and local governments, and high-tech industry (Administration for Cyber Security 2022). The context of these intrusions has been elections in Taiwan or periods of heightened tensions between the two countries. The effect of incidents and the context could lead to a twofold interpretation of cyber operations against targets in Taiwan. Firstly, the disruptive activity could be understood as an effort to create compellent effects towards the government in Taiwan, where the activity signals a threat of future harm. This effect could be strengthened by the fact that the government in Taiwan regards this activity as

a threat to critical infrastructure, as the analysis illuminated (Cheung, Ripley, and Gladys 2021). Secondly, information extraction – particularly from government systems – could be understood as an effort to achieve a decision advantage by reducing the uncertainty of how Taiwan might act towards China in the future.

Overall, my analysis suggests an alignment between policy and practice in this area of state activity. The practice is mainly classified as information extraction. Based on the alignment between policy and practice of information extraction, I conclude that China conducts cyber operations in and related to the South China Sea for the purpose of achieving a decision advantage. Decision advantage signifies a situation where a state has achieved a reduced level of uncertainty about other states' intentions and capabilities because it has access to private information about these aspects through the exfiltration of information. In an extension of this, decision advantage could be understood as a source of power because it could lend a hand in developing more efficient policies toward other states, resulting in a higher degree of outcomes in line with the state's policy objectives.

My findings in this thesis contradict parts of the literature, which expects cyber operations to be used in conjunction with military force (see i.e., Egloff and Shires 2021; Smeets 2018) or as an instrument of disruptive or destructive effects in conflicts short of war (Buchanan 2020; Harknett and Smeets 2020b; Harknett and Fischerkeller 2019; Kello 2017; Warner 2019). Clearly, a single case study cannot provide a definite link between policy and practice. Therefore, wider investigations should develop this idea to show that behaviour in cyberspace, to some extent, could be predicted by policy objectives. This fact is overlooked in much of the literature, and our understanding of this should be expanded in future research. The simple reason for this is that to understand the utility of cyber operations in international politics; we must understand whether or how it functions as an instrument of achieving a state's foreign policy objectives. An analysis comparing cases – such as China and Russia – would increase our understanding of the (dis)alignment of cyber operations and foreign policy. The novel theoretical framework and methodological approach I developed in this thesis could support this effort to acquire a more nuanced understanding of this dynamic in future research.

9 Appendix

9.1 List of Incidents in the South China Sea from 2005-2023

The list is an overview of all publicly reported incidents occurring in the South China Sea region from around 2005 to 2023. In addition to these incidents, there is more generalized information, such as the sectors the cyber units commonly target.

Threat Actor	Year	Target	Target Sector	Effect	Source
APT30	2005 -->	Vietnam	Government and commercial	Information extraction	Alintanahin (2015).
APT30	2005 -->	Malaysia	Government and Commercial	Information extraction	Alintanahin (2015).
APT1	2007	Taiwan	Electronics company	Information extraction	Alperovitch (2011, 4, 7)
APT1	2007	Taiwan	Government owned technology company	Information extraction	Alperovitch (2011, 6–7)
APT1	2008	Taiwan	Government	Information extraction, surveillance	Alperovitch (2011, 8)
APT1	2011	Taiwan	Government	Information extraction	Alperovitch (2011, 4, 7)
APT1	2011	Vietnam	Government	Information extraction	Alperovitch (2011, 4, 7)
BlackTech	2014	Taiwan	Government and administration	Information extraction	Alintanahin (2014)
APT40	2014-2015	US	US universities with military interest, most frequently related to the navy	Information extraction	Proofpoint (2017)

APT30	2015	Vietnam	Likely energy sector, global political representatives, local IT service companies, government ministries controlling media and news organisations, and local law enforce-ment agencies	Information extraction	Baumgartner & Golovkin (2015)
APT30	2015	Philippines	Likely energy sector, global political representatives, local IT service companies, government ministries controlling media and news organisations, and local law enforcement agencies	Information extraction	Baumgartner & Golovkin (Baumgartner and Golovkin 2015)
APT30	2015	Malaysia	Likely energy sector, global political representatives, local IT service companies, government ministries controlling media and news organisations, and local law	Information extraction	Baumgartner & Golovkin (Baumgartner and Golovkin 2015)

			enforcement agencies		
APT40	2015	Taiwan	Government, heavy industry	Information extraction	FireEye (2015)
APT40	2015	Philippines	Military agencies	Information extraction	Alintanahin (2015)
APT40	2015	Philippines	Department of Justice	Information extraction	Proofpoint (2017)
APT40	2016	Taiwan	Executive Yuan	Information extraction	Ray et.al. (2016)
APT40	2016	Taiwan	Energy sector	Information extraction	Ray et.al. (2016)
APT3	2017	Vietnam	Telecommunications, science and technology research, education	Information extraction	Symantec (2019)
APT3	2017	Philippines	Telecommunications, science and technology research, education	Information extraction	Symantec (2019)
APT40	2017	Malaysia	Rail corporation	Information extraction	United States District Court Southern District of California (2019, 6)
APT40	2017	Malaysia	Political party	Information extraction	United States District Court Southern District of California (2019, 6)
APT40	2017-2018	South China Sea	Maritime industry, engineering, research institutes, private firms in the US	Information extraction	United States District Court Southern District of California (2019, 6)

APT30	2018	Vietnam	Likely defence, energy or government	Information extraction	Check Point Research (2020)
APT40	2018	US	US navy contractor	Information extraction	Liptak (2018)
BlackTech	2019	Taiwan	Media	Information extraction	Symantec(2020)
Chimera	2020	Taiwan	Superconductor industry	Information extraction	CyCraft Technology(2020a).
APT17	2020	Malaysia	Unknown		Glyer et.al (2020b).
APT17	2020	Philippines	Unknown		Glyer et.al (2020b).
APT27	2020	Vietnam	Government, military	Information extraction	Kaspersky(2021).
APT30	2020	Vietnam	Likely government entities	Information extraction	Check Point Research (2020).
APT30	2020	Philippines	Likely government entities	Information extraction	Check Point Research (2020)
APT41	2020	Taiwan	CPC corporation, semiconductor vendor, Chunghwa Telecom, eight other organizations in critical infrastructure	Disruption	CyCraft Technology (2020b)
BlackTech	2020	Taiwan	Government	Unknown	CyCraft Technology(2020c)
BlackTech	August 2019-June 2020	Taiwan	Media Company	Likely information extraction	Symantec(2020)
BlackTech	August 2019-March 2020	Taiwan	Finance Company	Likely information Extraction	Symantec(2020)

