Factors Determining Cyber Strategy: the Differences Between Active and Passive Cyber Attacks

By

Francis William Engli

A thesis

presented to the University of Waterloo

in fulfilment of the

thesis requirements for the degree of

Master of Arts

In

Political Science

Waterloo, Ontario, Canada, 2020

Author’s Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

China and Russia have increased their pursuit of using cyber-attacks as an offensive tool in overall state strategy. China pursues passive cyber-attacks while Russia pursues active cyber-attacks. This study intends to answer the question: what factors encourage China and Russia to pursue differing cyber-attack strategies? A review of the current literature reveals that four primary factors influence cyber strategy: economic incentive, international hierarchy, institutional organization, and state interpretation of deterrence. These four factors are analyzed through policy analysis, using documents from NGOs, and government documents from the US, China and Russia. The results conclude that each factor contributes significantly to cyber-strategy; however, state interpretation of deterrence is the only factor that adequately explains China's and Russia's choices in determining cyber strategy. The study discusses the implications of these findings and possible areas for further research.

Keywords: Active Cyber Attacks, Passive Cyber Attacks, Cyber Strategy, China and Russia

Acknowledgments

I would like to express my great gratitude to Professor Kitchen, my research supervisor, for her patient guidance, endless encouragement and useful critiques of this research work. Even in the current less-optimal circumstances she continued to provide consistent help and moral boosting to complete this project.

I would also like to express my deep appreciation to Professor Lanoszka for his valuable suggestions over the course of this research work. His willingness to give his time so generously has been very much appreciated.

I would like to offer my special thanks to Nadine Thibeh and Kevin McCaffrey who always had time to listen and help.

Dedication

For my parents, who always encourage me to go further.

Table of Contents

List of Tables

Introduction

The state embraced the internet during the Cold War to secure itself by providing an interconnected system capable of withstanding nuclear destruction. Paradoxically, it has created new threats since these new cyber capabilities have opened new spaces in which states and their institutions are now vulnerable. The state has embraced cyber capabilities to increase its efficiency and effectiveness without anticipating the risks that online exposure creates. Cyber attacks have become a tool of offence, exploiting the vulnerabilities in rival state's systems. This use of cyber attacks has become a new normal in international relations, with states using cyber capabilities to survey, sabotage, and steal from their rival states.

When the Advanced Research Projects Agency Network (ARPANET, precursor to the internet) was first conceived in 1966, the Unites States (US) was a global hegemon, challenged by the Soviet Union. Today, the US maintains its hegemon status but faces challenges by two rival states: China and a resurgent Russia. Both states seek to reduce US hegemony to reshape the world order to their benefits. They each have embraced cyber technology after significant hesitation due to communist ruling ideology and are heavily investing in their cyber capabilities, trying to use this technology in the most effective way to help gain an advantage against their American rival. However, Russia and China are using their newly found cyber capabilities in inherently different ways, through active and passive cyber attacks. Russia engages in more "active" attacks against their foe than a typical state. An "active attack" is a cyber-attack specifically designed to disrupt or damage the recipient state. However, China favours "passive" cyber attacks, which primarily focus on information collection and internal monitoring of the attack's victim. This proposed the question: Why do both states use their offensive cyber capabilities so differently when facing a similar threat? I hypothesize that China and Russia’s fundamental interpretation of conventional deterrence influences how cyber attacks are used in both countries.

In this study, I will examine the predominant factors in determining cyber-attack strategy. These four factors: economic incentives, international hierarchy, institutional organization, and interpretation of deterrence, provide a well-rounded analysis of the motivations behind the strategy of cyber attacks. The reasons for comparison is that these two states are the primary challengers to US global hegemony, both are non-democratic, both have a similar history of communist ideology, and both challenge the US throughout the latter half of the 20th century. This analysis will provide a comparison since China and Russia are the most prolific in reported cyber attacks against the US and NATO allies. Few other countries challenge the US, and even fewer with sophisticated cyber capabilities can attack the US. China and Russia are the only two states outside of NATO influence that can carry out multiple, long-term cyber operations. Iran and North Korea have fewer capabilities than either China or Russia. They remain relatively isolated from the international community as opposed to China and Russia, which are integrated and are two of the five permanent votes on the UN Security Council. China and Russia have key similarities, but their differences in cyber strategy are what I will be highlighting.

This study will provide insight into how states determine their offensive cyber strategies, whether they focus on active or passive attacks. This can infer how states might engage cyber attacks in the future. It will also illuminate different factors behind decision making in a cyber capable world and provide the basis upon which such attacks can be anticipated, and the effects mitigated. Current research focuses on the conceptual ontology of cyber attacks or specific attack case studies. This research will contribute to the limited literature on cyber strategies by introducing a policy analysis framework rarely done due to its historical novelty of cyber attacks in the state security realm.

Basics of Cyber Conflict

Due to the novelty of cyber operations, there is still debate on the terminology of cyber capabilities. When analyzing cyber strategy, there must be a precise terminology so that there is a clear line delineating what consists of a cyber "attack." The terminology of what a cyber-attack consists of is itself under review by several authors. Valeriano (2015) argues that offensive cyber operations are distinguished between attacks and operations. Attacks are sophisticated attempts to breach the security of a computerized system. An example of an "attack" would be Russian attempts to compromise voting registration records in the 2019 US midterm elections. Operations are an attempt to breach security using the user's ignorance to the offensive actor's advantage. An example of an operation would be the Russian 2016 Democratic National Convention (DNC) hacks, which targeted an individual (John Podesta) to unknowingly give his password to cyber operatives, which then were used to gain access to DNC documents. Authors such as Carr (2012) and Reveron (2012) do not distinguish these two types of offensive cyber operations due to problems of discovery, attribution, and response problems. In this research, I will adhere to Valeriano's definitions and maintain analysis of cyber "attacks" rather than the simpler cyber operations.

A significant issue facing states when determining cyber strategy is the problem of attribution. No cyber-attack, be it passive or active, can be attributed to a specific actor with 100% certainty (Reveron, 2012). Attribution creates a large amount of leeway for states in creating a cyber-attack strategy since there is a high chance that the attacking actor can attack without repercussions. The culprits can be inferred through investigation, but proving beyond doubt is utterly impossible due to the nature of computing (This problem of attribution increases uncertainty since nobody can effectively blame another actor for a cyber-attack.). Reinforcing a norm of non-conventional response since no state wants to appear to attack another with conventional military capabilities without justified cause (Clausewitz, 1832). Trying to determine attribution through the timeline of attacks can also be uncertain due to the sources provided and when the attack is discovered; often, cyber attacks can go weeks or months without detection (Mandiant Report, 2014). When regarding the theft of intelligence, there can be little indication besides leaking the information that a theft took place. The problem of attribution creates a high incentive for the state to pursue passive cyber attacks due to the low chance of discovery, while also closing the information gaps that cyber conflict inherently presents.

No cyber-attack has merited a conventional military response from the defending state (Carr, 2012; Berghel 2017). The first reported cyber attack was carried out by the Americans by allegedly sabotaging a piece of pipeline equipment, which used primitive programming to overload the pressure valve, causing a massive explosion (Carr, 2012). This attack remains unverified since both the Soviet Union and the US denied this ever taking place. However, there is enough compelling evidence to infer that this was the first known instance of a "cyber" attack (Rid, 2012). This attack merited no conventional response from the Soviet Union. More recently, we can see this norm of non-conventional response continued in both the passive cyber attack "Titan Rain" carried out by China on US military infrastructure, and the active cyber attack "Stuxnet" which destroyed Iranian nuclear equipment (Mandiant Report, 2014; Lindsay, 2013; Rid, 2012; Austin, 2014). This norm is established today with all countries even though some states threaten conventional responses, but none have followed through (Valeriano, 2015). The norm is also due to the constant inflow of cyber attacks that states receive. Most states are being attacked by state and non-state actors constantly, to the point of singling out all but the most severe attacks are incredibly difficult (Carr, 2012; Reveron, 2012). Most of these attacks are benign and are testing weaknesses within the state for further exploitation (Mandiant Report, 2014). However, this constant cyber conflict between state, non-state and regional actors has solidified the norm of non-conventional response even in the face of physically destructive active cyber attacks, creating an incentive to use cyber attacks. It creates an inherently low-risk strategy with the potential for comparatively high rewards due to the norm of non-conventional response.

Finally, the last major issue regarding cyber capabilities is that of the offensive advantage. Cyber capabilities have a natural offensive advantage due to technological innovation (Carr, 2012; Reveron, 2013). Cyber attacks can only be used once or twice, then the defender (if they have realized the attack) will learn how the attack happened and defend itself against it. However, these defensive actions will only protect against the previously obsolete attack. The fast-paced nature of technological innovation gives the advantage to the attacker. It is not realistic for a state or region to effectively monitor all internet and computer traffic; therefore, they must hoard their resources to protect their most vulnerable assets. These defensive capabilities must be used sparingly due to logistical limitations; consequently, the attacker can always find new vulnerable areas or exploit previously unseen flaws. Due to the nature of cyber attacks, and their reliance on exploiting flaws within programming, defenders often do not know what resources they must prioritize (Carr, 2012). This offensive advantage contributes to cyber attack strategy since a state cannot invest too many resources in a single attack or defensive strategies, since it has a one-use limitation, and often unreliable in its success. When pursuing an active attack, this one-use policy is very relevant as the likelihood of discovery is far higher than passive attacks that can go undetected for months or years.

Basis of Comparison

China and Russia have unique history and circumstances which formed their cyber strategies, but they also have some key commonalities. China's cybersecurity realm has been expanding rapidly since the early 2000s. The opening of China to world trade in the 1990s exposed China's lack of technological progress compared to the West.

China did not have an official cybersecurity policy until 2006 and created an independent branch of government for cyber concerns in 2014 (Lei 2016; Austin, 2014). However, this has not stopped other branches of the Chinese Security Forces from engaging in cyber attacks against states since 2003 (Mandiant Report 2014; Austin, 2014). Over the past decade, Chinese cyber capacity has grown exponentially, and an accurate estimation of their capacity is hard to determine. Currently, China's cyber-attack strategy has been focused on passive attacks, engaging in intelligence operations (Cheng, 2018; Fravel, 2018). This does not discount that Chinese actors have engaged in active cyber attacks. In more recent years, China is slowly breaking out of passive attack strategy and has pursued more active cyber attacks. Its strategy remains primarily reliant on passive attacks. Stealing information for the benefit of the state rather than interfering with a rival state's capacity.

Russia's cyber strategy has changed rapidly over the past ten years, mostly due to the increase in the state's cyber capabilities. Russia feared the embrace of computer technology during the final years of the Soviet Union, due to the loss of social control this technology would introduce (Lunde, 2014. Bolt, 2018). This lack of investment hit Russia hard when it transitioned to a capitalist economy, following the collapse of the Soviet Union. This state-sponsored ignorance caused Russia to fall behind in the cyber realm, with only the military having access to basic computers for logistics (Austin, 2014). Only in 2000, once Vladimir Putin became president, did the government actively engage in expanding the cyber capacity of the state and its citizens (Lunde, 2014; UK National Cyber Security Center, 2018; US Department of Defense, 2018). What makes Russia unique in its cyber strategy is its use of information and propaganda warfare to interfere in critical state infrastructure. Russian attacks include attacks on the Ukrainian, US, and UK elections (Bolt, 2018; Lunde, 2014; Klimburg, 2011). These attacks include hacking and releasing harmful documents or active cyber attacks to the institutions of democracy (voting records/registration)(Bolt, 2018; Whitehouse, 2016). Some of these attacks are difficult to classify. Some could be considered hybrid attacks, especially those which pursue disinformation campaigns. These attacks do not engage by destroying the systems they attack in the traditional method of active cyber attacks, but still cause significant damage to the defending country. They are designed to gain information and weaken the target and focus on internal dissension and polarization rather than challenge Russian influence. However, for this study's purposes, I will focus on their active attack strategy, which remains Russia's dominant cyber strategy.

This study's goal is to identify the determining factors as to why a state favours an active or passive cyber strategy. There is a crucial difference between China and Russia in its cyber strategy. Russia favours active attacks while China maintains a passive based cyber strategy.

Organization of the Research

The first step will be defining my conceptual frameworks through a literature review. Information collection will be through public documents provided by states, NGOs and think tanks, and private security company documents (Mandiant Report, 2014), which will be available in a separate appendix. Currently, there are translated documents from China, Russia, which describe their countries' cyber policy. The trustworthiness of the state documents from Russia and China is often unreliable and will need secondary sources to confirm or disprove the official policy. This study will be structured in four major parts, first beginning with a literature review of the current content on cyber strategies and their relations to Russia and China. The second section will outline the research design and methodology. Third, I will move on to a discussion of the results and analysis. I will finish with a concluding section that will highlight the research findings and possible further research.

I will compare both these states through the four major contributing factors that determine the cyber attack strategy: economic incentives, international hierarchy, committed resources and interpretation of deterrence. For economic incentives, there are three possible indicators, the prevalence of economic targets, the economic policy, and if there is a direct net benefit to the attacking state. International hierarchy has the indicators of state isolation from the international community, reliance on international trade, and ongoing territorial disputes. In the analysis of committed resources, the three indicators are publicly allocated funds, organizational structure, and human capital availability. While committed resources create a problem of endogeny, it will be a factor of analysis since there are indicators outside of strategic policy that determines allocated resources. Finally, to analyze deterrence policy, I will use the indicator of a state's accepted definition of deterrence, perceived conventional and non-conventional threat to the respective state and response, and publicly acknowledged cyber attacks against the respective state. These indicators for comparison will provide an extensive overview of the main motivating factors driving a state to pursue an active versus passive cyber strategy.

This study will expand the limited literature on cyber conflict, and update the preconceived knowledge to reflect better the expanded capabilities of cyber conflict. It will delve into the analysis of the strategy of cyber conflict, rather than debate the conceptual nature of cyber attacks generally. While this study only looks at two states, it will contribute to the ongoing debate in political science about the nature of these newly formed cyber capabilities. By determining the major contributing factor of the formation of cyber strategy, one can apply the conclusions to other states and anticipate a state's offensive actions in the cyber realm.

Literature Review

The significant gap within the literature is that there are few concrete explanations as to what factors determine a state's cyber attack strategies between passive and active attacks. This gap is due to the clandestine nature of cyber capabilities, and there is little policy analysis on state actions regarding overall cyber strategy. The focus of analysis in cyber strategy tends to either be on individual attack case studies (i.e. Stuxnet or Fancybear), or ontological analysis of the concept of “cyber,’”cyberwar,” and attack classification (Rid, 2011; Stone, 2012). Is there a central motivating factor that supersedes all others when determining how a state determines its cyber strategy between primarily active and passive attacks? There is an apparent attempt by countries like Russia and China to present a picture of their cybersecurity policies as purely defensive. Yet, both states do engage in offensive cyber attacks that violate their own declared mandates. The base division between cyber-attack strategies is between active and passive cyber attacks. Russia pursues the former while China relies on the latter. Why do these two states pursue different cyber strategies?

The difficulty within the literature is that most policy analysis provide a biased perspective on non-western states that assume western forms of division, control, and redundancy. Organizations in the US often silo cyber capabilities, and there is a clear delineation between civilian and military organizations. This often results in specific branches of government focusing on passive attacks (i.e. intelligence groups) and active attacks (i.e. military organizations). In Russia and China, the division is far less pronounced. Russia has no clearly defined civilian intelligence services or cyber departments. The closest would be the Federal Security Service (FSB); however, they engage in both internal and external intelligence and military work (Cross, 2018). In China, they have an established Chinese intelligence service and cyber operations. However, they also have been prone to using civilian organizations such as the University of Shanghai to engage in foreign intelligence gathering (Fravel, 2019; Mandiant Report, 2014). This difference in approach creates difficulty when analyzing these institutions from an outside perspective.

Fundamental Debates in Cyber Ontology

There are several concurrent debates and problems which face policy analysts in confronting the new cyber frontier. The literature around cyber attacks and cyber capabilities is currently dealing with a major debate as to what "cyber" consists of and if cyber capabilities open up a new theatre of conflict, similar to the introduction of airpower in the early 20th century. There are scholars like Rid (2012) who argued in his piece that cyber capabilities are merely an enhancement of currently established intelligence capabilities rather than a tool for large scale conflict. He goes through a case by case basis of the major cyber attacks that took place before 2011. In his case by case analysis, he concludes cyber capabilities are most effective when used as an intelligence tool, and have proven relatively ineffective in more convention conflict settings. Rid’s (2012) analysis focuses on the use of cyber attacks that are usually classified as "passive." Valeriano (2015) continues this argument in his book, distinguishing specific passive cyber attacks as "cyber operations" rather than including them in cyber attacks. Valeriano (2015) comes to a similar conclusion that cyber capabilities are most effective when applied to intelligence gathering capabilities.

However, this debate is far from settled. Some notable academics, such as Stone (2013), argue that cyber capabilities introduce a new concept for the battlefield. He argues that the vulnerabilities that states face by integrating themselves into the online infrastructure present significant vulnerabilities. Essential state functions rely on the internet, and through cyber attacks, can be brought to a standstill. These types of cyber attacks are classified primarily as "active" cyber attacks. An example of this is the "Bronze Soldier" attack in Estonia, which crippled the country's internet infrastructure for three days (Lunde, 2014). Stone (2013) argues that these capabilities, combined with conventional warfare, create a new frontier of conflict that directly attacks the homeland, causing a state to lose the ability to conduct a war effectively. McGraw (2012) also argues that the cyber realm has opened a new frontier of possible conflict and argues that the vulnerabilities presented would be a likely target if a large scale state-to-state conflict occurred. McGraw (2012) argues the need for a new priority on securing these online vulnerabilities to prevent such a cyber conflict from ever occurring. While these debates are interesting, they miss significant elements of analysis by arguing about the categorization of "cyber" as a concept and its use, rather than breaking down the motivation of how cyber is used strategically and the factors behind the possible difference in strategy.

