Master’ s Thesis of International Relations

Imperfect Attribution and Contingent Deterrence in Cyber Warfare

August 2023

Graduate School of Political Science and International Relations
Seoul National University
International Relations Major

Maximilian Fred Hermann Hinze

Imperfect Attribution and Contingent Deterrence in Cyber Warfare

Park, Jong Hee

Submitting a master's thesis of
International Relations

July 2023

Graduate School of Political Science
Seoul National University
International Relations Major

Maximilian Fred Hermann Hinze

Confirming the master's thesis written by
Maximilian Fred Hermann Hinze
August 2023

Chair	Okyeon Yi
Vice Chair	Brandon Ives
Examiner	Jong Hee Park

Abstract

Navigating the evolving complexities of cyber warfare, this thesis examines the pivotal role of accurate attribution in effective cyber deterrence. It pioneers an interdisciplinary approach, converging insights from cyber security and political science, to unravel the motivations behind cyber attacks. Through the utilization of the Q Model and MICTIC framework, the study bridges the technological and political divide, offering a comprehensive view of cyber deterrence. Deep diving into the real-world scenarios, the research scrutinizes the U.S. response to Chinese cyber espionage and Iran's strategy against cyber aggression. These case studies illuminate how internal politics, global norms, and strategic culture influence state behavior in the digital arena. The introduction of "Contingent Deterrence" adds a fresh perspective to the conceptualization of cyber deterrence. This thesis further underscores the crucial role of international collaboration and establishment of shared norms in enhancing mutual security in cyberspace. It culminates in a persuasive call to action for unity, innovation, and multidimensional strategies to combat the evolving cyber threats. By providing actionable insights and emphasizing the need for accurate attribution, this research contributes significantly to ongoing discussions on cyber security, ultimately paving the way towards a more resilient and secure cyber ecosystem.

Keywords: Cyber Warfare, Deterrence, Attribution, United States, China, Iran

Student Number: 2018-28029

Table of Contents

List of Figures

Chapter 1. Research Problem

1.1 Background

The swift advancement of technology and the emergence of the digital age have inaugurated a new epoch of conflict characterized by the phenomenon of cyber warfare. This contemporary form of warfare presents unprecedented challenges for both policymakers and scholars in the field of political science as they strive to comprehend the dynamics of this intricate domain. A crucial issue in this context is the concept of deterrence in cyberspace, which has gained prominence due to the potential repercussions of cyber attacks on national security, critical infrastructure, and global stability. Conventional deterrence strategies, primarily grounded in military power and nuclear deterrence principles, may not adequately address the complexities of cyber warfare. Consequently, this master thesis aims to propose an innovative approach to augment the attribution process in cyber attacks by amalgamating insights from both cyber security and political science disciplines.

Attribution in cyber warfare is of utmost importance, as it constitutes a vital element in achieving effective deterrence. Without precise and dependable attribution, deterring potential adversaries becomes exceedingly challenging, as they might perceive a lack of consequences for their actions in the cyberspace domain. To cultivate a more refined understanding of the actors and motives implicated in cyber attacks, this thesis adopts an interdisciplinary method, drawing upon cyber security whitepapers and political science frameworks. In doing so, it underscores the significance of collaborative endeavors and inventive thinking in addressing the multifaceted challenges presented by cyber warfare. To bridge the divide between theoretical discourse and practical

implementation, the thesis scrutinizes two case studies of cyber attacks, exploring various factors that influence state behavior in cyberspace, such as domestic politics, international norms, and strategic culture. These case studies offer valuable insights that contribute to the formulation of a more comprehensive deterrence strategy in cyberspace.

Ultimately, this master thesis adds to ongoing debates surrounding deterrence in cyberspace by introducing the notion of "Contingent Deterrence." Through the analysis of real-world situations, the research provides practical insights that can inform policymakers in bolstering attribution capabilities, thereby fostering greater accuracy and confidence in identifying cyber attackers. By emphasizing the importance of attribution in cyber warfare, this thesis highlights the pivotal role it plays in achieving effective deterrence and, ultimately, safeguarding national and global security in the digital era.

In recent years, political scientists have made significant progress in integrating the discipline's knowledge with the rapidly emerging field of cyber warfare. The literature review in this study will illuminate these achievements as scholars have endeavored to develop novel approaches to understanding cyber conflict and its broader implications. However, despite these strides, a critical element in the discourse on cyber warfare remains underemphasized: the concept of "attribution." While numerous approaches explore the notion of deterrence in cyberspace, they often overlook the importance of attribution in formulating effective strategies. Engaging in discussions about deterrence without adequately addressing attribution is not only unproductive but potentially harmful. Inaccurate attribution can exacerbate the situation, leaving the defending state in a more precarious position than before. To address this gap and promote more rigorous thinking about attribution, this research will employ the Q Model and the MICTIC framework. Both models concentrate on the attribution

of cyber attacks, with the Q Model providing insights into "what" happened (tactical), "who" might be responsible (operational), and "why" an adversary executed the attack (strategic). Nevertheless, to adequately answer these questions, it is crucial to incorporate knowledge and analysis generated by cyber security companies. Cybersecurity companies possess unparalleled insights into network traffic and have access to extensive data logs, which are indispensable for forensic investigations. Consequently, their involvement is crucial in every attempt to attribute cyber attacks accurately. Once sufficient information is gathered to attribute an attack to a specific adversary, policymakers can then progress toward devising a deterrence policy.