BlackTech	March 2020	Taiwan	Electronics Company	Likely information extraction	Symantec(2020)
Goblin Panda	2020-2021	Vietnam	Government, military, health, diplomacy, education, politics	Information extraction	Kaspersky(2021).
APT40	2021	Malaysia	Kasawari Gas Project	Information extraction	Raggi & Scenarelli (2022)
Bronze Butler	2021	Southeast Asia	Government	Information extraction	Check Point Research (2023)
TAG-22	2021	Philippines	Department of Information and Communications Technology	Information extraction	Insikt Group (2021)
TAG-22	2021	Taiwan	The Industrial Technology Research Institute (ITRI)	Information extraction	Insikt Group (2021)
TAG-22	2021	Taiwan	Universities	Information extraction	Insikt Group (2021)
APT10	2022	Taiwan	Financial sector	Information extraction	CyCraft Technology (2022)
APT40	2022	Malaysia	Offshore energy	Information extraction	Raggi & Scenarelli (2022)
APT40	2022	Taiwan	Yunlin Offshore windfarm	Unknown	Raggi & Scenarelli (2022)
RedAlpha	2019-2022	Taiwan	American Chamber of Commerce	Information extraction	Insikt Group (2022)
RedAlpha	2019-2022	Taiwan	Democratic Progressive Party	Information extraction	Insikt Group (2022)
RedAlpha	2019-2022	Taiwan	American Institute in Taiwan	Information extraction	Insikt Group (2022)

RedAlpha	2019-2022	Taiwan	Ministry of Foreign Affairs	Information extraction	Insikt Group (2022)
RedAlpha	2019-2022	Vietnam	Ministry of Foreign Affairs	Information extraction	Insikt Group (2022)

10 Literature

Accenture iDefence. 2019. ‘Mudcarp’s Focus on Submarine Technologies’. Accenture. https://www.accenture.com/_acnmedia/pdf-96/accenture-security-mudcarp.pdf.

Administration for Cyber Security. 2022. ‘Cyber Security Defense of Critical Infrastructure-Operations’. Administration for Cyber Security, Moda. 27 August 2022. https://moda.gov.tw/en/ACS/operations/ciip/650.

Alintanahin, Kervin. 2014. ‘PLEAD Targeted Attacks Against Taiwanese Government Agencies’. Trend Micro. 1 July 2014. https://web.archive.org/web/20140701005650/https://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2/.

———. 2015. ‘Operation Tropic Trooper: Relying on Tried-and-Tested Flaws to Infiltrate Secret Keepers’. Trend Micro. https://web.archive.org/web/20160424150645/https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-tropic-trooper.pdf.

Alperovitch, Dmitri. 2011. ‘Revealed: Operation Shady RAT’. White Paper. MacAfee. https://icscsi.org/library/Documents/Cyber_Events/McAfee%20-%20Operation%20Shady%20RAT.pdf.

Anomali Threat Research. 2019. ‘China-Based APT Mustang Panda Targets Minority Groups, Public and Private Sector Organizations’. Anomali. https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations.

Asia Maritime Transparency Initiative. 2021. ‘Contest at Kasawari: Another Malaysian Gas Project Faces Pressure’. Asia Maritime Transparency Initiative. 7 July 2021. https://amti.csis.org/contest-at-kasawari-another-malaysian-gas-project-faces-pressure/.

Bartholomew, Brian, and Juan Andres Guerrero-Saade. 2016. ‘Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks’. *Virus Bulletin Conference*.

Baumgartner, Kurt, and Maxim Golovkin. 2015. ‘The MsnMM Campaigns: The Earliest Naikon APT Campaigns’. Kaspersky Lab.

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf.

Benson, Sy, and Kawabata Kohei. 2017. 'ChessMaster Makes Its Move: A Look into Its Arsenal'. Trend Micro. 27 July 2017. https://www.trendmicro.com/en_us/research/17/g/chessmaster-cyber-espionage-campaign.html.

Bermejo, Lenart, Razor Huang, and CH Lei. 2017. 'The Trail of BlackTech's Cyber Espionage Campaigns'. Trend Micro. 22 June 2017. https://www.trendmicro.com/en_us/research/17/f/following-trail-blacktech-cyber-espionage-campaigns.html.

Betts, Richard K. 1978. 'Analysis, War, and Decision: Why Intelligence Failures Are Inevitable'. *World Politics* 31 (1): 61–89.

Biddle, Tami Davis. 2020. 'Coercion Theory: A Basic Introduction for Practitioners'. *Texas National Security Review* 3 (2). http://dx.doi.org/10.26153/tsw/8864.

Borghard, Erica D., and Shawn W. Lonergan. 2017. 'The Logic of Coercion in Cyberspace'. *Security Studies* 26 (3): 452–81. https://doi.org/10.1080/09636412.2017.1306396.

———. 2019. 'Cyber Operations as Imperfect Tools of Escalation'. *Strategic Studies Quarterly* 13 (3): 122–45.

———. 2021. 'Deterrence by Denial in Cyberspace'. *Journal of Strategic Studies*, August, 1–36. https://doi.org/10.1080/01402390.2021.1944856.

Bratberg, Øivind. 2021. *Tekstanalyse for Samfunnsvitere*. 3rd ed. Oslo: Cappelen Damm Akademisk.