Strategy and Cyber Attacks

The first major concept to define is "strategy," explicitly concerning state offensive action. Defining strategy is required since there is a possibility of variation in interpretation based on the specific state. The Chinese National Defence University defines strategy as: "a sovereign states relatively long term, comprehensive plans and guidelines for a … state to use its capabilities to pursue national interests in the international struggle" (Cheng, 2017, p 343.) Monaghan (2013) outlines that Russia defines its strategy, like China, not simply in militaristic terms but "encompasses a more global [connotation], reflecting the attainment of the state's wider aims by whatever means are considered the most expedient" (Monaghan, 2013, p 1224).

Both of these definitions of state strategy overlap, and essentially are congruous with exceptions in diction, not meaning. There is a consensus of using all means necessary to accomplish long-term state goals. How a state uses these capabilities is up to its interpretation, and China and Russia have significantly different state goals outside of the preservation of the state. Russia perceives itself as a bridge between two continents and two cultures (Lunde, 2014; Cross, 2018). Constantly under threat from both sides, with wide expanses of land and peoples to protect and maintain control. However, China sees itself as more secure, considering itself the "middle kingdom," a centre of power and culture, unified against any external aggressor (Fravel, 2018; Cheng 2019). Even with these differences, there is a significant overlap as to how each state interprets strategy.

Cyber attacks are used for general state strategy to accomplish long-term national interests in the international system. These cyber capabilities are still novel in the international community, and states are now pursuing consistent strategies to help their overall national goals. National goals are divided into three primary groups: military, economic and political (Weber, 2018). Cyber attacks can help contribute to a state's ability to achieve all of these potential goals. The fundamental division of cyber attacks is active cyber attacks and passive cyber attacks. Each has its specific advantages and disadvantages, but neither seems to have an overall advantage in helping achieve a state pursue its military, economic or political goals. Therefore, what other factors might explain the difference in how states approach their cyber strategy?

Cyber Attacks: Passive versus Active

Passive cyber attacks attempt to gain access and information with no residual effects on the system, whereas active cyber attacks attempt to change the structure or operations of the recipient network (Uma, 2013; Kramer, 2009). This terminology is from the intelligence community about their forms of operations. Intelligence would have "active" and "passive" operations with similar definitions. Active intelligence operations engage and attempt to sabotage or modify an existing institution, while passive is information gathering. Overall, passive attacks tend to outnumber active attacks by a large margin since the risks of discovery are far less, and inherent costs lower than active cyber attacks. Since both intelligence and the cyber community contain a substantial overlap with this adoption of intelligence taxonomy, active cyber attacks can cripple infrastructure by overloading the networks, stopping the network's ability to communicate with itself, and the surrounding connected networks. A prime example is the Russian attacks on Georgia in 2008, where denial of service attacks crippled the government's websites and communication networks during the Russian sponsored campaign (Carr, 2012; UK Government, 2008). Denial of Service attack is a method of active cyber-attack that intentionally flood the targeted program with information, causing the system to either crash or shut itself down. These attacks hindered the governments ability to communicate with its citizens and defence networks, allowing Russia to invade its disputed territory with a coordinated response. Passive attacks include primarily reconnaissance attacks, traffic analysis and the acquisition of private message content (Uma, 2013). This form of attack is used mainly in coordination with intelligence services to aid in their information gathering. An example of a passive attack would be China's "Operation Aurora," which targeted Google and Adobe, along with several other silicon valley companies, to gain access to protected confidential information (Google, 2010; CSIS 2020). This attack was discovered and still managed to access several email accounts of Chinese human rights activists. These examples of cyber attacks demonstrate each respective state's concept of strategic by using any means available to accomplish their overall goals. With Russia, it is attempting to maintain their state by attacking outside threats to distract them away from Russian interests. However, China is attempting to increase its technological prowess not only to maintain the state but to increase their relative power with rival international states.

The line between passive and active attacks can be slightly blurred. When pursuing a passive cyber attack for information gathering against an institution, the leaking of information can cause similar damage to the institution as a well-placed active cyber attack. The prime example of this situation was the 2016 DNC hack, which resulted in the release of senior democratic figures' private emails during an election campaign (CSIS, 2020; US Treasury, 2018). While this attack did not cause any sabotage to the networks used, it created incredible damage in the institution the network served. This leaking of classified information was technically passive in its characteristics; however, the results of this form of a cyber attack can result in far more damage than a single attack taking down an email server. The broad terminology does allow exceptions and muddled boundaries. Still, it remains the most precise way of classifying cyber attacks without specifying the specific forms of programs required to carry out such an attack. It also remains a clear form of classifying cyber attacks that have not had conclusive investigations on their network failures, which resulted in such an attack. This form of classification is based on the results of the attacks rather than the programming (Uma, 2013). With this blurring of concepts, it still demonstrates that both China and Russia are using tools at their disposal to accomplish state strategies.

Active and Passive cyber attacks are the predominant strategy; there is significant usage of hybrid strategies. Defining these hybrid strategies is difficult due to the scope of the analysis. Are disinformation campaigns a hybrid strategy? It depends on the level of analysis pursued. The technology used to pursue disinformation campaigns is often simple and falls under passive attack strategy since the goal is not to disrupt the program itself. However, the resultant devastation of engaging in disinformation campaigns can cause similar results to an active cyber attack. Disinformation campaigns are not inherently difficult, since actors often use tools already available to the public to target specific groups of vulnerable people. These tools are used similarly to advertisers. Specifically, websites like Facebook and Twitter pride themselves on providing user-friendly advertising and demographic targeting tools which can be exploited by nefarious actors. This form of cyber attack strategy is difficult to classify since nothing systemically was attacked; it is merely tools available to the public being used in ways the creators never intended. There is also a significant difference from some scholars between kinetic and cyber attacks. Both use cyber capabilities to attack another state; however, kinetic cyber attacks cause physical damage outside of the connected systems, while classic cyber attacks damage the cyber system itself. However, for this study, these hybrid and kinetic style strategies will not be discussed.

Problems of Attribution and the Consequences

The problems with attribution, outlined by Finlay and Payne (2017), create a significant challenge for counterintelligence services. The attribution problem does not change significantly between identifying the culprits of active or passive cyber attacks (Berghel, 2017). Determining who carried out an active or passive cyber attack, intelligence services pursue three significant avenues of inquiry. First is faith-based assumption, through inference and historical analysis. Finlay and Payne highlight this in the case of the 2016 DNC hack, where the US government pronounced Russia's culpability. The US Congressional Report provided plenty of circumstantial evidence and assumptions but did not offer any irrefutable evidence favouring their conclusions (Payne, 2017; Berghel, 2017; US Senate, 2017). Finlay and Payne further explain that this is used to maintain political narrative, providing the state with a clear enemy even when the evidence is circumstantial.

Attribution can be done through network analysis, breaking down the source code, and comparison to previous cyber attacks (Payne, 2017). However, cyber attacks are consistently changing, making this form of analysis lacking, only preparing the state for the attack that already happened. Cyber conflict is similar to the adage of war strategy: you're always fighting the previous war rather than the one at hand. There is only one reliable method of determining attribution through human intelligence (HUMINT) gathering (Berghel, 2017). HUMINT is defined by NATO as "a category of intelligence derived from information collected and provided by human sources [instead of technological methods]"(NATO, 2004.) These HUMINT resources creates another issue of attribution for HUMINT resources. The revealing evidence that might prove the attribution of cyber attacks could expose the state's capabilities to gain intelligence on these cyber attacks. In public government announcements on cyber attacks, legitimacy can be unreliable. This possible lack of legitimacy leads back to the faith-based assumptions through inference (Payne, 2017). With this problem of attribution, active and passive cyber attacks become an increasingly attractive tool in pursuing state strategy since the threat of retribution is far lower than any conventional attack.

Problems of Defense

Cyber attacks are nearly continuous and ongoing between states, but there is little retaliation against attacks (Carr 2012, Reveron, 2012; Valeriano, 2015). Both passive and active cyber attacks attack the pre-existing weaknesses already present within the recipient program's code. However, there are cases where external resources are required to carry out active cyber attacks on critical "air-gapped" systems, but these cases are in the minority. Air-gapped systems are computer networks not connected to the internet, creating an "air gap" (Carr, 2012.) For instance, the Iran Stuxnet virus is an example, where an individual needed to connect a flash drive to the air-gapped nuclear centrifuge system to be able to sabotage its capabilities properly (Lindsay, 2013). However, most active and passive cyber attacks are carried out entirely through the internet (Carr, 2012). The main issue in states defending themselves from such cyber attacks is the offensive advantage of cyber weapons. When a cyber-attack happens, the coding of this attack becomes obsolete. The defending vulnerabilities are now exposed, and the recipient of the attack has the code of the attack to analyze (Denning, 2014; Fischerkeller, 2017). This lack of a shelf life incentivizes attackers to change the method attack continuously, looking for new vulnerabilities to exploit. Using the Stuxnet virus again as an example: now that the attack is executed, it becomes useless since now the Iranian state knows how to defend against it and also use it for itself (Carr, 2012). However, it is obsolete since the attacking state would likely have protected itself against such an attack.

Defence against a cyberattack is nearly impossible since the whole function of a cyber attack is to exploit existing vulnerabilities (Costigan, 2016). If an institution knows about the vulnerability that can be exploited, it will usually take steps to mitigate the risk. There is the ability to attempt to defend against an attack in progress; however, it is constrained. Defence capabilities are extremely limited to shutting down the system in its entirety (often impossible), or closing off infected sections of the network (often impractical in a short time-span). Defending is almost impossible to do in real-time against an attack, regardless of it being an active or passive cyber attack. The unknown vulnerabilities are the cause for concern. Defending against a cyber attack would essentially require omniscience or a complete breakdown of a program through every line of code. Because even the most basic programs can contain millions of lines of code, it becomes impractical to sift through all the data to find one tiny mistake that could be overlooked. The work required to create an attacking program is far less than the work required to defend a system against all possible eventualities. This imbalance creates a significant advantage for offensive operations (Shaji, 2019; Valeriano, 2015; Reveron, 2012). Another issue that affects the defence is the pace of technological change. Everytime a computer system updates with a new operating system or downloads a new program it introduces a new vulnerability. Defence also implies that the institution attacked is aware that cyber capabilities are attacking them. Most cyber attacks take three months or longer after the initial breach to be detected (Mandiant Report, 2014). However, there is a difference between active and passive cyber attacks. Active attacks tend to be discovered far sooner due to the drastic consequences of a successful attack. In contrast, the whole goal of a passive cyber attack is to remain undiscovered. This gap between attack and discovery allows plenty of time for the attackers to infiltrate the systems and steal or sabotage. An example of this ignorance of being attacked is in the 2016 Russian hacks of US voter registration rolls, which were only announced in 2018 (U.S. Committee of Homeland Security, 2018.) The one-off nature of cyber attacks does provide a significant disadvantage to using cyber attacks in strategy. In spite of this, the problems of discovery and attribution often negate this issue. Since states are often not even aware cyberweapons attacked them or discover it long after the attack has taken place, cyber attacks have accomplished the goals of the offensive state.

Cyber Attacks and Deterrence

Deterrence has been a key concept in all state action, even before the concept itself was fully developed and analyzed by the academic community. Deterrence is a policy of making their defensive capabilities, or offensive responses to an attack, so devastating that the aggressor state would have all benefits of attacking denied (Gallagher, 2017). Cyber attacks create an environment of offensive advantage since the cost of defending is far higher than attacking. Nuclear deterrence relates closely to cyber deterrence due to the similarities to the offensive advantage. However, where they differ is the significant damage that either attack could inflict. Nuclear devastation and the resultant logic of nuclear deterrence between two armed states create a finality, assuming that any massive attack from either side would destroy both states (George, 1989; Honkova, 2010). This destruction would result in no net benefits to either attacker, thus creating a fairly stable stalemate. An example is the policy of detent carried out by the US and the Soviet Union, nicknamed "MAD," or mutually assured destruction (Honkova, 2010). Cyber attack deterrence also differs from the interpretation of deterrence in regards to space-based missile defence. The equation of deterrence significantly changed by allowing one state to annihilate another without destroying itself. Cyber-weapons do not have the capability of societal destruction; therefore, punishment does not carry the same weight in strategy compared to nuclear strategy.

Lindsay (2015) argues that deterrence by denial works in only the most significant cyber attacks since the problems of attribution are less significant. Deterrence by denial is a strategy of creating significant defences that would make any attack ineffective. It would either mean creating defensive capabilities or making systems able to recover quickly from such attacks in the cyber realm. Attribution is easier to determine the larger the scale of the attacks. Attribution is also easier if the cyber attack is active rather than passive. China can carry out attacks on a larger scale than North Korea due to the gap in capabilities. In contrast, Nye (2016) argues deterrence by denial only works when facing inconsistent small scale attacks from smaller states and non-state actors. When facing significant state opponents such as China and Russia, deterrence by entanglement is the most effective strategy (Ryan, 2018). Deterrence by entanglement is a strategy when both states are so intertwined through other means, either economic or cultural, that any attack would significantly harm themselves and their opponents (Ryan, 2018). This concept is demonstrated by the relationship between the US and China, which are economically linked and cannot take significant harmful action against each other in fear of hurting their domestic economies. Both strategies of deterrence have significant flaws since deterrence by denial only works in large scale attacks, and deterrence by entanglement only works when the two opposing states have tied themselves intrinsically together.

Basic deterrence theory is based on the three key concepts of capability, credibility and communication (Johnson, 2015; Vesna, 2002). There is a breakdown in how capability, credibility and communication functions with cyber deterrence since each concept does not work in regards to cyber attacks. In regards to capability, each state has its resources, which they guard all knowledge. It becomes unclear, like in all intelligence operations, what are the overall capabilities of a state. One can only surmise what the capabilities are through past actions and the estimation of committed resources. Past actions is the best indicator of a state's interpretation of deterrence, but still creates an information gap (Johnson, 2015). This information gap leads to the next issue of credibility. Without a base knowledge of the capabilities of each state, credibility for cyber attacks becomes unclear. Unlike with nuclear deterrence, where credibility is easier to determine, for cyber attacks, there is no realistic way to maintain the credibility of an attack unless it is ongoing (Carr, 2012.) Deterrence policy requires an analysis of credible threats to the state as an indicator. In regards to communication, there is no significant issue since states can communicate their capabilities and threats like all other conventional warfare. However, there can still be a breakdown in communication when a state denies an attack, or a state does not discover that it was attacked (Ryan, 2015). In regards to cyber attacks, states communicating when they face an attack is a key indicator due the authoritarian norm of maintaining silence. Due to these factors, cyber deterrence itself in isolation is practically impossible. Despite these factors, when combined with other more conventional arms and state strategy, it does affect deterrence policy since it does breakdown these key concepts of capability, credibility and communication. It merely adds a new unknown facet as to how a state will apply deterrence in the cyber age.

While cyber capabilities can be included within a state's general deterrence policy, maintaining a policy of complete deterrence against other cyber attacks is nearly impossible. First, this is impossible due to the interconnected nature of cyber-space, making isolating a specific attack impossible (Davis, 2015). Secluding a state from the global internet, maintaining an internal internet system loses many of the internet's inherent benefits. There are some states, most notably China, which can isolate its networks through essential cybersecurity functions. However, they cannot maintain a complete seal from the global internet due to new tools such as VPN's (Virtual private networks), unregistered connections, satellite connection, and other workarounds (Fravel, 2018). China's "Great Firewall" does protect the state, but only for the access of information from outside of the state not harmful attacks designed to mitigate the basic functions of the Great Firewall (Cheng, 2017 p 5). In modern cyber deterrence policy, the best action is retribution through their cyber capabilities, convention military actions, or international legal actions. In the majority of cases, a state will pursue retribution through cyber capabilities. There is a norm of non-conventional response to cyber attacks (Carr, 2012; Reveron, 2012). However, in the face of large devastating attacks on critical infrastructure, many states have an outlined policy of convention attack (US Department of Defense, 2016). The US's defence policy most clearly demonstrates this at the end of the Clinton presidency, which stated a conventional military response would be used in the event of a devastating attack on financial networks, air traffic control networks, or power systems (Clinton Whitehouse, 1999). This policy has never been put into practice and remains theoretical.

The most common form of cyber deterrence is creating retaliatory cyber attacks to distract and deter further cyber attacks. They can either be passive or an active retaliatory cyber attack, though the effectiveness is limited (Davis, 2015; Jensen, 2012). Another major form of deterrence is using legal consequences to the attacking state. These legal actions include state sanctions, legal challenges against individuals from the attacking state to restrict their global movement, or prosecuting individuals in their respective states (Davis, 2015). Legal actions are not an effective form of deterrence due to the continuing onslaught of cyber attacks that a typical state faces daily. It still does create a balance of continuous attacks between states, which distracts a state from carrying out more damaging cyber attacks. It also creates an ongoing tension between states and helps establish a norm of non-conventional response to avoid escalation into the conventional military realm. This new form of deterrence creates a constant base level of cyber attacks that allows states to engage each other in the cyber realm but maintaining a norm of limitation in the scale and damage of cyber attacks. Limitation plays into the generalized policy of defence since there is an assumption of consistent cyber attacks (Carr, 2012; Valeriano, 2015). At the same time, each state attempts to decide how far to push the norms of limitation. Cyber capabilities contribute to the overall deterrence policy since it creates an information gap, where a rival state has little knowledge of the information gathered. There is also the fear of "sleeper" cyber attacks only activated in worst-case scenarios. These attacks are mostly hypothetical, and would only be confirmed in a situation of an all-out conflict between the two states (Carr, 2012). Pure "cyber" deterrence is nearly an impossible concept, but how cyber capabilities play into general state deterrence policy is still relevant in how a state mitigates threats from other rival states.