Buchanan, Ben. 2016. *The Cybersecurity Dilemma. Hacking Trust and Fear Between Nations*. London: Hurst & Company.

———. 2020. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, Mass.: Harvard University Press.

Buchanan, Ben, and Fiona S. Cunningham. 2020. 'Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis'. *Texas National Security Review* 3 (4).

Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz. 2013. 'The Diamond Model of Intrusion Analysis'. ADA586960. CENTER FOR CYBER INTELLIGENCE ANALYSIS AND THREAT RESEARCH HANOVER MD. https://apps.dtic.mil/sti/citations/ADA586960.

Central Committee of the Communist Party of China. 2016. 'The 13th Five-Year Plan for Economic and Social Development of The People's Republic of China (2016-2020)'. Beijing, China: Central Compilation & Translation Press. https://en.ndrc.gov.cn/policies/202105/P020210527785800103339.pdf.

Chantzos, Ilias. 2010. 'The Trends of Cyber Incidents Leading to Large Scale Cyber-Crisis'. Symantec. https://www.enisa.europa.eu/events/2nd-enisa-conference/presentations/ilias-chantzos-symantec-the-trends-of-cyber.pdf.

Check Point Research. 2020. 'Naikon APT: Cyber Espionage Reloaded'. Check Point Research. 7 May 2020. https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/.

———. 2022. 'Cyber Security Report 2022'. Check Point Research. https://resources.checkpoint.com/cyber-security-resources/2022-cyber-security-report.

———. 2023. 'Pandas with a Soul: Chinese Espionage Attacks Against Southeast Asian Government Entities'. Check Point Research. 7 March 2023. https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/.

Chen, Joey, Hiroyuki Kakara, and Masaoki Shoji. 2019. 'Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data'. TrendMicro. https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf.

Cheung, Eric, Will Ripley, and Tsai Gladys. 2021. 'How Taiwan Is Trying to Defend against a Cyber "World War III" | CNN Business'. CNN. 24 July 2021. https://www.cnn.com/2021/07/23/tech/taiwan-china-cybersecurity-intl-hnk/index.html.

China's National People's Congress. 2011. '12th Five-Year Plan (2011-2015) for National Economic and Social Development'. Asia Pacific Energy. https://policy.asiapacificenergy.org/node/37.

CISA. 2021. 'Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department | CISA'. 20 July 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-200a.

Clarke, Richard A., and Robert K Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collins e-books.

Clinton, Hillary. 2011. ‘America’s Pacific Century’. *Foreign Policy* (blog). 11 October 2011. https://foreignpolicy.com/2011/10/11/americas-pacific-century/.

Cordesman, Anthony H, Arleigh A. Burke, and Max Molot. 2019. ‘The Critical Role of Chinese Trade in the South China Sea’. Center for Strategic and International Studies (CSIS). http://www.jstor.com/stable/resrep22586.30.

Costigan, Johanna M. 2022. ‘Why the Obvious Geopolitics of the Taiwan Policy Act of 2022 Matter’. The Diplomat. 23 September 2022. https://thediplomat.com/2022/09/why-the-obvious-geopolitics-of-the-taiwan-policy-act-of-2022-matter/.

Côté Cyr, Alexandre. 2022. ‘Mustang Panda’s Hodur: Old Tricks, New Korplug Variant’. WeLiveSecurity. 23 March 2022. https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/.

Creemers, Rogier. 2022. ‘China’s Emerging Data Protection Framework’. *Journal of Cybersecurity* 8 (1): tyac011. https://doi.org/10.1093/cybsec/tyac011.

Cronk, Terri Moon, and US Department of Defense. 2016. ‘Chinese Seize U.S. Navy Underwater Drone in South China Sea’. U.S. Department of Defense. 16 December 2016. https://www.defense.gov/News/News-Stories/Article/Article/1032823/chinese-seize-us-navy-underwater-drone-in-south-china-sea/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F1032823%2Fchinese-seize-us-navy-underwater-drone-in-south-china-sea%2F.

CrowdStrike. 2023. ‘2023 Global Threat Report’. CrowdStrike. https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf.

Cunningham, Fiona S. 2022. ‘Strategic Substitution: China’s Search for Coercive Leverage in the Information Age’. *International Security* 47 (1): 46–92. https://doi.org/10.1162/isec_a_00438.

Cyberint. 2020. ‘Targeted Ransomware Attacks in Taiwan’. Cyberint. 14 May 2020. https://cyberint.com/blog/research/targeted-ransomware-attacks-in-taiwan/.

CyCraft Research Team. 2020. ‘CyCraft Stops Year-Long Cyberattack Targeting Taiwan Semiconductors’. *CyCraft* (blog). 14 April 2020. https://cycraft.com/chimera/.

CyCraft Technology. 2020a. ‘Taiwan High-Tech Ecosystem Targeted by Foreign APT Group’. *CyCraft* (blog). 6 April 2020. https://medium.com/cycraft/taiwan-high-tech-ecosystem-targeted-by-foreign-apt-group-5473d2ad8730.

———. 2020b. ‘China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware’. *CyCraft* (blog). 2 June 2020. https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5.

———. 2020c. ‘Taiwan Government Targeted by Multiple Cyberattacks in April 2020’. *CyCraft* (blog). 8 October 2020. https://medium.com/cycraft/taiwan-government-targeted-by-multiple-cyberattacks-in-april-2020-1980acde92b0.

———. 2022. ‘China Implicated in Prolonged Supply Chain Attack Targeting Taiwan Financial Sector’. *CyCraft* (blog). 23 February 2022. https://medium.com/cycraft/china-implicated-in-prolonged-supply-chain-attack-targeting-taiwan-financial-sector-264b6a1c3525.

Department of Justice. 2018. ‘Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information’. The United States Department of Justice. 20 December 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

Department of Justice Office of Public Affairs. 2020. ‘Seven International Cyber Defendants, Including “Apt41” Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally’. The United States Department of Justice. 16 September 2020. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

———. 2021. ‘Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research’. United States Department of Jusrtice. 18 July 2021. https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

Devanny, Joe, Ciaran Martin, and Tim Stevens. 2021. ‘On the Strategic Consequences of Digital Espionage, Journal of Cyber Policy’. *Journal of Cyber Policy* 6 (3): 429–50. https://doi.org/10.1080/23738871.2021.2000628.