Economic Incentives for Cyber Attacks

Economics also plays a vital role in determining cyber strategy. If there is enough economic incentive, states pursue cyber attacks to gain an economic advantage (Inkster, 2015; Schofield, 2016). These activities can range from passive based attacks stealing proprietary information from large corporations to engaging in an active attack intended to sabotage an economic competitor. The targets of these active cyber attacks tend to be private corporations rather than state institutions. However, these attacks are still carried out by a state or with state support. There is an issue of distinguishing public and private institutions. In Russia and China, state-sponsored companies have the advantage of government support in their security priorities (Fravel, 2018; Austin, 2014). While government management of private entities has significant disadvantages compared to free-market enterprise, state companies benefit from being central to government legitimacy and access to offensive capabilities. These state corporations give the state an increased incentive to maintain their competitiveness in the global markets through any means necessary (Cheng, 2017). Whether a state attacks primarily private or public institutions is a key indicator of economic motivation behind cyber attacks.

Conflict and economics are tightly linked, with multiple theorists analyzing the bonds between economic interest, war and strategy. Cyber attacks can provide an economic advantage by either stealing information of an adversary or destroying a possible market rival's capabilities. However, offensive conflict and economics are not as applicable to cyber capabilities due to the norm of non-conventional retaliation. When analyzing conflict and economics, there is the base assumption that the state is pursuing a full wartime strategy, and its existence is in jeopardy (Clausewitz, 1956). With cyber. attacks, there is a constant ongoing conflict between states. However, it does not threaten the overall legitimacy or existence of the state itself. Passive cyber attacks are prominent for economic purposes since it focusses on the theft of economically advantageous information. Active cyber attacks are not as common f since it is easier to determine attribution and is far more costly. Brooks' (2013) analysis on economic actors and the prospects of peace state that economic actors are always in favour of maintaining peaceful actions since any conflict between states would damage the global economy. This theory applies to the use of cyber attacks as a tool of conflict since it allows economic actors to maintain the status quo of global peace. Since all cyber attacks still follow the norm of non-conventional response, cyber attacks are useful for economic actors to gain the advantages of attacking rival states while mollifying the possible disadvantages of global conflict and economic disruption. A state can attack another state for economic purposes. However, the fundamentals of global trade are not cut off by conflict, and the recipient state might not even be aware that an attack occurred. This ignorance allows for an offensive strategy of covert economic conflict without risking it spilling into a conventional conflict, which would overall harm the majority of the economic actors.

While the priority is on countries, governments are also at risk for economic-based attacks on their major non-state corporate institutions. These attacks can be hacks to their communication networks, reading emails to gain an advantage in economic negotiations, or leaking the information to sabotage any negotiated deals. An example of this would be the Chinese Night Dragon cyber attacks, which targeted the international petroleum industries (CSIS 2020; Cheng, 2017). The attackers sought to hack the emails of their executives and market intelligence reports and company databases. This attack was a passive based attack discovered in 2008, and no systems were modified - this was an attempt to gain information for a purely economic benefit. There are very few examples of state-directed active cyber attacks against private institutions. Most active attacks against private companies tend to be from non-state actors. One example of state-directed active attacks against a private institution from a state is the North Korean attacks against Sony Pictures, in an attempt to dissuade them from releasing "The Interview," a movie that satirizes the North Korean regime (BBC, 2014). There is significant difficulty in analyzing cyber attacks against private institutions due to the problems of attribution. In the majority of attacks, it can never be certain that it was indeed a state which attacked them. Industrial espionage and cybercriminals attack private companies at a far higher rate than states (Schofield, 2016; Mandiant Report 2014; CSIS 2020). There is an incentive to attack private companies over public institutions due to the resulting responses to security and liability. Private companies rarely have the complete capabilities to engage in continuous cyber campaigns, and in most cases, it would violate the laws of the respective state (Goetz, 2008). A state would not want to give that power its private companies since it would violate a state’s monopoly on the use of violence and enforcement. The liability also becomes an issue since when a private company is attacked, it is liable for the stolen information (Inkster, 2015). The company is at fault since they could not anticipate the impossible, and the attribution problem makes it almost impossible to prosecute the attackers. It also becomes even murkier when discussing state companies, since determining if a state-directed its own state-run company to engage in industrial espionage for the benefit of the state, or the company pursuing its policy to gain an economic advantage.

A states economic policy is another key indicator in economic incentives to potential attackers. If a state is highly focused on sectors of the economy vulnerable to cyber attacks, then they immediately become a more valuable target merely due to the abundance of targets compared to other states (Carr, 2012; Reveron, 2011). These vulnerable sectors are high-technology development, internet marketplaces, and online databases. If a state is also trying to compete in similar markets, there is a high incentive for them to steal information to gain an economic advantage. Due to the issues with attribution, and the ability to detect certain cyber attacks, engaging in cyber theft through passive attacks can be very appealing. The advantages of economic cyber attacks leads to the next indicator, direct net economic benefit from cyber attacks. There are incredible upsides to attacking more technologically superior states, without many downsides since their guilt can never be completely proven.

However, these attackers can face retaliatory cyber attacks to either mitigate the information that was stolen or hinder the attackers' ability to carry out further cyber campaigns. There are multiple cases where a state has engaged in economically beneficial cyber attacks against other states, mostly in the theft of proprietary information (Jackson, 2014). Lindsay (2013) distinguishes that gathering information and converting it into economically advantageous information is significantly different. China, Russia, Iran, North Korea and Ukraine have all engaged in cyber attacks for economic benefits rather than merely state security, but do they have the ability to use it. It is similar to Soviet espionage regarding nuclear weapons. Stalin's spies managed to steal the information on how to construct a nuclear weapon but still lacked the engineering capabilities to act on the information (Schwartz, 1996). While this is a significant problem for both China and Russia, it does not dissuade them from attacking rival companies. Companies in the US are losing up to 4 billion dollars a year to cyber attacks carried out by both states and third-party actors (Jackson, 2014). These attacks both disrupt the economic functions of a company and decrease the confidence of possible investors into the private entity.

The Motivation of Cyber Attacks based on Relative State Power

International relative power also plays a role in how the state determines its cyber strategy. Countries that perceive themselves to be under more significant threats tend to pursue a more aggressive cyber policy since cyber attacks are an efficient way fight asymmetrically (Carr, 2012; Saltzman, 2013). State isolation is a key indicator of international relative power, since an isolated state does not have the same abundance of resources. When facing an asymmetrical conflict, it becomes far more valuable to engage in cyber campaigns than risk using conventional military action (Breen, 2011). Smaller states can have significant cyber impact compared to their conventional military power. Using North Korea is a prime example; it is a fragile state with a military slowly rusting away with outdated weaponry and training. In cyberspace, a minimal investment can produce substantial results. North Korea's list of cyber attacks dwarfs even major western states like Germany or the UK (CSIS, 2020). The problem of attribution also benefits states facing more asymmetrical conflict since they can attack without much threat of retribution from a powerful offended state. The size of the state also benefits in securitizing its cyberspace when facing retaliation. A smaller state means a smaller network, resulting in fewer vulnerabilities and access points (Saltzman, 2013). Cyber attacks are becoming the tool of choice for countries with fewer resources. While passive cyber attacks are advantageous due to the small amount of resources required, active cyber attacks are useful tools for asymmetric conflict. Passive cyber attacks allow small states to target larger opponents without the threat of conventional retribution. Ebert and Maurer (2013) argue that cyber-space is one of the only areas where rising powers such as the infamous BRICS (Brazil, Russia, India, China, and South Africa) states can effectively challenge US hegemony. In their negotiations with the US concerning international law and security treaties. China and Russia advocate for more closed systems to protect themselves from cyber threats and information that could weaken their domestic political control.

In international relations, there is the conventional concept that a "revisionist power" would be more apt to violate international norms or rules to increase their power at the expense of their dominant adversaries. This concept is argued by Mearsheimer (2014), who claims that China is a revisionist power, and that conflict between status quo powers and revisionist powers is inevitable. A revisionist power would have the incentive to pursue a strategy that reshapes the international system and hasten the decline of the status quo power. In this case, these revisionist powers would be more likely to use active attacks to weaken the international system's hegemon. This theory is not airtight since China actively avoids international conflict, and maintains a net benefit in the current international system. Jones and Hart (2011) answer this problem by stating that rising powers are happy to allow the current reigning hegemon to maintain the costs and burdens of international leadership. In contrast, revisionist powers maintain focus on their growth and domestic politics. In this case, revisionist states would use passive cyber attacks to gain information and focus on internal growth. As the leading power, the US does not have the same ability to pick conflicts to involve itself, both military and non-military. They must engage all across the world to maintain their international order while a rising, or resurgent power like China and Russia can take a back-seat to global leadership while maintaining the benefits of the international system (Ebert, 2013). By pursuing a strategy of selective engagement rising powers prefer to maintain dominance within their regional spheres to maintain security without extending themselves past their capabilities. In this system, they can also challenge US leadership in specific areas, with more focus, and without the distractions of international leadership. Russia is a clear case with its policy focused on maintaining its security in its regional sphere, confronting any encroachment by western powers (Lunde, 2014). This idea can be challenged, since China has recently taken on more responsibility for the international order, and is trying to reshape a global economic system for its benefit. The "Belt and Road" initiative helping connect China securely to global markets in the Global South is a clear example (Fravel, 2018). This economic integration within the global economic is another indicator of international relative power. With this increase in leadership, China is quickly becoming a second global hegemon.

With these possible explanations to a state's actions within the international order, it clarifies how this affects cyber strategies. With the problems of attribution and detection, cyber operations allow rising or resurgent powers to challenge the global hegemon without significant risk to themselves, in specific conflicts of their choosing. One significant indicator of challenges to the international order is that of territorial disputes. When a state claims another's territory, there is a problem in the international system to the claimant state. With these claims, the stagnation of these claims' resolution means that a state will have to act outside of the traditional international order to regain territory (Ebert, 2013). Acting outside of international norms can be achieved through multiple policy areas. However, the one with the least outward consequences to the claimant state is the use of their cyber capabilities. Active cyber attacks would signal that a state is pursuing strategies that break international norms, while passive cyber attacks would be in line with maintaining the international norms. This difference in strategy is demonstrated with the information campaigns China pursues in Taiwan to increase the popularity of reunification and Russia's attacks on Georgian and Ukrainian infrastructure during the 2008 and 2014 conflicts (Renz, 2016).

Institutional Organization and Cyber Strategy

Another key factor highlighted by scholars is how the respective state organizes institutions that carry out their cyber-security policies. When determining cyber-attack strategies, these attacks are carried out by a state's cyber-security institutions. Most governments create specific departments to manage the cyber-security of their respective states. However, specific indicators of institutional organization provide a more in-depth analysis of how these resources are used and the potential pools of resources. An indicator of institutional organization is how funds are allocated to individual departments. States which spend lavishly on specific cyber capabilities would be more likely to pursue more costly active cyber attacks. In contrast, a state which spends less on specific cyber capabilities could only carry out low-resource passive attacks. States have the incentive to misrepresent their capabilities by either over or under-reporting their spent resources to either convince their rivals that they are either not a legitimate threat or that they are too threatening to challenge directly. Determining if a state is over or under-representing their figures is incredibly difficult without a specific analysis of the dependent military-industrial complex. Even then, these figures remain tightly held secrets. To Chen (2009) and Oxenstierna (2016), it is the standard norm for larger states to under-represent their allocated defensive spending to convince the hegemon that they are not as threatening to their interests.

This norm of under-reporting is consistent, and both China and Russia under-report their military spending to hide their true capabilities in the face of possible conflict. These figures can also be represented through public spending in other possible policy areas, with domestic security spending contributing to external defence capabilities. Often this type of spending does double duty in both increasing internal and external security. China spends lavishly on its internal monitoring capabilities that can also be used for international monitoring and cyber attacks. This norm is especially present in authoritarian governments since defensive spending has the double capabilities of maintaining domestic and international control of their respective interests (Chen, 2009).

The structure and division of these institutions regarding cyber capabilities is essential. Without the same delineation as western governments, the institutions of cyber capabilities in other states can be far more muddled or folded into other institutions with their specific priorities. Authoritarian states can often use defensive capabilities to maintain domestic as well as international security. Russia is a clear demonstration of this concept with its use of the FSB, the successor organization to the KGB (Lunde, 2014). These institutions also do not have the same limitations as their western counterparts, which have mandates and legal restraints to maintain individual freedoms and freedom of information. If a state has a specific department dedicated to its own goals and mandate, their use of the allocated resources is far more efficient. It guarantees the funds are directed to specific cyber-security goals. Having specific delineation between departments would allow for states to organize and carry out more sophisticated active cyber attacks. While in the case of a more muddled administrative organization, the priority of cyber strategy can be overruled by other state priorities, allowing neglect and fewer resources directed to cyber specific capabilities. This situation would encourage the primary use of less resource-intensive passive cyber attacks. There is also the issue of non-state actors acting on behalf of the state, being paid through unrecorded back-channels. These "grey" hat hackers often act in concert with the state's specific goals, sometimes directed by the state or acting on their initiative. Klimburg (2011) argues that these cyber "grey hats" function similarly to the former paramilitary units of communist regimes, which have their autonomy but still need some form of control exercised in the case of disagreement with the state. A state directs cyber attacks without identifying themselves to the hacking unit, which operates independently for their own ideological or financial reasons. Their interests might align with the state, but they do not hold any loyalty to the state's goal. These "grey hats" are only loyal to their specific interests.

Lunde (2014) argues that the lack of human capital creates a significant problem for the institutional organization for cyber conflict. Without a large pool of trained individuals in such an advanced skills-set or providing programs to increase the state's ability to create human capital, the institutions will struggle to increase their cyber capacity. Fravel (2018) contributes to the importance of human capital by emphasizing China's ability to create specific educational programs to train individuals in the skillset required to pursue cyber capabilities. In respect to the United States, they maintain the best educational system in the world with specific programs created to funnel capable individuals directly into state institutions involved in cyber conflict. This human capital also extends into the non-state cyber actors, with access being a key component.

Having access to a ready supply of well-trained human capital will allow a state to engage in more complex active cyber attacks. In contrast, a lack of human capital will limit a state to less sophisticated passive cyber attacks. Klimburg (2011) argues that if a state has access to these non-state cyber actors, they can achieve similar goals to maintain their large base of human capital, but they are not nearly as reliable. These third-party actors can mitigate the lack of training and help states with low human capital carry out sophisticated, active cyber attacks. Having access to domestic human capital with the training to aid in a state's cyber strategy can be carried out far more effectively and with peace of mind. Many smaller states use the human capital of other nations to boost their cyber capabilities, such as Brazil and Turkey (Ebert, 2013). This inclusion of foreign actors into their clandestine cyber operations creates significant risk since they can report back to their own home countries. However, this risk is seen as necessary to develop their nascent programs to expand the base of their human capital by allowing their foreign actors to train their state in the same skillset.

This literature review outlines that there are several key factors in determining how cyber strategy is determined. It highlights several possible indicators to test if they are, in fact, significant influences on strategy. However, due to the clandestine nature of cyber operations, other possible factors remain unclear due to the lack of documentation. While several key academics provide an exceptional understanding of the factors around cyber capabilities and have access to classified material, they are still subjected to their personal bias and the bias of the institutions. It cannot be clear if these academics are receiving all the possible facts and data to create an informed decision, or have limited access to sources that merely confirm their suspicions and allow the analyzed state to present an advantageous perspective. A new possible explanation of how a state determines a cyber strategy can be unearthed by providing an analysis of these factors from a fresh perspective on the policy analysis front.

Methodology:

Research Question

The world of cyber capabilities is muddled with multiple conflicting accounts of strengths, weaknesses and active campaigns. In this paper the question, "Is there a specific factor which encourages Russia to pursue active cyber attacks and China to pursue passive cyber attacks ?” will be answered using document and policy analysis. A case study analysis of Russia and China will be done to see if there is a persuasive answer. While policy analysis has its weaknesses, this study will provide an accurate picture of these two country's cyber capabilities. This analysis will only include publicly available information due to the limitation of classified information. Using multiple sources from private institutions, government documents from both NATO member states, and Russia and China, respectively, an accurate picture is developed and can be pursued further when access to more guarded information becomes available.

Policy Sources

The documents used as evidence for this paper come from multiple sources, government and private institutions, from NGOs, secondary sources, and personal accounts of key actors within the cyber-security and conventional security realm. The first set of documents is from NGOs and the private institutions, which catalogue all known cyber attacks against NATO members and the suspected perpetrators and the specific institutions attacked in the private and public sectors. The second set of documents pursued are from western NATO governments, providing public records detailing their cyber capabilities and their perceived and realized threats. The third set of documents are government documents provided by Russia and China, some translated by their respective governments, and others translated by other academics or western governments. Also included is an analysis of secondary documents provided by established experts in cyber-security and specialists on Russia and China. Finally, the last set of analyzed reports are first-hand accounts and the established doctrines from several key members of China and Russia's security policy before and after the advent of cyber strategy as a significant factor in state security. The main advantage of using document analysis is the availability of information provided and the ease of access to public documents. In pursuing research into such a clandestine activity, few other methods can be used when not having full access to classified data concerning a state's cyber activity. Comparing multiple documents from both the attacking, defending and observing actors will create an accurate picture of the motivations.

Problems and Mitigation

There are distinct disadvantages to policy analysis that must be addressed and mitigated—the first being access to classified documents. Many documents which could provide more precise detail in this analysis are classified. While this study does not have access to these documents, the use of multiple public documents can mitigate this issue regarding the most recent attacks and capabilities. Maintaining state secrecy about these capabilities often does not remain secret for long, and NGOs and other private institutions provide enough analysis to infer conclusions that remain state secrets. Another issue is biased selectivity, where the selection of the documents is subject to personal bias. This bias is mitigated by using multiple sources to provide legitimacy to the provided evidence. Another method of reducing selective bias will be using sources attempting to disprove the initial conclusions of the research in a thorough attempt to maintain a rigorous analysis. Finally, the last major issue of this study is dealing with government documents from Russia and China that might not provide an accurate depiction of their capabilities. Since both states are authoritarian and do not guarantee freedom of information, the public-facing information can often be misleading or inaccurate. These documents are prone to either over-exaggeration or complete denial of offensive attacks, even in response to recorded attacks by the defending institutions. This inaccuracy can be mitigated by pairing them with sources from NGOs and other government institutions to ensure accuracy.

First Factor: Economic Incentives

When analyzing economic incentive, many potential indicators can explain whether these attacks are carried out for primary economic rather than a political benefit. The first significant indicator chosen is that of the directly attacked institutions, are they primarily private businesses, or are they attacking specific government institutions? If it is primarily businesses, what type of businesses are they attacking and what information was stolen or destroyed. Which government institutions are attacked? Are the attacks focused on the state's defensive capabilities, or are they focused on their domestic economic institutions? Initial conclusions state that if the cyber attack targets are primarily commercial, a state will use passive cyber attacks as their dominant strategy (Cashell, 2004; Goetz, 2008). However, some active cyber attacks on defensive capabilities can be for economic benefits. In contrast, attacks on domestic economic institutions can be motivated to disrupt the state's functions. Analyzing the context of these attacks and information from both NGOs and government documents will clarify motivating factors.

Another possible indicator of the economic incentive behind the attacks is the economic focus of the attacking states. Are the states primarily focused on developing their technology-based economy, or are they focused on resource extraction? Is the state itself attempting to diversify its economy beyond its current focuses for a competitive advantage? If a state is attempting to expand its technology focused economy, passive cyber attacks are favoured over active attacks. If a state's economy is focused on resource extraction, they would have less incentive to use passive cyber attacks to gain economically advantageous information. They are also more encouraged to pursue active cyber attacks since their economy is not as vulnerable to cyber attacks when facing possible retaliation.

Finally, the last indicator is if the likelihood of cyber attacks provides a direct economic net benefit to the attacking state. This link can be either intellectual patents being stolen and put on the market early, or the theft of personal private data. Passive attacks are more likely to provide economic benefit to the attacking state, while active attacks are more likely to cause economic harm to the attacking state. Passive attacks are less likely to be discovered and cause international consequences and the reverse when engaging in active cyber attacks. China and Russia have a blurry separation between state and private enterprise, due to their reliance on large state-run businesses such as Gazprom (Russia) and Sinopec (China) (Lunde, 2014; Fravel 2018). Therefore state cyber attacks can benefit specific companies rather than the state as a whole. By analyzing if there is a net benefit after cyber attacks, the motivation behind them can help determine the cyber strategy pursued. Table one (below) helps explain how the indicators would theoretically determine the effect economic factors have on the difference between active and passive cyber strategy.

Table 1. Theoretical Application of Economic Factors on Cyber Strategy

Theoretical Application of Economic Factors on Cyber Strategy	**Passive Cyber Attack**	**Active Cyber Attack**
Institutions attacked?		
Private	**X**	
Public		**X**
Economic Focus?		
High Technology	**X**	
Resource Extraction		**X**
Direct Net Benefit?		
Yes	**X**	
No		**X**

Second Factor: Relative International Power

Relative international power provides another possible explanation for the difference in cyber strategy. One of the indicators for the international position is the isolation of the attacking state by the international community, either through sanctions or public denouncements. A state's isolation from the international community will encourage it to pursue strategies that are more disruptive to the international community since they hold little share in the benefits of these institutions (Mearsheimer, 2014). Being isolated also encourages the state to become a more revisionist power, looking to change the rules of international conflict to better their goals rather than maintain the liberal rules-based order established after WW2. This isolation would imply that the state would be more agreeable with using active cyber attacks in regards to state strategy. An isolated state would be more likely to pursue active cyber attacks over passive cyber attacks since the international community could not punish the offending state effectively.

Another indicator concerning the attacking state's international position is the reliance on international trade. If the state relies on international trade with other states, the appearance of being low risk to information theft or sabotage is key to maintaining these economic benefits. If a state appears to be a more risky endeavour for investment, there is a higher likelihood that a state will pursue an active cyber attack since it would not lose much economic benefit (Goetz, 2008). If a state is heavily reliant on international investment, it will pursue passive cyber attacks since the risk of discovery and attribution is far less. These actions tie back to the definitions of strategy in using any tools to achieve state goals. If state goals are heavily reliant on trade, they will not pursue a strategy that puts that aspect of their economy in danger.

The last indicator is the response to ongoing territorial disputes with neighbouring states. A territorial dispute is one of the most explicit indications that the respective state is not fully accepting of the international order and is possibly willing to break certain norms to achieve their territorial goals. However, there is a difference in analysis when looking at territorial disputes, including conventional military action, and those without conventional military action. The differences demonstrate which state is adhering best to the international regime since conventional warfare to gain territory is illegal under international law (UN, 1945). By analyzing their past actions in pursuing state goals of expansion, we can interpret which state would use a more aggressive strategy to pursue these territorial disputes. If a state is actively breaking international norms to solve territorial disputes, they are more likely to pursue active cyber attacks. They are already breaking international norms such as using conventional force; therefore, the international community's ability to punish them is reduced. If a state is not breaking international norms, they are more likely to use passive attacks, since it does not overtly violate the International norms they are upholding. Table two (below) illustrates what the theoretical explanation would say in determining the difference in pursues active or passive cyber attacks.

Table 2. Theory of International Power and its Impacts on Cyber Strategy

Theory of International Power and its Impacts on Cyber Strategy	**Active Cyber Attack**	**Passive Cyber Attack**
Is the state isolated?		
Yes	**X**	
No		**X**

Theory of International Power and its Impacts on Cyber Strategy	Active Cyber Attack	Passive Cyber Attack
Is the state reliant on international trade?		
Yes		X
No	X	
How does the state respond to territorial disputes?		
Breaking norms	X	
Maintaining norms		X

Third Factor: Institutional Organization

Another possible factor in explaining the differences in using passive versus active cyber attacks is how officially committed resources are used and divided between the cyber organizations of the respective state. The amount of resources a state has, influences the strategies they use to pursue state goals, and also shows the priorities of the respective state. This analysis does create a problem of endogeny; however, the availability of funds has a significant influence on cyber capabilities potential strategies. One indicator is the publicly presented budget of cyber-security presented by each state and where it is allocated. While the budgets are not always accurate, they will also be compared with NGO and NATO estimates. While it becomes speculative determining which is the most accurate number, it does provide a window of allocated costs that will be compared between states. This analysis will include military spending and civilian spending on cyber-security to provide a more accurate picture of the allocated resources. The underlying assumption is that a state with less committed resources would not be able to carry out large-scale cyber attacks, especially active cyber attacks, which in theory is more resource intensive.

The next indicator for institutional organization will be the governmental structure determined to manage their cybersecurity capabilities. Is their cybersecurity division a singular entity? Alternatively, is it merged with other government functions such as intelligence or military? When these cyber-security teams are merged under other institutions, they tend not to have as many resources or a direct mandate for their operations. The division of tasks also determines if there are any specific restrictions or mandates placed on these institutions. The division of tasks shows how a state prioritizes its resources and where the emphasis is placed upon pursuing state strategy. This analysis becomes complicated with Russia and China's specific cases since the division between civilian and military institutions can often be blurred, as well as the separation between private entities and government (Lunde, 2014; Fravel 2018). With a more defined separation of government entities, a state would have a higher capacity to carry out cyber attacks due to the direct focus of government priorities on using these tools in the overall state strategy. If a state has separation between their government entities, the theory is that they would be more capable of carrying out active cyber attacks. A state with less organizational distinction would only have the capabilities to carry out less intensive passive cyber attacks.

The last indicator analyzed for institutional focus is the availability of human capital to carry out cyber attacks. To determine human capital requires an analysis of their technology sector, and the specific use of government resources to carry out cyber attacks. In certain specific attacks, third parties are contracted out to carry out cyber attacks on behalf of the state (Carr, 2012; Lunde, 2014). Sometimes these attacks are carried out by these third-party actors (grey hats) without even having confirmation that they are acting on behalf of a specific state (Klimburg, 2011). It will also require an analysis of educational programs and the availability of access to these programs to train individuals in the skill set required to carry out such attacks. Training individuals to engage in such attacks required a significant investment on behalf of the state to gain enough human capital to enact large scale cyber attacks (Valeriano, 2015). The initial thoughts on how human capital affects cyber capabilities are that with a smaller number of trained individuals, a state cannot carry out large active cyber attacks. State strategy requires a state to use the resources and tools it has and must plan around the limitations presented. In theory, a state with less access to human capital would be limited to carrying out passive cyber attacks. However, there is a counter-intuitive argument that could incentivize states to use third party actors, which are much more likely to carry out more disruptive active attacks in their strategy (Valeriano, 2015). Table 3 explains how the theory would expect a state to pursue cyber strategy in relation to institutional focus.

Table 3. Theory of Institutional Organization and the Impacts on Cyber Strategy

Theory of Institutional Organization and the Impacts on Cyber Strategy	Active Cyber Attack	Passive Cyber Attack
Allocated Budget?		
High Investment	**X**	
Low Investment		**X**
Institutional Separation		

Theory of Institutional Organization and the Impacts on Cyber Strategy	**Active Cyber Attack**	**Passive Cyber Attack**
Specific institutions for cyber security	**X**	
Merged into other government institutions		**X**
Availability of Human Capital		
High Availability	**X**	
Low Availability		**X**

Fourth Factor: Interpretation of Deterrence

The last factor in determining whether a state primarily carries out an active or passive cyber attack is the state's application to and concept of deterrence policy. Cyber deterrence in isolation is an impossible task; however, cyber capabilities still affect how a state pursues a general deterrence policy. Cyber capabilities add new challenges to the underlying deterrence factors of capability, credibility and communication (Fischkeller, 2017; Libicki, 2009; Johnson, 2015; Danilovic, 2002). A state engages in cyber deterrence by providing a continuous low level of cyber attacks to distract the defending state by occupying it while demonstrating the attacking state's capabilities working in concert with a state's conventional forms of deterrence. The first indicator of deterrence is how the state has historically applied deterrence concepts to previous problems of state security. If the state has historically pursued deterrence by using information as its advantage, they would be more likely to pursue passive cyber attacks. If a state uses deterrence through overwhelming force, it is more likely to pursue active cyber attacks. Historical deterrence is defined by the state's previous policies when confronting a security problem. Historical deterrence policy requires a detailed analysis of previous military and intelligence commanders and their previous interpretations.

The next indicator of the state's deterrence policy is the credibility of the perceived threat posed to the state. Each state has a unique hierarchy of threats to the existence of the regime and enacts a policy of deterrence as apart of state strategy to mitigate the risks. Both China and Russia require an analysis of the specific deterrence policies and how their cyber strategies are included within their defensive posture. There is also an analysis of specific threats within the cyber realm and how it differs from conventional military threat and how these two threats act in unison. If a state perceived a high level of a credible threat, it would more likely engage in active cyber attacks. If a state perceives a low level of credible threats, it would be more likely to invest in passive cyber attacks. This analysis will look through these states current perceived credible threats and determine if there is a significant different in posture between states.

Finally, the last indicator of differing concepts of deterrence affecting the primary method of cyber attacks is communication, represented by how many cyber attacks the state acknowledged. In authoritarian states, acknowledging cyber attacks is a risky endeavour since it can undercut the public perception of citizens to the effectiveness of the state's security. Since authoritarian regimes primarily rely on the concept of protecting their citizens, and acknowledgement of failure undercuts a primary reason why the state does not allow typical individual freedoms protected in most democracies. Suppose the state admits it receives cyber attacks and accuses a state. In that case, it shows a break in the norms of communication found in most authoritarian regimes and demonstrates that the regime perceives itself secure enough to admit weakness. These occasions are incredibly rare, but they also provide a window into the defensive nature of their cyber-security apparatus, and how much their adversaries are attacking them. Finding a record of cyber attacks by western states on Russia and China is incredibly difficult, with such information being highly protected. If a state admits to receiving attacks by the US, it can be assumed that these accusations are legitimate since the usual norm is to conceal and publicly ignore. If an authoritarian state admits they face cyber attacks, they are more likely to pursue passive cyber attacks as a response. The state perceives itself to be secure and does not need to pursue destructive active cyber attacks to deter rival states. If a state does not admit they receive cyber attacks, they are more likely to use active cyber attacks. The threat to the state is significant and it must use active cyber attacks as a deterrence to stop rival states from exploiting possible weakness. Table 4 helps explain how each state should choose between active and passive cyber attacks concerning its interpretation of deterrence. If deterrence is the significant factor in determining cyber strategy, the following indicators will relate in this way between active and passive cyber attacks.

Table 4. Theory of Deterrence Interpretation and the Impacts on Cyber Strategy

Theory of Deterrence Interpretation and the Impacts on Cyber Strategy	Passive Cyber Attacks	Active Cyber Attacks
Historical Deterrence interpretation is based on?		

Theory of Deterrence Interpretation and the Impacts on Cyber Strategy	Passive Cyber Attacks	Active Cyber Attacks
Information Superiority	X	
Military Threat		X
Perceived Threat Level?		
Low	X	
High		X
Does the state Acknowledge Attacks?		
Yes	X	
No		X

This methodology will provide an accurate picture of the significant factors influencing the prevalence of a specific cyber-attack strategy. These four factors: economic incentive, international position, institutional organization and interpretation of deterrence are the factors which will be used as a basis for analysis in this study.

Discussion and Results:

The findings of this policy analysis have unearthed several compelling explanations for why states might pursue active or passive cyber attacks. However, the most compelling arguments that determine if a state primarily pursues active or passive cyber attacks are its historical application and interpretation of deterrence policy. Each state interprets the concept differently according to its political structure, history and the prominent policy leaders in each state. This research does not discount the possibility that economic factors, international hierarchy, or institutional organization are contributing factors. However, historical deterrence interpretation primarily explains how a state enacts its cyber strategy. To explain how these four factors affect the policy outcomes, I will explore each contributing factor and the preliminary conclusions I have reached on the effects these factors have on each state's cybersecurity policy. These partial explanations also contribute to the understanding of the policy decisions. Deterrence, however, is the only one that adequately explains both why Russia pursues active attacks, while China favours passive attacks.

Economic Incentives

The first factor, economic incentives, initially is one of the primary drivers explaining why a state would pursue passive cyber attacks against other states. There is a clear cut benefit for engaging in passive attacks due to its ability to go unnoticed and, at the same time, stealing information that can provide a market advantage to the attacking state. If Russia and China follow the theoretical model outlined in Table 1, the conclusion is that economic factors are the primary driver behind determining cyber-attack strategy.

Institutions Attacked

China's cyber-attack targets have been relatively equal between private and public institutions, but they often combine attacks in tandem. In an analysis of Centre for Strategic and International Studies' (CSIS) significant cyber attacks between 2006-2020, there is an even distribution between attacks on private institutions and public institutions, often in tandem (CSIS, 2020). The US-China Economic and Security Review Commission states that:

"*The Chinese government is directing and executing a large-scale cyber espionage campaign against the United States and to date has successfully targeted the networks of U.S. government and private organizations, including those of DoD and private firms.*" *(US China Economic and Security Commission, p259, 2013)*

There are attacks on the pharmaceutical industry and the U.S. health department in 2020 and attacks on Mitsubishi engineering and the U.S. defence department to gain proprietary information on military contracts and patents (CSIS, 2020). These are primarily passive attacks and do not affect the systems in which the information is stolen. These attacks are advantageous since it often takes months to years to discover, and a culprit identified (Valeriano, 2017). In many cases outlined in CSIS' data set of significant cyber incidents since 2006, many attacks are inferred from China but with no irrefutable proof. However, due to their strategic attacks on both public and private institutions simultaneously in similar fields, the conclusion is that China is the only state with the resources and motivation to carry out such large-scale attacks.

Russia, on the other hand, carries out a different style of attack. The majority of Russian attacks are carried out against public institutions, referring to the list of significant cyber incidents provided by CSIS(2020). These attacks are both passive and active. Their passive attacks are for information gathering, but the focus is more on the governing representative institutions than the regulatory agencies or related departments. (Austin, 2014; Fravel, 2018; CSIS, 2020). Their attacks are also multi-staged attacks using passive cyber attacks to gain the information, then use the gathered information for active cyber attacks and information warfare, by distributing propaganda and undermining governing institutions (Lunde, 2014). An example of this is highlighted by the U.S. Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies of the Committee on Homeland Security:

"In 2009, … cyber-spies from Russia … had penetrated the U.S. electrical grid, leaving behind software programs. The intruders did not cause damage to U.S. infrastructure, but sought to navigate the systems and their controls". (USHS, 2013)

When Russia attacks private institutions, they tend to be institutions that are critical for state functions such as power grids or internet access (CSIS, 2020). In 2008, during the Brown Soldier protests, Russia attacked Estonia, engaged in Denial of Service attacks, which caused internet access to and from Estonia to be severely restricted (Lunde, 2014). In 2014, coordinating in hybrid conflict, Russia attacked several power stations in Ukraine and managed to sabotage the electric grid severely hampering the state's ability to coordinate against incoming Russia sponsored conventional military attacks (Kshetri, 2017; ICS, 2016). These attacks demonstrate that while they engage in passive cyber attacks, Russia favours active attacks far more prominently than other comparable states.