Doshi, Rush. 2021. *The Long Game: China’s Grand Strategy to Displace American Order*. Oxford University Press. https://doi.org/10.1093/oso/9780197527917.001.0001.

Egloff, Florian J., and James Shires. 2021. ‘Offensive Cyber Capabilities and State Violence: Three Logics of Intergration’. *Journal of Global Security Studies* 7 (1).

EuRepoC. 2023. ‘EuRepoC: European Repository on Cyber Incidents’. EuRepoC: European Repository on Cyber Incidents. 2023. https://eurepoc.eu/dashboard.

Fearon, James D. 1994. ‘Domestic Political Audiences and the Escalation of International Disputes’. *American Political Science Review* 88 (3): 577–92. https://doi.org/10.2307/2944796.

FireEye. 2015. ‘APT30 AND THE MECHANICS OF A LONG-RUNNING CYBER ESPIONAGE OPERATION’. FireEye. https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf.

———. 2018. ‘Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries’. Mandiant. 16 March 2018. https://www.mandiant.com/resources/blog/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.

———. 2019. ‘Double Dragon: APT 41, A Dual Espionage and Cyber Crime Operations’. Special Report. FireEye. https://web.archive.org/web/20191219145707/https://content.fireeye.com/apt-41/rpt-apt41.

Fischerkeller, Michael P., and Richard J. Harknett. 2017. ‘Deterrence Is Not a Credible Strategy for Cyberspace’. *Orbis* 61 (3): 381–93. https://doi.org/10.1016/j.orbis.2017.05.003.

Fraser, Nalani, Fred Plan, Jaqueline O´Leary, Vincent Cannon, Raymond Leong, Dan Perez, and Chi-En Shen. 2019. ‘APT41: A Dual Espionage and Cyber Crime Operation’. Mandiant. 7 August 2019. https://www.mandiant.com/resources/blog/apt41-dual-espionage-and-cyber-crime-operation.

Fraunhofer FKIE. 2023. ‘Malpedia (Fraunhofer FKIE)’. Malpedia Fraunhofer FKIE. 2023. https://malpedia.caad.fkie.fraunhofer.de/.

Freund, Eleanora. 2017. ‘Freedom of Navigation in the South China Sea: A Practical Guide’. Asia Maritime Transparency Initiative. 10 August 2017. https://amti.csis.org/freedom-of-navigation-practical-guide/.

Gartzke, Erik. 2013. ‘The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth’. *International Security* 38 (2): 41–73. https://doi.org/10.1162/isec_a_00136.

Gartzke, Erik, and Jon R. Lindsay. 2015. ‘Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace’. *Security Studies* 24 (2): 316–48. https://doi.org/DOI: 10.1080/09636412.2015.1038188.

Gilli, Andrea, and Mauro Gilli. 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): 141–89. https://doi.org/10.1162/isec_a_00337.

Glyer, Christopher, Dan Perez, Sarah Jones, and Steve Miller. 2020a. 'This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits'. Mandiant. https://www.mandiant.com/resources/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.

———. 2020b. 'This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits'. Mandiant. 25 March 2020. https://www.mandiant.com/resources/blog/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.

Goodman, Will. 2010. 'Cyber Deterrence: Tougher in Theory than in Practice?' *Strategic Studies Quarterly; Maxwell Air Force Base* 4 (3): 102–35.

Grossman, Derek. 2018. 'Why March 2018 Was an Active Month in Vietnam's Balancing Against China in the South China Sea'. The Diplomat. 23 March 2018. https://thediplomat.com/2018/03/why-march-2018-was-an-active-month-in-vietnams-balancing-against-china-in-the-south-china-sea/.

Hải, Đỗ Thanh, and Nguyễn Thị Linh. 2021. 'Vietnam and the East Sea in Its Strategic Thinking'. In *Security, Strategy, and Military Dynamics in the South China Sea*, edited by Gordon Houlden, Scott Romaniuk, and Nong Hong, 1st ed., 101–16. Bristol University Press. https://doi.org/10.46692/9781529213478.007.

Hansen, Lene. 2006. *Security as Practice: Discourse Analysis and the Bosnian War*. 1st ed. London & New York: Routledge.

Harknett, Richard J., and Michael P. Fischerkeller. 2019. 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation'. *The Cyber Defense Review*, SPECIAL EDITION: International Conference on Cyber Conflict (CYCON U.S.), November 14-15, 2018: Cyber Conflict During Competition, , 267–87.

Harknett, Richard J, and Max Smeets. 2020a. 'Cyber Campaigns and Strategic Outcomes'. *Journal of Strategic Studies*. https://doi.org/10.1080/01402390.2020.1732354.

Harknett, Richard J., and Max Smeets. 2020b. 'Cyber Campaigns and Strategic Outcomes'. *Journal of Strategic Studies*. https://doi.org/doi.org/10.1080/01402390.2020.1732354.

———. 2022. ‘Cyber Campaigns and Strategic Outcomes’. *Journal of Strategic Studies* 45 (4): 534–67. https://doi.org/10.1080/01402390.2020.1732354.

Harnisch, Sebastian, Kerstin Zettl-Schabath, Kim Schuck, Matthias Schulze, Annegret Bendiek, Jakob Bund, Camille Borrett, Matthias Kettemann, Martin Müller, and Mika Kerttunen. 2023. ‘Codebook European Repository of Cyber Incidents (EuRepoC) 1.0’. European Repository of Cyber Incidents. https://strapi.eurepoc.eu/uploads/Eu_Repo_C_Codebook_1_0_56e75eac57.pdf.

Hegel, Tom. 2018. ‘Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers’. 401trg. https://401trg.github.io/pages/burning-umbrella.html.