Economic Focus of China and Russia

The next indicator of economic incentives is the primary economic focus of each of the respective states. Overall, China is aggressively pursuing a technology-focused economy to gradually transfer away from its manufacturing-based economy pursued for the past 30 years (Austin, 2014; Fravel, 2017). The seeds of this high-tech focus on the economy go back to the opening of China under Deng Xiaoping and the establishment of special economic zones (Austin, 2014). These zones allowed for international investment and private businesses without the traditional restriction of a command economy. The first being the Shenzen high-tech economic zone, with a particular focus on attracting outside economic investment to boost their nascent technology sector (Austin, 2014). In 2006, China enacted its "National Strategy for Informationization Development 2006-2020," which focused on:

- *promoting the information technology sector,*
- *increase the accessibility of computers and computer networks,*
- *expand digital network technologies*

- *and expanding their national information infrastructure (Fravel, p202, 2017).*

These key policy goals demonstrate that China's economic focus is the technological innovation of its domestic economy. This focus is partially due to their attempt to transition away from their manufacturing focus, which is becoming less competitive in the international market due to increased labour costs compared to other developing nations (Fravel, 2017; Cheng 2018). In enacting new policy goals, China's cyber attacks strategy works in tandem to increase competitiveness in the international market. Attacking key industry leaders such as Google in 2010 and 2011 under the name "operation Aurora" and against South Korean, Japanese and Taiwanese technology companies in 2011 labelled "Icefog" (CSIS, 2020; Cheng, 2018). These are only a few of the recorded and discovered attacks carried out by China. However, there are possibly far more operations that have not been detected due to the difficulty in identifying passive based cyber attacks.

Russia has a similar attempt at pursuing a competitive high tech sector following China's model (Lunde, 2014). Primarily their economy is based on natural resource extraction and export (Worldbank, 2019). During the Soviet era, the government distrusted new computer technology in fear that it would help precipitate the loss of political control the party maintained (Lunde, 2014). After the collapse of the Soviet Union, the incentives to maintain a lucrative resource extraction economy remained with a heavy focus on oil and gas production and mineral extraction. This focus away from high-technology towards resource extraction did not provide the same incentive structure for Russia to engage in attacks on private institutions since their benefits for technological gain are not as prevalent in the resource extraction sector. Russia has been inching towards export diversification; however, it has been slow without much progress (Worldbank, 2019; Kremlin, 2019). Russia is attempting to create high technology centres in the model of China's Special Economic Zones (SEZ). The Government of Russia states in an investment presentation on SEZ's that:

"A number of established Special Economic Zones in Russia has considerably increased since the Federal Law No. 116-FZ of July 22, 2005 "On the Special Economic Zones in the Russian Federation" passed. The law was aimed at attracting both foreign and national investment to boost economic development in manufacturing industries and infrastructure." (Government of Russia, 2017)

They have fallen short of their initial goals and have not been pursued as doggedly as its resource extraction policy (Hanson, 2019). They are also facing an increasingly volatile commodity market and a shift away from fossil fuels, which provides them less of a budget to help invest in these nascent industries and encourages attempts to diversify the economy (Hanson, 2019; Worldbank, 2019). This lack of a high tech industry creates a shortcoming in state function to carry out multiple long term cyber campaigns, requiring reliance on third-party actors (Austin, 2014; Liblicki, 2009). These third-party actors are less likely to engage cyber attacks for economic purposes since passive economic attacks require a level of knowledge to determine the most advantageous information.

Direct Economic Benefit

The final indicator of economic factors is determining if there was a direct economic benefit for the attacking state when engaging in cyber attacks. In China's case, there is a clear net economic benefit demonstrated with the technology they are putting on the market to compete with western tech giants. There have been legal cases brought against China in the theft of information technology such as smartphones and operating systems (Roper, 2013; Dept of Justice, 2018). In 10 years, China has managed to compete internationally with its own Huawei smartphones, which draw heavily from American companies' established patents (Cheng, 2019; USCC, 2010; Dept of Justice, 2018). However, in the case of Chinese hacking, western countries are often hesitant to report their security breaches. It can reduce confidence in business security and risk access to the Chinese markets, which remain profitable even with the risks of passive cyber attacks stealing proprietary information (NPR, 2019). One specific example is the July 21st indictment of two Chinese hackers attacking U.S. businesses. The U.S. Justice Department states:

"*The cybercrime hacking occurring here was first discovered on computers of the Department of Energy*'s *Hanford Site in Eastern Washington. As the grand jury charged, the computer systems of many businesses, individuals and agencies throughout the United States and worldwide have been hacked and compromised with a huge array of sensitive and valuable trade secrets, technologies, data, and personal information being stolen (U.S. Department of Justice, 2020).*

While determining direct economic benefit is difficult, the costs put on western companies can result in, on average, 225 billion - 600 billion dollars lost per year (IP Commission Report, 2017). However, there is a limitation to the effectiveness of cyber attacks for economic benefit. There is a significant limitation on the effectiveness of information and patent theft due to the inherent problems with reverse engineering. Gaining patents and information does not encompass the full picture of technological innovation. There are still significant entry barriers for Chinese specialists since they still lack the level of resources, the ability to experiment, and the institutional knowledge used by potential rivals (Gilli, 2018). This threat of attack also creates a significant economic disadvantage when facing Chinese companies which do not have the same burdens of attack. This lack of cyber threat is partially due to the "Great Firewall," which provides a base level of protection due to the closed nature of their internet service. There is also less incentive to attack Chinese companies since they still technologically lag behind comparable western institutions (Cheng, 2019). Therefore, there is less incentive for other actors to engage in cyber attacks against Chinese tech businesses.

In Russia's case, there is little evidence that Russia gains any economic benefit from its continued cyber campaigns. This lack of economic benefit is mostly due to their target choices, primarily government institutions rather than private companies (CSIS, 2020). Russia also does not have the same incentives due to its lack of a developed technology sector (Hanson, 2019). Russia's pursuit of more active-based attacks garners far more public attention, resulting in severe economic consequences. Western democratic states have far more of an incentive to reveal these active cyber attacks on their institutions due to policies of freedom of information and democratic accountability. Russia, due to its continuous attacks on U.S. governmental institutions resulting in harsh economic sanctions (U.S. Treasury, 2018). These sanctions directly state that:

"Treasury intends to impose additional CAATSA sanctions, informed by our intelligence community, to hold Russian government officials and oligarchs accountable for their destabilizing activities by severing their access to the U.S. financial system." (U.S. Treasury, 2018)

Any attack on private institutions has been minimal, mostly targeting fossil fuel competitors (CSIS, 2020). There can be a clear line between a hindrance to economic progress and access due to their increased use of active cyber attacks against Western states.

The preliminary conclusion drawn from the economic incentives analysis provides a compelling reason as to why China engaged in passive-based cyber attacks; however, it lacks any explanation of why Russia would engage in active attacks. This conclusion is due to the clear economic dis-incentive that Russia faces when engaging in their active attacks. They received no economic benefit, demonstrating more harm than benefit to their economic growth. That leads to the conclusion that there must be another factor at play that might explain the differences in attacks. It also does not explain why China does not favour active attacks alongside its passive cyber campaigns. China could still engage in active attacks against government institutions without losing its economic power due to the global community's reliance on its continued manufacturing dominance and central position in the global economy. China cannot be isolated in the same way that Russia is due to its growing economic power as the second largest or largest domestic economy

(Worldbank, 2019). At the same time, Russia still trails behind comparably smaller states like Italy in their global economic weight (Worldbank, 2018).

Table 5. Results of Economic Factors and the Impacts on Cyber Strategy

Results of Economic Factors and the Impacts on Cyber Strategy	**China (Passive Cyber Attacks)**	**Russia (Active Cyber Attacks)**
Institutions attacked?		
Private	**X**	
Public	**X (to help attacks on private institutions)**	**X**
Economic Focus?		
High Technology	**X**	
Resource Extraction		**X**
Direct Net Benefit?		
Yes	**X (But limited)**	
No		**X**

Relative International Power

Another possible factor in explaining why states pursue different cyber strategies is relative international power. A state's position in the international hierarchy can change the incentive structure for the respective state to engage in differing policies, especially if a state going against international consensus, and the established rules-based liberal regime (Mearsheimer, 2014). A low position in the international hierarchy increases the incentives for a state to pursue more aggressive and asymmetrical strategies. The three indicators are not the only possible frames of analysis but are the most common found in the literature. This analysis provides a broad overview of how states respond to the international community and its relations to its cyber strategies.

International Hierarchy

China's position within the international hierarchy has changed significantly since the advent of state cyber attack strategies. China's rise in the international order has been predicted since the days of Napoleon. However, in the past two decades, China has risen to become a new prominent global power. During the 20th century, China remained isolated due to its communist ruling party and documented human rights abuses (U.S. Department of State, 2019). However, in the 21st century, China has taken a far more central role to the international community. The Tiananmen sanctions imposed on China in 1989 by the western international community have lessened in importance, and the US has become China's largest trading partner (Austin, 2014; Cheng, 2019). These sanctions initially restricted the sales of arms to China but did not affect other sectors of the economy (Austin, 2014). The current U.S. sanctions state:

"The United States government maintains a prohibition on exporting defense articles and defense services to China under the general authority granted to the President and Secretary of State to control the import and export of such goods and services in the context of U.S. foreign policy, as well as pursuant to the Tiananmen Sanctions" (Congressional Report, 2006)

The reliance on China's manufacturing created an environment where the U.S. and western states could not fully isolate China from the international community. Instead, it focused on the trade of arms, which helped cause the massacre (Austin, 2014). In 2008, China was fully embraced into the international community by hosting the Olympics - widely seen as China's "coming out party," establishing them as a firm pillar of the international order. While some sanctions are still in place by the international community, especially western NATO members, they have minimal effect on continued economic and political integration of China into the international community. Due to this integration, China does not have the same incentive to outwardly break international conventions and reshape the global community to their benefit.

Russia has taken an opposite trajectory to China's position in the global hierarchy. Russia has always faced restrictions and isolation from the international community for similar reasons to China. However, after the Soviet Union's dissolution, Russia was quickly embraced by the Western world to integrate the state within the capitalist economic order (Lunde, 2014). This warmth between NATO member states and Russia began to change rapidly after the ascension of Vladimir Putin to the presidency of the Russian Federation. In 2008, Russia engaged in an attack against its neighbour Georgia establish and maintain the puppet state of South Ossetia. While this created international consternation - it did not overall affect the relationship established between Russia and NATO due to their coordination to combat Islamic terrorism. However, in 2014 this changed significantly with the Russian annexation of the Crimean peninsula and the subsequent support of eastern Ukrainian separatists. This attack provoked a significant reaction from NATO member states with the establishment of several condemning statements from the U.N. and the U.S. They adopted a resolution that:

"urg(es) the Russian Federation to withdraw its military forces from Crimea and end its temporary occupation of Ukraine's territory without delay" (U.N., 2019)

Russia was also removed from the economic group: G8 (now G7) in response to their territorial grab. The annexation of the Crimea violated U.N. law in territorial acquisition and violation of Ukraine's sovereignty (U.N., 1949). These denouncements were followed by significant economic sanctions targeting their energy-exporting markets. After these sanctions, Russia's subsequent cyber attacks on the Democratic National Convention and U.S. voting records in 2016 resulted in a strong response from the Obama administration. The sanctions created further isolation from the international community and caused significant damage to Russia's economy (Congressional Research, 2020). From 2014 onward, Russia has been increasingly isolated from the international community, driven by the NATO member states to condemn and reverse Russia's blatant land grab. This isolation from the international community demonstrates that Russia faces a new incentive to ignore the international community due to its limits to punish Russia's actions. It also demonstrates Russia's use of active cyber attacks in the 2014 Ukrainian annexation and the 2016 Democratic National Convention (DNC) hacks. Without fear of any more repercussions from the international community, Russia does not need to hide attacks while presenting the same deniability statements.

Reliance on Trade

The next indicator is the reliance of either state on international trade within the global economy. As stated previously, China is integrated into the international global markets as a hub on manufacturing and a growing tech giant, with the ability to compete against more technologically advanced economies. In 2001, China was accepted into the WTO, initially excluded due to continuing disputes with Taiwan and its human rights records (WTO, 2001). Since then, China has grown to encompass 13.5% of global exports (CSIS, 2018; Worldbank 2019). It is abundantly clear that China's growth and its domestic economy is heavily reliant on international trade and maintaining a working relationship with NATO member states. China currently maintains a significant trade imbalance with the US, which gives them leverage against the US and provides an element of risk since China relies on a single market (CSIS, 2018; US Census, 2020). Western businesses still face the risk of theft by engaging with the Chinese market; however, the risks associated with information theft are not enough to dissuade companies from investing in China's rapidly growing economy (NPR, 2019). China's trade is facing competition with lower-wage markets, which can provide the same manufacturing resources with a cheaper labour cost (Cheng, 2019). China is beginning to focus on creating its service and consumer economy within the country. The 11th Five Year Plan outlined China's priorities to shift towards a service-based economy to maintain its economic growth to offset the competition faced within the manufacturing markets (Fravel, 2019). With this change, China might become less reliant on international trade, but it will take decades for the manufacturing trade imbalances to shift away from China's favour. This economic structure maintains China's incentive to work within the liberal world order and not break norms to invite sanctions or condemnation (Mearsheimer, 2010). However, western governments are turning a blind eye to several ongoing human rights violations, due to their reliance upon an economically stable China.

Russia is engaged in international trade in energy exports and natural resource extraction. Europe remains reliant upon Russia's natural gas exports to supply the EU's ever-growing energy demands. Over 50% of their exports are either unrefined and refined crude oil or natural gas (Worldbank, 2019). Russia however, still retains a positive trade balance with most of its international partners. Europe's reliance on Russian energy exports has led the EU to attempt to diversify and seek other markets to provide them with their energy needs such as Saudi Arabia, the US and other OPEC countries (CRS, 2006; Kim, 2014). Russia's economy is heavily reliant on international trade. However, due to the majority of their income from natural resources, they are subject to changes in commodity prices. Commodity prices can drastically shift, resulting in volatile economic output. In the face of western sanctions, Russia can export their goods due to the high demand for hydrocarbons and the availability of markets in the Global South (Worldbank, 2019). These markets in the Global South are less restricted and care less about international norms than their western counterparts. This reliance on international trade is a large part of Russia's economy. Russia remains reasonably immune to economic sanctions since many European NATO members and other states remain reliant on their energy demands (Kim, 2014). This immunity allows them a certain amount of leeway to pursue far more aggressive actions than other states, which could be isolated from the international community, such as Iran. The immunity to international condemnation results in different incentives since they wish to change their position within the international hierarchy. Russia can operate outside of the established international conventions and laws without more repercussions. The lack of repercussions provides more incentive to engage in more active cyber attacks without the fear of international blowback.

Territorial Disputes

Both states have outstanding territorial disputes with neighbouring states. However, China and Russia's approaches have been significantly different in their attempts to resolve these issues. China currently has multiple outstanding territorial disputes with many of its neighbours. The most prominent territorial dispute is the island of Taiwan, functioning as a separate state even though the Chinese government considers it its province. Another major territorial dispute China faces is its maritime borders in the South China Sea (Hayton, 2014). This stretch of ocean colloquially known as the "cow's tongue" is claimed by six other countries. This dispute has not stopped China from building military bases throughout the smaller island chains within the area to secure their position (Hayton, 2014). The final major territorial dispute is the Sendaku Islands currently administered by Japan. This claim goes back to the first Sino-Japanese war and remains a sore point in the relations between the two countries (Hayton, 2014). In pursuing territorial claims, China does not engage in conventional warfare to annex these regions, preferring to engage in a long diplomatic dance with the respective countries (Fravel, 2018). They do not push these claims outright out of fear of a conventional response upon their mainland. In all these three cases, China has not responded conventionally due to the protection of the US. The US has defensive policies with many states around China to reduce its potential expansion (Hayton, 2014; Fravel, 2018). This cordoning forces China to engage in intelligence gathering and information warfare to gain a strategic edge against these possible combatants in the event of a defensive war (Fravel, 2018; Cheng, 2019). China uses passive cyber attacks for intelligence gathering and hacking the disputing governments to gain information on how to delay UN sanctions and win international court cases (Hayton, 2014; Cheng, 2019). They firmly maintain the norms established in 1945 of no aggressive territorial gain. However, there are isolated cases within the South China Sea of aggressive actions against civilian fishing vessels (Hayton, 2014). These territorial claims create a policy of information gathering through cyber attacks to delay or stall any international attempts to combat their gradual expansion of influence into disputed territories.

Russia pursues an entirely different policy when facing territorial disputes. They often engage using conventional warfare to either gain their territory or sponsor an internal rebellion with their military support (Delcour, 2014). This policy was demonstrated by the 2008 invasion of Georgia and South Ossetia. This internal conflict, encouraged by Russia, provided a context for the Russian military to engage. The most infamous recent territorial dispute Russia faces is the annexation of the Crimean peninsula and their sponsored invasion of eastern Ukraine. In both cases, Russia used its cyber capabilities to engage in active attacks against opposing state institutions to help their conventional military invasion (Connell, 2017). Russia's use of their conventional military to back up their international claims is a clear violation of UN law, and the norms of sovereignty established in 1945. Due to the lack of following international norms, Russia does not hesitate to use active cyber attacks against defending states and western states since they have already proven they can violate international norms and laws without severe repercussions. Russia currently maintains several unrecognized puppet states in several neighbouring countries like South Ossetia, Transnistria and Nagorno Karabach (Delcour, 2014). They have created a stalemate in these conflicts but have achieved their goals of claiming their disputed territory in practice, if not in writing. The aggressive pursuit of their international claims using hybrid conflict creates an established experience in engaging in active cyber attacks that other states do not have.

In analyzing a state's relative power in the international regime, China and Russia occupy significantly different positions. China maintains the international order and rules-based society since it remains a net benefit to their overall economic growth even if it hinders their territorial expansion. However, Russia shucks the conventions of international relations by using their conventional and non-conventional military assets to either expand their territory or weaken their perceived international rivals. At the same time, the dependence on their natural resource exports provides them with a layer of protection. On the other hand, China has grown in the rules-based order and has no desire to drastically alter the international regime since it remains a beneficiary of the system. Russia's inability to maintain international conventions is a compelling argument to explain why they engage in active cyber attacks. The repercussions of such attacks would not be any more severe than the current sanctions they face. However, it does not fully explain why China favours a passive cyber strategy since they retain an even more central position within the international world order. China can weather any international condemnation and due to its centrality to the world economy.

Table 6. Results of International Power and the Impact on Cyber Strategy

Results of International Power and the Impact on Cyber Strategy	China (Passive Cyber Attacks)	Russia (Active Cyber Attacks)
Is the state isolated?		
Yes		X
No	X	
Is the state reliant on international trade?		
Yes	X	X
No		
How does the state respond to territorial disputes?		
Breaking norms		X
Maintaining norms	X	

Institutional Organization

The institutions a state constructs for its cyber capabilities are critical in determining how a state will carry out its cyber-attack strategy. China and Russia have a commonality of historical communist institutions and similar concerns about investing in technological progress due to their authoritarian structures. However, the modern organizational natures of China and Russia are significantly different, and this is a compelling factor as to why these two states pursue differing strategies. There is a possible issue of endogeny, but the allocation of budgets, the institutional organization and availability of human capital are independent of cyber attack strategy. This difference in budget use is due to the possibility of resources and institutions used differently depending on the state. It is not a guarantee that a larger budget implies that a state can carry out more sophisticated cyber attacks. At the same time, the scale and capabilities of each state's investments create two different perspectives in the most efficient way to organize their cyber institutions—each looking for the most effective results in their cyber attacks compared to their available resources. The base assumption is that if institutional organization is a significant factor in cyber attack strategy, the actor with high investment, distinct organizations, and the most human capital would carry out the more complicated active cyber attacks over passive cyber attacks.

Allocation of the Budget

The first indicator is the declared budget. China has a declared cybersecurity budget of approximately 7.35 billion dollars, mostly spent on hardware capacity over software and human capital (Worldbank, 2020; Xinhua, 2019). This declared budget by Chinese state media is disputed by multiple military analysts claiming that this could underrepresent their budgets by approximately 30% (CSIS, 2020). This estimation by policy experts is mostly speculative. China's military budget is the second-largest and publicly declared at 177 billion dollars. Still, several industry experts expect that this is an under-representation of their total military spending (Worldbank 2020; China Daily, 2019). Several institutes put the overall military spending in China at approximately 239 billion dollars, increasing almost a third (CSIS, 2020). While China itself reported to the UN that they spend approximately 133 billion dollars (UN, 2018), these differing figures create confusion around what is the correct military budget of China. However, there is no universally accepted standard for reporting military budgets, since civilian spending can often mask areas that are mainly used to assist the military budget. These estimates create a window of spending between 133 billion dollars to 239 billion dollars, with several field experts that the figures could be far higher. These differing figures provided by the Chinese government are also part of a strategy to confuse their adversaries on the military's actual capabilities. Another report has also claimed that China is slowing down on its increase in military spending due to its slow economic growth in recent years (Fravel, 2018). However, there is no solid confirmation that this is the case. With such a high military budget and the second-highest allocated spending toward cyber capabilities, it can be determined that China's cyber capabilities are vast, with very few limitations. This high budget would lead to the assumption that China would be able to carry out sophisticated, active cyber attacks; however, they do not pursue this strategy.

Russia is very cagey with their military and cyber-security spending. There are few official figures and many estimates, which creates a smokescreen to hide capabilities. The most consistently reported number allocated specifically to their cyber capabilities is approximately 250 million dollars; however, that figure is merely an estimate (Crane, 2019). Russia's military budget is officially reported at 65.1 billion dollars, which, compared to its economy, is a far higher percentage than China's (SIPRI, 2020). However, estimates put the official figure much higher at almost three times that cost at 150-180billion dollars (Kofman, 2019). Another issue with determining the specific cyber-security budget is Russia's involvement and reliance upon criminal elements to help carry out specific attacks. There are no official statements, even acknowledging this possibility from the Russian government. This use of third party criminal actors is highly documented despite Russian denials. Russia has funded several criminal cyber-attack groups like FancyBear, CozyBear and EnergeticBear (Ortiz, 2020). There are no accurate estimates of Russia's spending on these operations due to its clandestine nature and the inability to identify many of these criminal attacks as state-sponsored. There is compelling circumstantial evidence that does make Russia the most likely actor funding these groups. Russia is facing a reduction in the estimated percentage of GDP spent on military assets in Russia due to their stagnant economy, and the reliance upon primary resource extraction and the fluctuating commodities market (SIPRI, 2020; Crane, 2019). Even with these shaky estimates, the window of allocated costs is still far lower than their neighbour China, mostly due to the size of each respective state economy.

Organization Division

The next indicator of institution organization is the division of institutions and the allocation of tasks. China does have delineated branches of government specifically focused on its cyber-security capabilities, but it does not eliminate the possibility of spillover into other governmental organizations (Fravel, 2017; Cheng 2019). The public face of China's cybersecurity capabilities is the Cyberspace Administration of China. This organization's mandate is to protect Chinese cyberspace and regulate the information through censorship and the promotion of state propaganda. While China does not engage in offensive capabilities outwardly, it does covert assistance to multiple cyber attacks (Cheng, 2019). The most infamous organization is the PLA Unit 61398, which has been accused by several NATO member states of carrying out several cyber attacks against private businesses and US military capabilities (Cheng, 2019; Dept of Justice, 2014; Mandiant Report, 2014).

"The indictment alleges that the defendants (5 members of PLA Unit 61398) conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). … it alleges, the conspirators also stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity." (Dept of Justice, 2014)

This unit of the People's Liberation Army is officially not acknowledged by the Chinese government, and it folded into the military institution. There is also another Unit, PLA Unit 61486, identified by the US National Security Administration, which accuses this unit of several attacks against several industry leaders in the US (CrowdStrike, 2014).

The Ministry of State Security of China also has been accused of fostering several groups responsible for cyber attacks on the US Navy and Japanese Universities (Cheng, 2019). From this available information, China has an established hierarchy and division of tasks within the specific institution of the Cyberspace Administration; however, there are multiple cases of cyber attacks being carried out from other state departments and the military. China does have a clear hierarchy; it still is undermined in an attempt to diversify where their attacks come from to help confuse their adversaries. This lack of clear delineation demonstrates that China does not maintain a clear separation of mandates, but it still has specific institutions to deal with cybersecurity.

Russia, on the other hand, has no clear administration set up to maintain its cybersecurity operations. Russia has its offensive and defensive military institutions that do not focus on maintaining the Russian state's cybersecurity. However, Russia does have the Foreign Intelligence Service, which is involved in several disinformation campaigns against the US and NATO allies (Lunde, 2014; Valeriano, 2019). The main issue with trying to determine the cybersecurity organization in Russia is the reliance upon third-party actors (grey hats) to carry out most of their cyber attacks. These groups are often criminals who are engaging in cyber attacks for criminal purposes, which are then hired by the Russian government (Lunde, 2014; Jasper, 2017; Klimburg, 2013). These groups are often unaware that they are in the employ of the Russian government due to the clandestine nature of the criminal cyber world and the Russian government. The most famous attacks from Russia, such as FancyBear and Guccifer against the DNC, were carried out by private entities in North Macedonia and Serbia (Valeriano, 2019). The Russian government did not directly carry out these attacks, but they still count as Russian operations even if the attackers are ignorant of their benefactor's overall goals (Jasper, 2017). This lack of organization clarity demonstrates that while Russia focuses on carrying out large-scale, active cyber attacks, it is often not carried out directly by state operatives. By doing so, Russia can maintain a distance from these damaging attacks while maintaining enough deniability to avoid the worst consequences of the international community. This behaviour is in contrast to the theoretical model since with a lack of organizational clarity, Russia would only be able to carry out less sophisticated passive attacks.

Availability of Human Capital

China's availability of human capital is an advantage of pursuing cyber attacks due to its large population. Along with such an endless supply of potential workers, China engages in an aggressive campaign to increase computer literacy to increase the potential pool of possible recruits (Fravel, 2017). One of their major campaigns is with its university programs at the University of Shanghai and the University of Shenzen (Cheng, 2019). Both universities created specific programs designed to educate students in the skills required to increase China's cyber literate recruitment pool. These programs are tailored explicitly for government recruitment and increasing the skills-set for cyber activities. It is estimated that China currently has between 50 000-100 000 individuals assisting their cyber-warfare campaigns spread out over multiple institutions. These individuals work in private companies, government departments and military units (Foreign Policy, 2010). There is also a significant portion of students studying at western institutions to gain knowledge and skillsets to bring back to China for the state's advantage. This use of western education can prove a disadvantage since there is a particular problem with the concept of "brain drain," where students leave China to study abroad and do not return for China to reap the benefits (Cheng, 2019). The problem of "brain drain" is reducing in significance since many students are returning to China to pursue their careers. Mostly due to China's economy broadening beyond a manufacturing-based economy towards a tertiary, service-based economy (Cheng, 2019). This diversified economy provides China with a large pool of possible human capital to carry out its cyber campaigns. With a pool of highly educated workers, China has a greater capacity to carry out destructive, active cyber attacks; however, it still focuses primarily on intelligence gathering passive cyber attacks.

Russia, however, faces an inverse problem of a significant lack of human capital. Russia is still a large state with a respectable population; however, the education levels are low (Lunde, 2014). This lack of human capital is partially due to Russia's focus on natural resource extraction, and lack of investment in education focused on its technology sector. Their educational programs are not focused on increasing their computer technology skillset. There are specific programs at the University of Moscow, and St Petersburg tailored for government cyber recruitments; these programs are lacking compared to competing Western and Chinese universities (Jasper, 2017). This lack of education creates a reliance on western education institutions, where Russia send their students to learn. The hope is they will return and bring back their learned knowledge. However, Russia is a prominent victim of the "brain drain," where many of the students who leave choose not to return, losing some of its best possible students to western state emigration (Lunde, 2014). This lack of education and supply of possible recruits creates a unique situation where Russia often relies on third-party non-state actors to help carry out their cyber attacks (Jasper, 2017). While these third parties are available to the highest bidder, it does carry some risk if these third party actors go rogue and fail to carry out the attempted attack. Contrary to the assumption, this lack of human capital does not hinder Russia's use of active cyber attacks.

The initial intuitive analysis would be that China would be able to carry out far more damaging active cyber attacks since they require significant resources. However, Russia is the dominant actor when discussing active cyber attacks (Carr, 2012; Jasper, 2017). China's availability of resources, human capital and more clearly delineated institutional structure assume that it can engage in these large scale active cyber attacks. However, China focuses on continuous and large-scale passive attacks to gain proprietary information. Russia focuses fewer resources on fewer attacks, but these are active cyber attacks with large-scale repercussions for the defending state. This focus on active cyber attacks also could be due to their reliance on third-party actors; however, there does not seem to be a specialty for these third party actors to carry out either active or passive cyber attacks (Lunde, 2014; Klimburg 2013). Russia might also attempt to focus their limited resources on getting the "biggest bang for their buck." In contrast, China can spend generously on maintaining large-scale, continuous passive cyber campaigns. However, in this analysis, it can be concluded that the institutional organization is not a significant influence on how each state determines its cyber-attack strategy.

Table 7. Results of International Organization Impact on Cyber Strategy

Results of International Organization Impact on Cyber Strategy	China (Passive Cyber Attacks)	Russia (Active Cyber Attacks)
Allocated Budget?		
High Investment	X	
Low Investment		X
Institutional Separation		
Specific institutions for cyber security	X	
Merged into other government institutions	X	X
Availability of Human Capital		
High Availability	X	
Low Availability		X

Interpretation of Deterrence

Cyber deterrence in isolation not possible due to the wide variety of possible attack angles, as well as the problems of attribution (Liblicki, 2009). The main issue is that cyber attacks break down one of the three essential components of deterrence: credibility. This break down is due to the problems of attribution and discovery highlighted previously. However, this does not mean that cyber capabilities cannot be used as a tool for general deterrence policy. There is severe difficulty in creating a cyber deterrence policy that can be as effective as possible when defending against actors that cannot be identified (Davis, 2015). These three outlined indicators provide essential context or how Russia and China interpret the novel concepts of cyber deterrence. Analyzing their interpretations of deterrence in the cyber context provides a critical demonstration of how they engage with this new context.

Historical Threats and Deterrence

China's current defence policy is "winning local wars under informative conditions.” (Fravel, p201, 2017) This policy was adopted in 2004, changing from their policy of "local wars under high technology conditions" (Fravel, p 202, 2017; CCP, 2004). This change of emphasis in their policies demonstrates their increased capacity to use their new cyber capabilities and maintains a through-line of information dominance over potential opponents. Historically, China has been mostly concerned with facing external threats, drawing back to their "century of humiliation" where colonial powers invaded China to gain beneficial trade arrangements. Then, China faced with invasion by their Japanese neighbours (Fravel, 2017). After all of that conflict, China dealt with the threat of intervention by capitalist and rival communist powers and attempts to reinstate the Taiwanese government over the ruling communist party. This history of conflict has led to China focusing on their defensive position to maintain its government, and territorial integrity. "Active defence," established in 1980 has been the policy on which all other modern defensive and deterrence policy has been based (Fravel, 2017; Cheng, 2019). Active defence is a concept based on actively maintaining information dominance over their rivals, and responding to their gathered information to prevent any wars from being engaged outside of the term of China. This policy of information gathering to maintain the strategic advantage goes back to the writings of SunTzu and carried through in Mao's policies in the civil war, and establishment of the communist state. Mao always emphasized engaging with the enemy on his terms and avoiding any situation which could be disadvantageous to their chances of winning. Mao states:

"Without preparedness, superiority is not real superiority and there can be no initiative either. Having grasped this point, a force that is inferior but prepared can often defeat a superior enemy by surprise attack." (On Protracted War, 1938)

His policy remains consistent in modern Chinese military thought. By pursuing a policy of "winning local wars under informatized conditions," information gathering and preparation provide the advantage in positioning themselves to protect against becoming involved in any conflict, which could be detrimental to the maintenance of the Chinese Communist Regime (Fravel, 2017, p 220). Regarding their cyberattack strategy, the information gathering provided is key to maintaining the strategic advantage and increasing their investment in the high tech sector. This strategy naturally ties to their historical application of deterrence through superior information gathering. By engaging in passive attacks, China can maintain its information superiority to assist in its attempts to only engage in conflict on their terms.

Russian defensive policy is based currently on the concept of conventional deterrence by maintaining a large offensive capability to discourage any status from violating territorial integrity. In interpreting the deterrence, Russia is far more eager to demonstrate its capabilities for credibility (Herspring, 1987; Kofman, 2019). Historically, this policy is consistent from the USSR to modern Russian strategic thought. Russia, like China, is also concerned with external threats over internal threats. Russia emphasizes the capabilities and credibility of its active cyber attacks by demonstrating its use whenever possible. Demonstrating their capabilities communicates to other rival states the legitimacy of Russia's threats. When regarding deterrence, Russia's policy is to demonstrate their outward capabilities to discourage any possible attack, cyber or otherwise. Russian foreign policy is based on the realist perspective, of might makes right. Russia does not trust the international institutions and the liberal order to maintain their security (Jasper, 2017). This distrust is both true in the modern era, and also during the Soviet regime. The outward-looking defensive policy has been in place since the communist revolution and the initial state goals of spreading communist across the world to overthrow the capitalist powers. Russia always viewed themselves under existential threat from capitalist powers, relied on using deterrence to maintain their security. Communist General Ogarkov emphasizes the necessity to adapt the Russian military to the modern conditions and embrace technological change and shift their priority away from the reliance on nuclear weapons. This policy included an emphasis on "weapons based on new physical principles.” (Fravel, 2017, p. 203) While he did not live to see cyber weapons - this shows incredible prescience on the future of how Russia would best move forward to increase capabilities in the computer era (Fitzgerald, 1986). Gareev also focused on incorporating new technologies in the Russian military, and puts a particular emphasis on information gathering, but also maintains the best cost-ratio to help the Russian military (Gareev, 2013) He states in "If War Comes Tomorrow:

"Major attention will be paid to the perfection of conventional precision weapons, with primary development not of defensive, but of offensive assault means, as being the most effective and economic." (Gareev, 2013, p. 49)

Russian deterrence policy is more based on demonstrating their capabilities to deter other possible attacks by enhancing the credibility of possible retaliatory attacks - coming for the Russian concept of "ustrashenie," literally translated to "intimidation" (Ven Bruusgaard, 2016, p. 8). In 2014 Russia introduced a new concept of non-nuclear deterrence defined as

"a complex of foreign policy, military and military-technical measures, aimed at the prevention of non-nuclear aggression" (Ven Bruusgaard, 2016, p. 21).