Huang, Razor. 2016. ‘New Targeted Attack Group Buys BIFROSE Code, Works in Teams’. Trend Micro. 16 February 2016. https://web.archive.org/web/20160216043456/https://blog.trendmicro.com/trendlabs-security-intelligence/new-targeted-attack-group-buys-bifrose-code-works-in-teams/.

Huong, Le Thu. 2020. ‘Fishing While the Water Is Muddy: China’s Newly Announced Administrative Districts in the South China Sea’. Asia Maritime Transparency Initiative. 6 May 2020. https://amti.csis.org/fishing-while-the-water-is-muddy-chinas-newly-announced-administrative-districts-in-the-south-china-sea/.

IBM Security X-Force. 2023. ‘IBM Security X-Force Threat Intelligence Index 2023’. IBM Security. https://www.ibm.com/downloads/cas/DB4GL8YM.

Insikt Group. 2017. ‘Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3’. Recorded Future. https://web.archive.org/web/20220303103643/http://www.recordedfuture.com/chinese-mss-behind-apt3/.

———. 2021. ‘Chinese State-Sponsored Cyber Espionage Activity Supports Expansion of Regional Power and Influence in Southeast Asia’. CTA-CN-2021-1208. Cyber Threat Analysis. Recorded Future. https://go.recordedfuture.com/hubfs/reports/cta-2021-1208.pdf.

———. 2022. ‘RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations’. TA-CN-2020-0816. Cyber Threat Analysis. Recorded Future. https://www.recordedfuture.com/redalpha-credential-theft-campaign-targeting-humanitarian-thinktank.

Jansen, Wouter. 2021. ‘Abusing Cloud Services to Fly under the Radar’. NCC Group Research Blog. 12 January 2021. https://research.nccgroup.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/.

Jennings, Ralph. 2020. ‘China, Vietnam Try to Make Amends After Stormy Start to 2020’. VOA. 2 September 2020. https://www.voanews.com/a/east-asia-pacific_china-vietnam-try-make-amends-after-stormy-start-202/6195334.html.

Jervis, Robert. 1978. ‘Cooperation Under the Security Dilemma’. *World Politics* 30 (2): 167–214. https://doi.org/10.2307/2009958.

Kaspersky. 2021. ‘Advanced Threat Actors Engaged in Cyberespionage in APAC up Their Game in New Campaign’. Kaspersky.Com. 26 May 2021. https://www.kaspersky.com/about/press-releases/2021_advanced-threat-actors-engaged-in-cyberespionage-in-apac-up-their-game-in-new-campaign.

Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven, Conn.: Yale University Press.

Kosar, Kevin R. 2011. ‘The Quasi Government: Hybrid Organizations with Both Government and Private Sector Legal Characteristics’. RL30533. CRS Report for Congress. Congressional Research Service. https://sgp.fas.org/crs/misc/RL30533.pdf.

Kostyuk, Nadiya, and Yuri M. Zhukov. 2019. ‘Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?’ *Journal of Conflict Resolution* 63 (2): 317–47. https://doi.org/10.1177/0022002717737138.

Kozy, Adam. 2018. ‘Two Birds, One STONE PANDA’. Crowdstrike.Com. 30 August 2018. https://www.crowdstrike.com/blog/two-birds-one-stone-panda/.

Kucharaski, Jeff. 2022. ‘Taiwan’s Greatest Vulnerability Is Its Energy Supply’. The Diplomat. 23 September 2022. https://thediplomat.com/2022/09/taiwans-greatest-vulnerability-is-its-energy-supply/.

Kuo, Lily. 2020. ‘Taiwan Election: Tsai Ing-Wen Wins Landslide in Rebuke to China’. *The Observer*, 11 January 2020, sec. World news. https://www.theguardian.com/world/2020/jan/11/taiwan-re-elects-tsai-ing-wen-as-president-in-clear-message-to-china.

Kuo, Mercy A. 2022. ‘How China’s Military Is Preparing for War With Taiwan’. The Diplomat. 19 November 2022. https://thediplomat.com/2022/09/how-chinas-military-is-preparing-for-war-with-taiwan/.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Libicki, Martin C., and Olesya Tkacheva. 2020. ‘Cyberspace Escalation: Ladders or Lattices?’ *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* 13.

Liff, Adam P. 2012. ‘Cyberwar: A New “Absolute Weapon”? The Proliferation of Cyberwarfare Capabilities and Interstate War’. *Journal of Strategic Studies* 35 (3): 401–28. https://doi.org/10.1080/01402390.2012.663252.

Lin, Herbert. 2012. ‘Escalation Dynamics and Conflict Termination in Cyberspace’. *Strategic Studies Quarterly* 6 (3): 46–70.

Lindsay, Jon R. 2013. ‘Stuxnet and the Limits of Cyber Warfare’. *Security Studies* 22 (3): 365–404. https://doi.org/10.1080/09636412.2013.816122.

———. 2015a. ‘The Impact of China on Cybersecurity: Fiction and Friction’. *International Security* 39 (3): 7–47.

———. 2015b. ‘Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack’. *Journal of Cybersecurity*, November, tyv003. https://doi.org/10.1093/cybsec/tyv003.

———. 2017. ‘Restrained by Design: The Political Economy of Cybersecurity’. *Digital Policy, Regulation, and Governance* 19 (6): 493–514.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190201265.001.0001.

Lindsay, Jon R., and Erik Gartzke. 2018. ‘Coercion through Cyberspace: The Stability-Instability Paradox Revisited’. In *Coercion: The Power to Hurt in International Politics*. New York: Oxford University Press.

Liptak, Andrew. 2018. ‘Chinese Hackers Reportedly Stole Data Related to Secret Projects from a US Navy Contractor’. The Verge. 9 June 2018. https://www.theverge.com/2018/6/9/17444312/chinese-hackers-reportedly-stole-data-related-to-secret-projects-from-a-us-navy-contractor.