This policy put specific emphasis on fighting "remote" wars using their asymmetric capabilities to prevent any attacks on their contiguous states. Active cyber attacks contribute to this outstanding policy by engaging in active attacks against rival states. The defending state becomes more focused on protecting themselves and their interests than on pushing back against Russian influence. This application of Russia's historical concept of deterrence to cyber capabilities is demonstrated in their attacks by its significant rivals: the EU and the US.

Credibility of Current Perceived Threats

The perceived threat is another key indicator of how a state would engage in cyber capabilities since it links to the concept of credibility in regards to deterrence. China's perceived credible threats are more focused on maintaining its territorial integrity. There is some variation in the credible threats China faces, but China is most concerned with maintaining territorial integrity. Since 1994, China has viewed its international position as the most secure since the establishment of the communist regime (Fravel, 2017). This perceived security allows China to relax its defensive posture. After the establishment of the communist regime, they faced the threat of NATO invasion from Taiwan or the Korean War. Currently, China focuses mostly on the possibility of smaller local conflicts in neighbouring states rather than a full-blown invasion (Fravel, 2017). While they do have intimidating rivals close to their borders such as Russia, Japan and the US, they are comfortable in the realization that any war carried out against them from these states would be so devastating to both parties that most would avoid it (Fravel, 2017; Cheng, 2019). China is currently a rising power, and are now the second most powerful state in close competition with the US. Due to this lack of a credible existential threat to their state regime, they can relax their armed stance. They have downgraded their large military to a more manageable size, in an attempt to increase their efficiency and reduce the burden on the state's economy (Fravel, 2017; Cheng 2019). This downgrade of military investment demonstrates that China faces a low credible threat from external actors. The most existential threat to the Chinese regime is its domestic political control. Due to their authoritarian structure and censorship, they face credible threats from an increasingly educated population and a growing middle class. These factors cause the state to invest far more heavily into cyber capabilities, not just to defend their state against outside attackers but also to monitor and maintain party control over their population (Cheng, 2019).

Russia's perceived credible threats are far more numerous and considered a more existential issue to the federation's maintenance. The numerous threats are also due to Russia's international goals of regaining some of the power they lost during the Soviet collapse (Lunde, 2014). Russia is also distrusting Western institutions, partially due to the Soviet regime's precipitated collapse, helped along by NATO. The incorporation of the Baltic and eastern European states into NATO created a fear that Russia itself could be incorporated into the western NATO block, becoming a puppet state for US interests (Jasper, 2017; Lunde, 2014). This distrust was compounded due to the NATO intervention during the 2012 Libyan civil war by using the pretext of setting up a no-fly zone to help precipitate regime change (Jasper, 2019). Putin sees a credible threat of a similar conflict in which the US will use the pretext of humanitarian aid to help overthrow Russia's authoritarian regime (Shlapentokh, 2009; Hill, 2013). This fear of regime change has caused Russia to pursue active cyber attacks and information warfare in their successful attempt to distract the US from their international concerns, and slowly dividing Europe away from both the US protection and to question the EU's ability to maintain European peace and prosperity (Jasper, 2019; Ingram, 2001). Russia's fear also comes from the overarching liberal international institutions such as the UN, which on multiple occasions, has denounced their actions, especially in response to their invasion of Crimea and the subsequent support of Ukrainian separatists. This attack is due to the Maidan revolution in Ukraine, and its stated intention to join NATO and the EU to protect themselves against Russian influence. This policy shift is a significant violation of Russian security interests and an unacceptable position for the regime's maintenance. The slow crawl of NATO towards the borders created the incentive to pursue aggressive actions and demonstrates a high level of a credible threat to Russia's interests both locally and abroad.

Communication

Authoritarian states often hesitate to admit weaknesses, and acknowledging cyber attacks demonstrates that authoritarian states are not invulnerable (Carr, 2012). When an authoritarian state admits weakness, it provides a window into the state's deterrence communication. When a state admits a cyber threat, it helps determine when a state will use communication when facing significant threats. China faces multiple continuous cyber campaigns against its government and private institutions. However, they are protected by its "great firewall" but still face most cyber attacks out of any state (Cheng, 2019). The Chinese government does not often admit specific cyber attacks against their institutions. China has acknowledged cyber attacks, but they never specify where or when these attacks and the targeted institutions. Unlike democratic states committed to freedom of information, China does not have the same compulsion to be transparent to its citizens or the international community. Most of the attacks they receive are internet scams used to steal basic information for minor financial gain (Cheng, 2019). Other attacks from rival states might be happening, but China remains tight-lipped in admitting possible weaknesses. China wishes to maintain its perception as a technological leader, maintaining a strict security regime. There are multiple attacks carried against China from their neighbouring rival states with territorial disputes. Vietnam and India are particular states that attack Chinese state institutions, often to gain information to help protect their interests in the South China Sea and the Indian-Chinese borders (CSIS, 2020). China and Chinese state-run companies regularly accuse the US of engaging in cyber attacks against Chinese interests (Zetter, 2010; Lecher, 2019). Passive cyber attacks are easier to maintain deniability and demonstrates China's more relaxed international posture. China does not fear being perceived as weak, and can admit when it faces challenges in the cyber realm. These accusations against the US also help boost the regime's domestic perception, providing proof that the state is being treated unfairly by the international community.

Russia is similar in its authoritarian instincts but does not give official reports of cyber attacks against their institutions. The few attacks reported by NGOs are attacks from North Korean hackers against several Russian business interests, but not against their state functions (CSIS, 2020). There have been attacks against Russia from China as well, focusing on business interests rather than attacking state functions (CSIS, 2020). One of the issues that face attackers targeting Russia is that their state functions are not as directly reliant on computer technology as the Chinese government (Lunde, 2014). Russia does not officially admit that it faces attacks from the US or other international actors. Communicating that they are under constant attack has the risk of admitting state weakness. Russia perceives itself to be in a far more precarious position than China, therefore, and admission of weakness is dangerous to the legitimacy of the regime. Russia maintains the norm of authoritarian states in either entirely denying or never acknowledging any state's weaknesses. In 2019 there was multiple reporting of cyber attacks against Russian energy grids from the US (NYT, 2019). Russia has not even mentioned these attacks publicly. This example shows that Russia uses communication differently than China, retaining a stonewall of silence.

The concept of deterrence is the most compelling factor to explain the difference in cyber attack strategy between China and Russia. China's concept of deterrence is far more focused on information gathering and avoiding disadvantageous conflicts. Russia's deterrence concept is more to distract others by creating conflicts from afar and demonstrating superior capabilities to deter others from attacking. China's focus on passive cyber attacks lines up with this concept of maintaining information dominance due to the primary goals of passive attacks is to gain covert information for the benefit of the attacker. Russia's use of active cyber attacks works perfectly with their interpretation of deterrence. It uses these attacks to distract rival states from engaging them directly while also demonstrating the possible consequences of a direct attack on Russian interests. This theory is demonstrated historically in both countries with these concepts of deterrence being espoused by their most influential military and foreign policy strategists. The indicator of acknowledged cyber attacks demonstrates that Russia prefers total silence while China communicates when it perceives an advantage. China is more relaxed in its international posture, allowing them to use more subtle tools with long term benefits rather than pursuing distracting attacks to maintain the regime. Overall, the concept of deterrence provides the best explanation for why these two states pursue differing strategies between active and passive cyber attacks. The other possible outlined factors do influence their cyber-attack strategy, but they find themselves under the umbrella of their interpretations of their deterrence policies. The following table demonstrates how China and Russia fit perfectly within the model of how deterrence can influence the different between a cyber strategy which uses active or passive cyber attacks.

Table 8. Results of Deterrence Interpretation on Cyber Strategy

Results of Deterrence Interpretation on Cyber Strategy	Passive Cyber Attacks (China)	Active Cyber Attacks (Russia)
Historical Deterrence interpretation is based on?		
Information Superiority	**X**	
Military Threat		**X**
Perceived Threat Level?		
Low	**X**	
High		**X**
Does the state Acknowledge Attacks?		
Yes	**X**	
No		**X**

Conclusion

With the advent of cyber attacks, new questions have emerged as to how and why states pursue differing strategies. There is a distinct lack in the literature on policy analysis as to why states favour specific cyber attack strategies: passive or active? In this paper, the question: why do states favour passive or active cyber attacks was discussed. Using two case studies, Russia and China, I have concluded that each state's interpretation of deterrence is the key factor in how each respective state pursues its cyber strategies. China's interpretation of an effective deterrence policy is focused on information gathering, and knowing the potential enemies, which aligns well with passive cyber attacks. Passive attacks focus mostly on information gathering and monitoring capabilities, which do not harm the overall functions of the attacked cyber networks. Russia's interpretation of deterrence, however, is fundamentally different. Its deterrence concept is based on proving and demonstrating its destructive capabilities while also distracts rival states away from key Russia interests. Russia's interpretation works well with the use of active cyber attacks, which focuses more on destroying and harming cyber networks, allowing Russia to demonstrate its capabilities to other states.

In the literature review, there is plenty of information on how states carry out cyber attacks from a broad conceptual standpoint and a focus down on individual attack case studies. However, there is a distinct lack of policy analysis on why states engage in specific cyber strategies. There is an analysis of individual case studies such as Stuxnet or FancyBear, but not an overall analysis of a state's policy goals and strategy. Four key factors emerged as driving elements in how a state determines its cyber strategy. They are economic incentives, relative international power, institutional organization, and interpretation of deterrence. These four contributing factors are not the sole factors as to why a state engages in cyber attacks, but they are the most convincing for policy analysis. The general literature on cyber attacks and cyber strategy distinctly lacks a policy explanation as to why a state would pursue differing cyber attack strategies. Almost all analysis tends to focus on defence policy against attacks rather than the attack policy itself.

Policy analysis methodology provides an accurate overview of the main motivating factors in how a state determines its cyber strategies. The key flaw in this analysis is the lack of confidential information and primary sources. Since cyber attacks are clandestine, the information on these attacks is unreliable. However, by approaching this problem from the policy side, and using documents from both NGOs, private institutions, and the attacking and attacked governments, a fairly accurate picture is created on the motivating factors behind cyber-strategy. An analysis of motivating factors can still be done by analyzing the states' general policies and inferring their clandestine activities. This study could be improved if there was access to classified information.

Summary of Results

In this study, I have looked at four possible contenders as the major factors influencing cyber strategy; economic incentives, relative international power, committed resources, and interpretation of deterrence policy. Economic incentives provide a possible explanation as to why China engages in passive cyber attacks. Despite these incentives, it does not adequately explain why Russia is partial to active attacks. Russia has a similar incentive structure for engaging in passive attacks for economic gain but do not engage nearly as often with passive attacks. Therefore, it is clear that China has a clear economic incentive to carry out passive cyber attacks, but Russia does not benefit from their active cyber attacks.

Relative international power provides a compelling explanation as to why Russia engages in active attacks. Russia is more internationally isolated than China and has more incentive to challenge the international laws and norms. However, it does not explain why China favours passive attacks. The three indicators, state isolation from the international community, reliance on international trade, and ongoing territorial disputes, provide an overview of how relative international power affects cyber strategy. These indicators highlight that Russia does not have the same incentives to function within the international system of norms. Therefore, Russia is more likely to engage in cyber attacks, which are more destructive and break international norms. China could engage in active attacks and have similar incentives to reshape the international order and challenge norms without severe consequences. However, China seems content with its relative international power.

Institutional organization is another possible explanation for why a state engages in either active or passive attacks. The conventional wisdom is that an active attack would require more resources to carry out effectively than a passive attack. The three indicators for allocated resources are the publicly declared resources designated towards cyber capabilities and military, the next being the division of cyber institutions, and finally, the availability of trained human capital. The largest surprise of the research is Russia and China bucking the conventional wisdom, pursuing the opposite strategy of what their institutional organization would encourage.

Finally, deterrence policy is the last possible factor and the most convincing in determining why China and Russia pursue passive and active strategies. The three indicators for deterrence policy is how a state and their prominent strategists interpret deterrence, next is the perceived threat to the state, and finally, how the state acknowledges cyber attacks against their institutions. China's interpretation of deterrence is based both on their history of external imperialist invasions, followed by the continuous threat of capitalist intervention. Their interpretation of deterrence is based on gathering information and engaging the enemy on their terms after significant preparation and intelligence gathering. A similar fear of capitalist intervention influences Russia's interpretation of deterrence. However, more recently, after the fall of the Soviet Union, their deterrence policy is based on maintaining their regional dominance. Russia believes that deterrence policy is based on intimidation by demonstrating cyber capabilities and distracting their international audience. The perceived threat to each state is also different, with China seeing themselves in a relatively secure international position without existential threats from the international community. Russia fears regime change from western governments and has been proven that their western neighbours cannot be trusted to allow Russia to maintain its regional influence. Finally, the last indicator shows how each state acknowledges that cyber attacks against their institutions demonstrate typical authoritarian state behaviour from each state. China is more likely to admit they receive cyber attacks on their institutions without specifying where or when these attacks have happened. Russia engages by using both complete denials, afraid to admit their weaknesses to both the international community and their respective citizens. Interpretation of deterrence is the most convincing argument as to why China and Russia engage in different cyber strategies.

Recommendations

This study's recommendation is to focus on a state's interpretation of deterrence free of western bias. Not all states similarly interpret these concepts, therefore their actions will be different and often contrary to conventional wisdom. China and Russia's interpretation of deterrence are significantly different compared to the US and NATO states. Another recommendation is that in the analysis of clandestine activities, general non-classified state policy can be critical indicators of how a state uses secretive capabilities. Classified and public policies do not operate within a vacuum, and both contribute to each other. By analyzing both simultaneously, they can provide convincing explanations to actions that might seem counter-productive to institutions' goals, especially when institutions are not separated by mandate or law like western institutions. The last recommendation is for more thorough policy analysis of each state's theoretical sources general cyber strategy. There is significant literature on individual attacks or the conceptual framework of cyber capabilities, but there is little analysis of each state's cyber strategies policy. This lack of analysis is due to the novelty of these capabilities. Now that these capabilities have become a firmly established tool for states and a historical record to draw upon, new conclusions of how these new cyber capabilities can now move away from the theoretical discussion to a discussion of policy and strategy.

Avenues of Future Research

This analysis also brings up new possible avenues of research in policy analysis of cyber capabilities. There is the possibility of applying this analysis to other cyber capable states such as North Korea, Iran, Israel, Brazil and Turkey. China and Russia are becoming increasingly aggressive in their pursuit of cyber capabilities and engaging in cyber attacks. Does the theory of deterrence interpretation work in these case studies? Does each state have fundamental differences in their understanding of deterrence policies, and does it affect their cyber actions similarly to Russia and China? Another possible avenue of research is a closer analysis of institutional organization and the use of cyber capabilities. Both China and Russia bucked the conventional wisdom of passive attacks using fewer resources and active attacks using more. Russia, which has less committed resources and less conventional organization, engages in more costly active attacks. China had far more resources, and delineated institutions are engaging in less expensive passive attacks. Is this a case of getting more bang for your buck and using minimal resources effectively, or is the conventional wisdom and analysis of cyber attacks flawed? Another question that stems from this study is the response of attacked states to these active or passive cyber attacks. Is the response of the state receiving these attacks significantly different, and is retaliation a significant component to this response? Finally, the last question is, would this analysis be substantially changed if there was access to the classified material of the respective states? Would the conclusion remain similar? Without access, there remains a significant gap in this analysis, which could change the initial findings and analysis. Without this information, inference through public policy analysis remains the best tool.

Other avenues of further research could look more closely at capabilities and targets and how that affects specific state cyber strategy. Does the strategy change based on civilian or military targets? How much does the target influence a state's strategy, does a state maintain consistency regardless of the target? Other areas of research could look into long versos short-term intentions and strategies. Does a cyber attack on a power plant in a combat situation have the same strategic thinking behind it as a disinformation campaign, or a cyber attack stealing proprietary information? Long-term intentions are difficult to determine. However, China and Russia have a continuity of administration that allows for much more long-term strategic thinking than democratic counterparts. Does long-term strategy change the cyber attack strategy? Does a state engage in more passive or hybrid cyber attacks when pursuing long term goals? Finally, another aspect that can be explored is each state's capabilities and how that determines cyber attack strategies. This research is focused mostly on intentions and incentives over capabilities, creating a gap that could be pursued further. Do the capabilities of a larger wealthy state like China influence the strategy compared to a more impoverished state like Russia? This problem connects to the findings that resources did not affect cyber strategy incentives, with China pursuing passive attacks and Russia pursuing active attacks. This research reveals plenty of new questions to be pursued in researching cyber attacks, and can provide the stepping off point for exciting new research.

In conclusion, a state's interpretation of the deterrence concept seems key to how a state will determine its cyber-attack strategy. This conclusion is due to historical precedent and policy leaders' views deterrence as a theory and the perceived threat to the state. However, this study does not discount that the other three factors can contribute to a state's cyber strategy. They can affect the incentives for a state to use cyber attacks, but it does not override deterrence priorities. The concept of deterrence has been around since the advent of human conflict. Key thinkers have had their interpretation tested throughout the centuries with the advent of new, more destructive technology that changes the equations of conflict. This analysis is merely another stepping stone, demonstrating how centuries-old theories can still influence even the most modern technology and resultant strategies.