Lowenthal, Mark M. 2017. *Intelligence: From Secrets to Policy*. 7th ed. Los Angeles: CQ Press.

Lynn, William J., III. 2010. ‘Defending a New Domain: The Pentagon’s Cyberstrategy’. *Foreign Affairs* 89 (5): 97–108.

Mahnken, Thomas G. 2011. ‘Cyber War and Cyber Warfare’. In *America’s Cyber Future: Security and Prosperity in the Information Age*, edited by Kristin Lord and Travis Sharp, 2:53–62. Washington, DC: CNAS.

Maizland, Lindsay. 2023. ‘Why China-Taiwan Relations Are So Tense’. Council on Foreign Relations. 18 April 2023. https://www.cfr.org/backgrounder/china-taiwan-relations-tension-us-policy-biden.

Malhotra, Asheer, An, and Kendall McKay. 2022. ‘Mustang Panda Deploys a New Wave of Malware Targeting Europe’. Cisco Talos Blog. 5 May 2022. https://blog.talosintelligence.com/mustang-panda-targets-europe/.

Maschmeyer, Lennart. 2021. ‘The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations’. *International Security* 46 (2): 51–90. https://doi.org/10.1162/isec_a_00418.

Maybaum, Markus. 2013. ‘Technical Methods, Techniques, Tools and Effects of Cyber Operations’. In *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, edited by Katharina Ziolkowski, 103–31. Tallinn: NATO CCD COE Publication.

McConkey, Kris, Jason Smart, Rachel Mullan, and Allison Wikoff. 2022. ‘Cyber Threat 2021: A Year in Retrospect - Annex’. PwC. https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html.

McGregor, Charles. 1993. ‘Southeast Asia’s New Security Challenges’. *The Pacific Review* 6 (3): 267–76. https://doi.org/10.1080/09512749308719046.

Mesquita, Bruce Bueno de, James D. Morrow, and Ethan R. Zorick. 1997. ‘Capabilities, Perception, and Escalation’. *American Political Science Review* 91 (1): 15–27. https://doi.org/10.2307/2952256.

Meyers, Adam. 2018. ‘Wicked Spider Adversary | Threat Actor Profile | CrowdStrike’. Crowdstrike.Com. 26 July 2018. https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider/.

Microsoft. 2022. ‘Microsoft Digital Defense Report 2022: Illuminating the Threat Landscape and Empowering Digital Defense’. Microsoft. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us.

Microsoft Digital Security Unit. 2022. ‘An Overview of Russia’s Cyberattack Activity in Ukraine’. Special Report. Microsoft. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

Miller, Maggie. 2022. ‘Taiwan Presidential Office Website Hit by Cyberattack Ahead of Pelosi Visit’. POLITICO. 2 August 2022.

https://www.politico.com/news/2022/08/02/taiwan-presidential-office-website-hit-by-cyberattack-ahead-of-pelosi-visit-00049255.

MITRE ATT&CK. 2023. ‘Groups’. MITRE ATT&CK. 2023. https://attack.mitre.org/groups/.

Nakashima, Ellen, and Paul Sonne. 2018. ‘China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare’. *Washington Post*, 9 June 2018. https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html.

Nasheri, Hedieh. 2004. *Economic Espionage and Industrial Spying*. Cambridge Studies in Criminology. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511610288.

Novetta Threat Research Group. 2014. ‘Operation SMN: Axiom Threat Actor Group Report’. Novetta. https://web.archive.org/web/20150420064803/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf.

Nye, Joseph S. 2011. ‘Nuclear Lessons for Cyber Security’: Fort Belvoir, VA: Defense Technical Information Center. https://doi.org/10.21236/ADA553620.

———. 2017. ‘Deterrence and Dissuasion in Cyberspace’. *International Security* 41 (3): 44–71. https://doi.org/10.1162/ISEC_a_00266.

Nye Jr., Joseph S. 2016. ‘Deterrence and Dissuasion in Cyberspace’. *International Security* 41 (3): 44–71.

Permanent Court of Arbitration. 2016. The South China Sea Arbitration (The Republic of Philippines v. The People’s Republic of China). Permanent Court of Arbitration (PCA).

Permanent Mission of the People’s Republic of China. 2009. ‘Note Verbale CLM 17/2009’. United Nations. https://www.un.org/depts/los/clcs_new/submissions_files/mysvnm33_09/chn_2009re_mys_vnm_e.pdf.

Plan, Fred, Nalani Fraser, Jaqueline O´Leary, Vincent Cannon, and Ben Read. 2019. ‘APT40: Examining a China-Nexus Espionage Actor’. Mandiant. 4 March 2019. https://www.mandiant.com/resources/blog/apt40-examining-a-china-nexus-espionage-actor.

Proofpoint. 2017. ‘Leviathan: Espionage Actor Spearphishes Maritime and Defense Targets | Proofpoint US’. Proofpoint. 16 October 2017. https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets.

Raggi, Michael, and Sveva Scenarelli. 2022. ‘TA423 - Red Ladon ScanBox Campaigns Identified’. Proofpoint. 25 August 2022. https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea.

Ray, Vicky, Robert Falcone, Jen Osborn-Miller, and Tom Lancaster. 2016. ‘Tropic Trooper Targets Taiwanese Government and Fossil Fuel Provider With Poison Ivy’. *Unit 42* (blog). 22 November 2016. https://unit42.paloaltonetworks.com/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/.

Regan, Helen. 2019. ‘Kim Jong Un Arrives in Vietnam to a Red Carpet Welcome Ahead of Summit’. CNN. 26 February 2019. https://www.cnn.com/2019/02/25/asia/kim-jong-un-vietnam-arrive-train-intl/index.html.

Reuters. 2020. ‘Vietnam Protests Beijing’s Expansion in Disputed South China Sea’. *Reuters*, 19 April 2020, sec. Emerging Markets. https://www.reuters.com/article/us-vietnam-china-southchinasea-idUSKBN2210M7.