Bibliography:

“Additional Information: Russia’s Malicious Cyber Activity.” https://www.ncsc.gov.uk/information/additional-information-russias-malicious-cyber-activity (July 20, 2020).

Austin, Greg. 2018. *Cybersecurity in China: The Next Wave*. Springer.

Berghel, Hal. 2017. “On the Problem of (Cyber) Attribution.” *Computer* 50(3): 84–89.

Bolt, Paul J., and Sharyl N. Cross. 2018. *China, Russia, and Twenty-First Century Global Geopolitics*. Oxford University Press.

Breen, Michael, and Joshua A Geltzer. “Asymmetric Strategies as Strategies of the Strong.” : 15.

Brooks, Stevens. “Economic Actors’ Lobbying Influence on the Prospects for War and Peace - ProQuest.” http://search.proquest.com/docview/1690478059?rfr_id=info%3Axri%2Fsid%3Aprimo (July 19, 2020).

Carr, Jeffrey. *Inside Cyber Warfare*.

Cashell, Brian, William D Jackson, Mark Jickling, and Baird Webel. “The Economic Impact of Cyber-Attacks.” : 45.

Chen, Sean, and John Feffer. 2009. “China’s Military Spending: Soft or Hard Threat?” *Asian Perspective* 33(4): 47–67.

“China (Includes Hong Kong, Macau, and Tibet).” *United States Department of State*. https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/china/ (August 17, 2020).

Clausewitz, Carl von. 1832. *On War*.

Committee on Cybersecurity, Infrastructure Protection, and Security Technologies. 2013. "- Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure." https://www.govinfo.gov/content/pkg/CHRG-113hhrg82583/html/CHRG-113hhrg82583.htm (May 27, 2020).

Connell, Michael, and Sarah Vogler. 2017. *Russia's Approach to Cyber Warfare (1Rev)*. Center for Naval Analyses Arlington United States. https://apps.dtic.mil/docs/citations/AD1032208 (May 14, 2020).

Costigan, Sean S., and Jake Perry. 2016. *Cyberspaces and Global Affairs*. Routledge.

Crane, Keith, Olga Oliker, and Brian Nichiporuk. 2019. "Trends in Russia's Armed Forces: An Overview of Budgets and Capabilities." https://www.rand.org/pubs/research_reports/RR2573.html (May 14, 2020).

"Cyber Tops List of Threats to U.S., Director of National Intelligence Says." *U.S. Department of Defense*. https://www.defense.gov/Explore/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/ (July 20, 2020).

"Cybersecurity Resources | CrowdStrike." https://www.crowdstrike.com/resources/#filter=.tag-case-study (May 29, 2020).

Danilovic, Vesna. 2002. *When the Stakes Are High: Deterrence and Conflict among Major Powers*. Ann Arbor: University of Michigan Press.

Davis, Paul K. 2015. "Deterrence, Influence, Cyber Attack, and Cyberwar.(Navigating Deterrence: Law, Strategy, and Security in the Twenty-First Century)." *New York University Journal of International Law and Politics* 47(2): 355.

Delcour, Laure, and Kataryna Wolczuk. 2015. “Spoiler or Facilitator of Democratization?: Russia’s Role in Georgia and Ukraine.” *Democratization* 22(3): 459–78.

Denning, Dorothy E. 2014. “Framework and Principles for Active Cyber Defense.” *Computers & Security* 40: 108–13.

Division, US Census Bureau Foreign Trade. “Foreign Trade: Data.” https://www.census.gov/foreign-trade/balance/c5700.html (May 14, 2020).

Dynes, Scott, Eric Goetz, and Michael Freeman. 2008. “Cyber Security: Are Economic Incentives Adequate?” In *Critical Infrastructure Protection*, IFIP International Federation for Information Processing, eds. Eric Goetz and Sujeet Shenoi. Boston, MA: Springer US, 15–27.

Ebert, Hannes, and Tim Maurer. 2013. “Contested Cyberspace and Rising Powers.” *Third World Quarterly* 34(6): 1054–74.

Electricity Information Sharing and Analysis Center. 2016. “Analysis of the Cyber Attack on the Ukrainian Power Grid.” https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (May 14, 2020).

“FireEye: Neuer Mandiant Threat Report.” 2014. *Datenschutz und Datensicherheit - DuD* 38(6): 427–427.

Fischerkeller, Michael. 2017. “Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies.” *Survival* 59(1): 103–34.

Fravel, M. Taylor. 2007. “Power Shifts and Escalation: Explaining China’s Use of Force in Territorial Disputes.” *International Security* 32(3): 44–83.

Fravel, Taylor M. 2019. “Active Defense, China’s Military Strategy since 1949.” https://play.google.com/books/reader?id=CgV1DwAAQBAJ&pg=GBS.PA217 (February 10, 2020).

Gallagher, Mike. 2019. “State of (Deterrence by) Denial.” *The Washington Quarterly* 42(2): 31–45.

Gareev, General Makhmut Akhmetovich. 2013. *If War Comes Tomorrow?: The Contours of Future Armed Conflict*. Routledge.

“General Assembly Adopts Resolution Urging Russian Federation to Withdraw Its Armed Forces from Crimea, Expressing Grave Concern about Growing Military Presence | Meetings Coverage and Press Releases.” https://www.un.org/press/en/2019/ga12223.doc.htm (May 27, 2020).

George, Alexander L., and Richard Smoke. 1989. “Deterrence and Foreign Policy.” *World Politics* 41(2): 170–82.

Gilli, Andrea, and Mauro Gilli. 2018. “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.

Gorham, Michael, Ingunn Lunde, and Martin Paulsen. 2014. *Digital Russia: The Language, Culture and Politics of New Media Communication*. London ; Routledge/Taylor & Francis Group.

Hanson, Philip. “Russian Economic Policy and the Russian Economic System.” : 22.

Hart, Andrew F., and Bruce D. Jones. 2010. “How Do Rising Powers Rise?” *Survival* 52(6): 63–88.

Hayton, Bill. 2014. *The South China Sea: The Struggle for Power in Asia*. Yale University Press.

Herspring, Dale R. 1987. “Nikolay Ogarkov and the Scientific-technical Revolution in Soviet Military Affairs.” *Comparative Strategy* 6(1): 29–59.

Hill, Fiona. “The Real Reason Putin Supports Assad.” : 4.

Honkova, Jana, and Petr Suchy. 2010. “Nuclear Deterrence and the Concept of MAD in the Relations between the U.S.A. and the RF.” *Obrana a strategie* 10(1): 79–99.

Hvistendahl, Mara. “China’s Hacker Army.” *Foreign Policy*. https://foreignpolicy.com/2010/03/03/chinas-hacker-army/ (May 11, 2020).

Ingram, Alan. 2001. “Alexander Dugin: Geopolitics and Neo-Fascism in Post-Soviet Russia.” *Political Geography* 20(8): 1029–51.

Inkster, Nigel. 2015. “Cyber Espionage.” *Adelphi Series* 55(456): 51–82.

Jasper, Scott. 2017. *Strategic Cyber Deterrence: The Active Cyber Defense Option*. Rowman & Littlefield.

Jensen, Eric Talbot. 2012. “Cyber Deterrence Symposium: International Law and the Internet: Adapting Legal Frameworks in Response to Online Warfare and Revolutions Fueled by Social Media.” *Emory International Law Review* 26(2): 773–824.

Johnson, Jesse C., Brett Ashley Leeds, and Ahra Wu. 2015. “Capability, Credibility, and Extended General Deterrence.” *International Interactions* 41(2): 309–36.

Kim, Younkyoo, and Stephen Blank. 2015. “US Shale Revolution and Russia: Shifting Geopolitics of Energy in Europe and Asia.” *Asia Europe Journal* 13(1): 95–112.

Klimburg, Alexander. 2011. “Mobilising Cyber Power.” *Survival* 53(1): 41–60.

Kofman, Michael. 2019. “Russian Defense Spending Is Much Larger, and More Sustainable than It Seems.” *Defense News*. https://www.defensenews.com/opinion/commentary/2019/05/03/russian-defense-spending-is-much-larger-and-more-sustainable-than-it-seems/ (May 11, 2020).

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. 2009. *Cyberpower and National Security*. University of Nebraska Press. https://www.jstor.org/stable/j.ctt1djmhj1 (February 10, 2020).

Kshetri, Nir, and Jeffrey Voas. 2017. “Hacking Power Grids: A Current Problem.” *Computer* 50(12): 91–95.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Rand Corporation.

Lindsay, Jon R. 2013. “Stuxnet and the Limits of Cyber Warfare.” *Security studies* 22(3): 365–404.

———. 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* 1(1): 53–67.

Liu. “China to Lead Global Cybersecurity Market Growth in next 5 Years - Xinhua | English.News.Cn.” http://www.xinhuanet.com/english/2019-09/09/c_138377152.htm (March 12, 2020).

Maness, Ryan C., and Brandon Valeriano. 2018. “International Cyber Conflict and National Security.” *The Oxford Handbook of U.S. National Security*. https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780190680015.001.0001/oxfordhb-9780190680015-e-25 (May 29, 2020).

"Marshal Ogarkov and the New Revolution in Soviet Military Affairs: Defense Analysis: Vol 3, No 1." https://www-tandfonline-com.proxy.lib.uwaterloo.ca/doi/abs/10.1080/07430178708405274?journalCode=cdan19 (February 10, 2020).

McGraw, Gary. 2012. "Cyber War Is Inevitable (Unless We Build Security In): Journal of Strategic Studies: Vol 36, No 1." https://www.tandfonline.com/doi/abs/10.1080/01402390.2012.742013 (July 10, 2020).

McGregor, James, a former chairman of the American Chamber of Commerce in China, and on U. S. businesses reacting to Chinese hacking. "As China Hacked, U.S. Businesses Turned A Blind Eye." *NPR.org*. https://www.npr.org/2019/04/12/711779130/as-china-hacked-u-s-businesses-turned-a-blind-eye (May 9, 2020).

Mearsheimer, John J. "Can China Rise Peacefully?" : 56.

Miao, Weishan, and Wei Lei. 2016. "Policy Review: The Cyberspace Administration of China." *Global Media and Communication* 12(3): 337–40.

"Military Expenditure (Current USD) - China | Data." https://data.worldbank.org/indicator/MS.MIL.XPND.CD?locations=CN (March 12, 2020).

Ministry of National Defence. "China's National Defense in the New Era - Ministry of National Defense." http://eng.mod.gov.cn/publications/2019-07/24/content_4846452.htm (February 10, 2020).

Ministry of Economic Development of the Russian Federation. 2017. "Russian Special Economic Zones Business Investigator." https://akitrf.ru/upload/bna271217.pdf (August 17, 2020).

Monaghan, Andrew. 2013. “Putin’s Russia: Shaping a ‘Grand Strategy’?” *International Affairs (Royal Institute of International Affairs 1944-)* 89(5): 1221–36.

“N Korea Refuses to Deny Sony Hack.” 2014. *BBC News*. https://www.bbc.com/news/world-asia-30283573 (August 17, 2020).

“NATO Glossary of Terms and Definitions - (August 17, 2020).

National Academy of Sciences. 1999. “Keeping America Secure for the 21st Century.” https://clintonwhitehouse4.archives.gov/WH/New/html/19990122-7214.html (August 17, 2020).

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

Office of the Press Secretary. 2016. “Actions in Response to Russian Malicious Cyber Activity and Harassment.” *whitehouse.gov*. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and (July 20, 2020).

Official Google Blog. “A New Approach to China.” *Official Google Blog*. https://googleblog.blogspot.com/2010/01/new-approach-to-china.html (February 10, 2020).

Ortiz. “Russian Cyber Attack Campaigns and Actors.” https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors (August 17, 2020).

Oxenstierna, Susanne. 2016. “Russia’s Defense Spending and the Economic Decline.” *Journal of Eurasian Studies* 7(1): 60–70.

Ozment, Andy, and Tom Atkin. 2016. “DHS, DoD, and the National Response to Significant Cyber Indicents.” https://dod.defense.gov/Portals/1/features/

2015/0415_cyber-strategy/docs/DOD-DHS-Cyber_Article-2016-09-23-CLEAN.pdf (August 17, 2020).

Payne, Christian, and Lorraine Finlay. "Addressing Obstacles to Cyber-Attribution: a Model Based on State Response to Cyber-Attack." 49: 34.

Rennack, Dianne E. 2006. *China: Economic Sanctions*. Library of Congress Washington DC Congressional Research Service. https://apps.dtic.mil/docs/citations/ADA462480 (May 14, 2020).

Research and Threat Intel. 2014. "Hat-Tribution to PLA Unit 61486." https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/ (May 29, 2020).

Renz, Bettina. 2016a. "Russia and 'Hybrid Warfare.'" *Contemporary Politics* 22(3): 283–300.

———. 2016b. "Why Russia Is Reviving Its Conventional Military Power." *Parameters* 46(2): 23-.

"Report_Volume1.Pdf." https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf (May 27, 2020).

Reveron, Derek S. 2012. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35(1): 5–32.

Roper, Carl. 2013. *Trade Secret Theft, Industrial Espionage, and the China Threat*. CRC Press. http://www.taylorfrancis.com/books/9780429252587 (May 9, 2020).

"Russia Economic Report." *World Bank*. https://www.worldbank.org/en/country/russia/publication/rer (May 9, 2020).

Russia, Team of the Official Website of the President of. “Meeting on Economic Issues.” *President of Russia*. http://en.kremlin.ru/events/president/news/62767 (May 27, 2020).

Ryan, N. J. 2018. “Five Kinds of Cyber Deterrence.” *Philosophy & Technology* 31(3): 331-.

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

Schofield, Julian. 2016. “Chinese Industrial Espionage: Technology Acquisition and Military ModernisationWilliam Hannas, James Mulvenon, and Anna Puglisi London: Routledge, 2013, Pp. 320.” *Canadian Journal of Political Science/ Revue canadienne de science politique* 49(1): 182–83.

Schwartz, Michael I. “The Russian-A(Merican) Bomb: The Role of Espionage in the Soviet Atomic Bomb Project.” *History of Science*: 6.

Cheng, D. 2017. *Cyber Dragon: Inside China’s Information Warfare and Cyber Operations*. ABC-CLIO, LLC. https://books.google.ca/books?id=apf2jgEACAAJ.

Shaji, Ramaswamy Swarnammal, V. Sachin Dev, and Thomas Brindha. 2019. “A Methodological Review on Attack and Defense Strategies in Cyber Warfare.” *Wireless Networks* 25(6): 3323–34.

Shlapentokh, Vladimir. 2009. “Perceptions of Foreign Threats to the Regime: From Lenin to Putin.” *Communist and Post-Communist Studies* 42(3): 305–24.

“Significant Cyber Incidents | Center for Strategic and International Studies.” https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents (February 10, 2020).

“SIPRI Military Expenditure Database | SIPRI.” https://www.sipri.org/databases/milex (May 11, 2020).

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

U.S.-China Economic and Security Review Commission. 2013. “2013 Annual Report to Congress.” https://www.uscc.gov/annual-report/2013-annual-report-congress (August 17, 2020).

“The United States Condemns Russian Cyber Attack Against the Country of Georgia.” *United States Department of State*. https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/ (July 20, 2020).

United States District Court for the District of Columbia. “United States of America v. Internet Research Agency LLC, Concord Management and Consulting LLC, Concord Catering.” https://www.justice.gov/file/1035477/download (May 11, 2020).

The National Bureau of Asian Research. 2017. “Update to the IP Commission Report.” http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf (August 17, 2020).

"Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks | U.S. Department of the Treasury." https://home.treasury.gov/news/press-releases/sm0312 (May 14, 2020).

"Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion (May 14, 2020).

"Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research." 2020. https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion (August 9, 2020).

"UK Condemns Russia's GRU over Georgia Cyber-Attacks." *GOV.UK*. https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks (July 20, 2020).

"UK Exposes Russian Cyber Attacks." *GOV.UK*. https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks (July 20, 2020).

Uma, M., and G. Padmavathi. 2013. "A Survey on Various Cyber Attacks and Their Classification." *I. J. Network Security* 15: 390–96.

United Nations Office for Disarmament Affairs. 2017. "Instrument for Standardized International Reporting of Military Expenditures." https://unodaweb.s3.amazonaws.com/wp-content/uploads/2019/03/MilEx-2017-China.pdf (May 11, 2020).

United Nations Security Council. "Provisions of Chapter XVI of the Charter."

"U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (May 14, 2020).

"U.S. Escalates Online Attacks on Russia's Power Grid - The New York Times." https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html (May 14, 2020).

Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press.

Ven Bruusgaard, Kristin. 2016. "Russian Strategic Deterrence." *Survival* 58(4): 7–26.

Weber, Valentin. 2018. "Linking Cyber Strategy with Grand Strategy: The Case of the United States." *Journal of Cyber Policy* 3(2): 236–57.

Welt, Cory, Kristin Archick, Rebecca M Nelson, and Dianne E Rennack. "U.S. Sanctions on Russia." : 75.

Worldbank. 2019. "Gross Domestic Product 2018." https://databank.worldbank.org/data/download/GDP.pdf (May 14, 2020).

"WTO | NEWS - WTO Successfully Concludes Negotiations on China's Entry - Press 243." https://www.wto.org/english/news_e/pres01_e/pr243_e.htm (July 20, 2020).

Zedong, Mao. 1938. “On Protracted War.” *The Selected Works of Mao Zedong* 2: 113–94.

Zetter, Kim. 2010. “China Accuses U.S. of Cyberwarfare.” *Wired*. https://www.wired.com/2010/01/china-accuses-us/ (August 11, 2020).