Rid, Thomas. 2012. ‘Cyber War Will Not Take Place’. *Journal of Strategic Studies* 35 (1): 5–32. https://doi.org/10.1080/01402390.2011.608939.

———. 2013. *Cyber War Will Not Take Place*. New York: Oxford University Press.

Rid, Thomas, and Ben Buchanan. 2015. ‘Attributing Cyber Attacks’. *Journal of Strategic Studies* 38 (1–2): 4–37. https://doi.org/10.1080/01402390.2014.977382.

Ronfeldt, David, and John Arquilla. 1993. ‘Cyberwar Is Coming!’ *Comparative Strategy* 12 (2): 141–65.

Rovner, Joshua. 2019. ‘Cyber War as an Intelligence Contest’. *War on the Rocks*, 16 September 2019. https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

Sacks, David. 2023. ‘Threatening to Destroy TSMC Is Unnecessary and Counterproductive’. Council on Foreign Relations. 9 May 2023. https://www.cfr.org/blog/threatening-destroy-tsmc-unnecessary-and-counterproductive.

Schelling, Thomas C. 2008. *Arms and Influence*. Yale University Press.

Seawright, Jason, and John Gerring. 2008. ‘Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options’. *Political Research Quarterly* 61 (2): 294–308. https://doi.org/10.1177/1065912907313077.

Secureworks Counter Threat Unit. 2017a. ‘BRONZE BUTLER | Secureworks’. 12 October 2017. https://www.secureworks.comhttp://www.secureworks.com/research/threat-profiles/bronze-butler.

———. 2017b. ‘BRONZE UNION | Secureworks’. 12 October 2017. https://www.secureworks.comhttp://www.secureworks.com/research/threat-profiles/bronze-union.

———. 2019. ‘BRONZE PRESIDENT | Secureworks’. 29 December 2019. https://www.secureworks.comhttp://www.secureworks.com/research/threat-profiles/bronze-president.

———. 2023a. ‘BRONZE ATLAS’. 2023. https://www.secureworks.comhttp://www.secureworks.com/research/threat-profiles/bronze-atlas.

———. 2023b. ‘BRONZE CANAL | Secureworks’. 2023. https://www.secureworks.comhttp://www.secureworks.com/research/threat-profiles/bronze-canal.

———. 2023c. ‘BRONZE GENEVA | Secureworks’. 2023. https://www.secureworks.comhttp://www.secureworks.com/research/threat-profiles/bronze-geneva.

———. 2023d. ‘BRONZE KEYSTONE | Secureworks’. 2023. https://www.secureworks.comhttp://www.secureworks.com/research/threat-profiles/bronze-keystone.

———. 2023e. ‘BRONZE MOHAWK | Secureworks’. 2023. https://www.secureworks.comhttp://www.secureworks.com/research/threat-profiles/bronze-mohawk.

———. 2023f. ‘BRONZE RIVERSIDE | Secureworks’. 2023. https://www.secureworks.comhttp://www.secureworks.com/research/threat-profiles/bronze-riverside.

Siedler, Ragnhild Endresen. 2016. ‘Hard Power in Cyberspace: CNA as a Political Means’. In *2016 8th International Conference on Cyber Conflict (CyCon)*, 23–36. Tallinn, Estonia: IEEE. https://doi.org/10.1109/CYCON.2016.7529424.

Sims, Jennifer E. 2022. ‘A Theory of Intelligence in International Politics’. In *Decision Advantage*, by Jennifer E. Sims, 1st ed., 405-C13.P174. Oxford University PressNew York. https://doi.org/10.1093/oso/9780197508046.003.0013.

Singer, J. David. 1958. ‘Threat-Perception and the Armament-Tension Dilemma’. *Journal of Conflict Resolution* 2 (1): 90–105. https://doi.org/10.1177/002200275800200110.

———. 1988. ‘Reconstructing the Correlates of War Dataset on Material Capabilities of States, 1816–1985’. *International Interactions* 14 (2): 115–32. https://doi.org/10.1080/03050628808434695.

Singer, J. David, Bremer Stuart, and John Stuckey. 1972. ‘Capability Distribution, Uncertainty, and Major Power War, 1820-1965’. In *Peace, War, and Numbers*, edited by Bruce M. Russett. Beverly Hills, London: SAGE Publications Ltd.

Slayton, Rebecca. 2017. ‘What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment’. *International Security* 41 (3): 72–109. https://doi.org/10.1162/isec_a_00267.

Smeets, Max. 2018. ‘The Strategic Promise of Offensive Cyber Operations’. *Strategic Studies Quarterly* 12 (3): 90–113.

Soesanto, Stefan, and Max Smeets. 2021. ‘Cyber Deterrence: The Past, Present, and Future’. In *NL ARMS Netherlands Annual Review of Military Studies*. NL ARMS. Springer Nature. https://directory.doabooks.org/handle/20.500.12854/39709.

State Service of Special Communication and Information Protection of Ukraine. 2023. ‘Russia’s Cyber Tactics: Lessons Learned in 2022 — SSSCIP Analytical Report on the Year of Russia’s Full-Scale Cyberwar against Ukraine’. Kyiv: Ukraine. https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine.

Storey, Ian James. 1999. ‘Creeping Assertiveness: China, the Philippines and the South China Sea Dispute’. *Contemporary Southeast Asia* 21 (1): 95–118.

Stout, Mark, and Michael Warner. 2018. ‘Intelligence Is as Intelligence Does’. *Intelligence and National Security* 33 (4): 517–26. https://doi.org/10.1080/02684527.2018.1452593.

Suffian, Jusoh. 2018. ‘The Impact of the BRI on Trade and Investment in ASEAN’. In *China’s Belt and Road Initiative (BRI) and Southeast Asia*. Kuala Lumpur: CIMB Southeast Asia Research. https://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-China-SEA-BRI.pdf.

Sungbahadoor, Patrick. 2017. ‘APT3, Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110, Group G0022’. MITRE ATT&CK. 31 May 2017. https://attack.mitre.org/groups/G0022/.

Symantec. 2019. ‘Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak’. Symantec Enterprise Blogs. 2019. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit.

———. 2020. ‘Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors | Symantec Enterprise Blogs’. 29 September 2020. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt.

———. 2023. ‘Blackfly: Espionage Group Targets Materials Technology’. 28 February 2023. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackfly-espionage-materials.

The State Council Information Office of the People’s Republic of China. 2019. ‘Full Text: China’s National Defense in the New Era’. The State Council Information Office of the People’s Republic of China. July 2019. http://www.scio.gov.cn/zfbps/ndhf/39911/Document/1660528/1660528.htm.

The State Council The Peoples Republic of China. 2011. ‘China’s Peaceful Development’. The State Council The People’s Republic of China. 2011. http://english.www.gov.cn/archive/white_paper/2014/09/09/content_281474986284646.htm.

Tung, Chen-Yuan. 2016. ‘Prospects of Taiwan-China Relations after the 2016 Elections’. *American Journal of Chinese Studies* 23 (1): 1–6.

Tweed, David. 2018. ‘Chinese Hackers Hit U.S. Firms Linked to South China Sea Dispute - Bloomberg’. Bloomberg. 15 June 2018. https://web.archive.org/web/20180615161843/https://www.bloomberg.com/news/articles/2018-03-16/china-hackers-hit-u-s-firms-linked-to-sea-dispute-fireeye-says.

U-Jin, Adrian Ang, and Olli Pekka Suorsa. 2022. ‘The “New Normal” in PLA Incursions Into Taiwan’s ADIZ’. The Diplomat. 27 September 2022. https://thediplomat.com/2022/09/the-new-normal-in-pla-incursions-into-taiwans-adiz/.

United States District Court Southern District of California. 2019. ‘United States of Amerivs v. Ding Xiaoyang, Cheng Quingmin, Zhu Yunmin, Wu Shurong’. United States District Court Southern District of California. https://www.justice.gov/opa/press-release/file/1412916/download.

Valencia, Mark J. 1988. ‘The Spratly Islands: Dangerous Ground in the South China Sea’. *The Pacific Review* 1 (4): 438–43. https://doi.org/10.1080/09512748808718792.

Valeriano, Brandon. 2018. ‘China and the Technology Gap: Chinese Strategic Behavior in Cyberspace’. In *Cyber Strategy: The Evolving Character of Power and Coercion*, by Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, 28. Oxford University Press. https://doi.org/10.1093/oso/9780190618094.001.0001.

Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press. https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190618094.001.0001/oso-9780190618094.

Volz, Dustin. 2019. 'Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets'. *Wall Street Journal*, 5 March 2019. https://cs.brown.edu/courses/csci1800/sources/2019_03_05_WSJ_ChineseHackersTargetUniversitiesInPursuitOfMaritimeMilitarySecrets.pdf.

Voo, Julia, Irfan Hemani, and Daniel Cassidy. 2022. 'National Cyber Power Index 2022'. Cambridge, Mass.: Belfer Center for Science and International Affairs. www.belfercenter.org/project/cyber-project.

Vuving, Alex. 2017. 'Tracking the Philippines' Force Build-up in the South China Sea'. Asia Maritime Transparency Initiative. 1 November 2017. https://amti.csis.org/tracking-philippines-force-build-up/.

Warner, Michael. 2002. 'Wanted: A Definition of Intelligence'. *Studies in Intelligence* 46 (3). https://apps.dtic.mil/sti/pdfs/ADA525816.pdf.

———. 2019. 'A Matter of Trust: Covert Action Reconsidered'. *Studies in Intelligence* 63 (4): 33–41.

Wheaton, Kristan J, and Michael T Beerbower. 2006. 'Towards a New Definition of Intelligence'. *Stanford Law and Policy Review* 17 (319). https://law.stanford.edu/publications/towards-new-definition-intelligence/.

Willams, Craig, Martin Lee, and Joel Esler. 2014. 'Threat Spotlight: Group 72'. *Cisco Blogs* (blog). 14 October 2014. https://blogs.cisco.com/security/talos/threat-spotlight-group-72.

Xinhua News Agency. 2021. 'Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035'. Center for Security and Emerging Technology (CSET). https://cset.georgetown.edu/publication/china-14th-five-year-plan/.

Yan, Jinny. 2018. 'The BRI in Southeast Asia'. In *China's Belt and Road Initiative (BRI) and Southeast Asia*. Kuala Lumpur: CIMB Southeast Asia Research. https://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-China-SEA-BRI.pdf.

Yang, Li. 2021. 'China's Security Interests and Strategies in the South China Sea'. In *Security, Strategy, and Military Dynamics in the South China Sea*, edited by Gordon

Houlden, Scott Romaniuk, and Nong Hong, 1st ed., 63–78. Bristol University Press. https://doi.org/10.46692/9781529213478.005.

Yin, Robert K. 2009. *Case Study Research: Design and Methods*. Fourth. Thousand Oaks, California: SAGE Publications Ltd.

Zeng, Jinghan, Yuefan Xiao, and Shaun Breslin. 2015. 'Securing China's Core Interests: The State of the Debate in China'. *International Affairs* 91 (2): 245–66. https://doi.org/10.1111/1468-2346.12233.

Zenglein, Max J, and Anna Holzmann. 2019. 'Evolving Made in China 2025: China's Industrial Policy in the Quest for Global Tech Leadership'. 8. Merics Papers on China. Berlin, Germany: MERICS | Mercator Institute for China Studies. https://kritisches-netzwerk.de/sites/default/files/merics_-_evolving_made_in_china_2025_-_chinas_industrial_policy_in_the_quest_for_global_tech_leadership_-_2._juli_2019_-_80_seiten.pdf.

Zhang, Feng. 2017. 'Chinese Thinking on the South China Sea and the Future of Regional Security'. *Political Science Quarterly* 132 (3): 435–66. https://doi.org/10.1002/polq.12658.