This research introduces the innovative concept of "contingent deterrence," shedding light on the various types of deterrence available to policymakers and exploring the potential for cyber attacks to escalate conflicts. Through a case study analysis, the research will offer a nuanced understanding of the dynamics at play, emphasizing the importance of attribution in crafting effective deterrence strategies in cyberspace. By adopting a persuasive and human-centric approach, this study aims to contribute to the ongoing academic discourse and facilitate practical solutions to the complex challenges posed by cyber warfare.

The study advanced in this discourse endeavors to contend that the age-old deterrence theory, an enduring pillar of international relations and conflict resolution, is increasingly untenable in the swiftly transforming landscape of cyber warfare. The preeminent hurdle emanates from difficulties tied to the accurate identification of the origin of cyberattacks. For deterrence to operate effectively in the cyber realm, it is of utmost importance to competently confront and resolve this attribution problem. Whereas traditional expressions of hostility, such as territorial invasions and missile launches, can be relatively easily traced, the digital domain of cyberattacks presents a bafflingly intricate sphere, thus

exacerbating the difficulty of assigning them to specific state or non-state actors.

This study sets out to establish a solid and exhaustive theoretical underpinning for cyber deterrence, deploying two discrete frameworks: the Q Model, a recognized instrument in political science with a focus on cybersecurity, and the MICTIC framework, tailored expressly for attributing malware operations. By applying these synergistic frameworks, this research elucidates an approach to dissect cyber incidents transpiring between nations. This approach attains a substantial degree of attribution precision, thereby encouraging deterrence endeavors and addressing the initial research query regarding the adaptation of conventional deterrence in contemporary settings.

Moreover, this study emphasizes the relevance of knowledge gleaned by cybersecurity firms, as their specialized understanding of network traffic patterns yield rich, informative data for political scientists. When properly leveraged, this data can help to improve the attribution process and guide the responses of policymakers and government entities to cyberattacks.

By exploring the analysis of two distinct cases, this research illuminates the disparate reactions of state actors to cyber threats. Faced with Chinese cyberespionage, the United States exercised prudence, opting to openly associate the attacks with Chinese agents and prosecute hackers linked to the Chinese People's Liberation Army (PLA). In marked contrast, the Iranian reaction to a cyber-first-strike launched against their nuclear program, executed by a less influential nation-state, sheds light on divergent strategies employed when a nation lacks considerable global clout and is insufficiently prepared to deter cyberattacks effectively. The Iranian government, apprehensive of potential escalation by the United States, employed a tactic the research labels "deterrence by proxy," by utilizing cyber mercenaries to target United States' financial institutions and Saudi Arabian oil companies.

This investigation also acknowledges the United States' readiness to escalate to kinetic responses, as exemplified by the highly-publicized drone attack on Iranian general Qasem Soleimani. Although these case studies limit the ability to generalize, the research introduces key variables that necessitate further exploration in future studies. Successive research efforts might scrutinize the notion of "deterrence by proxy," considering factors such as a state's standing in the cyber warfare arena, its alternate deterrence capacities, the geopolitical milieu in which it functions, and ties to third parties.

Achieving potent deterrence in cyberspace calls for a collective endeavor from diverse stakeholders, with cybersecurity firms offering detailed perceptions into network traffic patterns and political scientists lending their geopolitical conflict expertise and understanding of state motivations. In addition, academic institutions can contribute significantly by fostering confidence in the attribution process via transparent, peer-reviewed knowledge that confronts the intrinsic asymmetry in public attribution of cyber incidents. Lastly, research on public opinion can serve a crucial role in strengthening deterrence policies by demonstrating national solidarity and backing for government measures in response to cyber threats.

1.2 Cyberwarfare and Deterrence

Applying traditional deterrence theory to the complex and ever-changing world of cyber warfare is no simple task. There are several key challenges that make creating an effective deterrent posture and theory in cyberspace much more difficult than in conventional military situations. These challenges include:

1) Attribution: In cyber warfare, it can be incredibly difficult to determine who is responsible for a cyber attack. This inability to accurately attribute an attack to a specific person or

group creates a major barrier to deterring or retaliating against the attacker. Without knowing who is behind an attack, it's tough to respond in a way that deters future aggression.

2) Perceptions: Managing the perceptions of potential adversaries is crucial in cyber warfare. We need to communicate our capabilities, intentions, and determination in a clear and believable way. However, managing perceptions can be complicated due to the risk of misjudgment, miscalculation, or irrational decision-making by aggressive actors.

3) Asymmetry: The lack of traditional targets and the involvement of non-combatants in the cyber domain make it difficult to determine appropriate responses to cyber attacks. This complexity makes it harder to establish clear norms and thresholds that can guide state behavior and promote stability in cyberspace, which is an essential part of effective deterrence.

4) Defensive vs. Offensive Capabilities: There is an ongoing debate among experts and policymakers about whether we should focus on building defensive capabilities or invest more heavily in offensive capabilities to achieve cyber deterrence. Finding the right balance between these two approaches is an open question that requires careful consideration.

Considering these challenges, we are faced with a critical research problem: How can we successfully adapt and apply traditional deterrence theory to the multifaceted world of cyber warfare, given the issues of attribution, perception management, asymmetry, and the debate between defensive and offensive capabilities? To address this problem and contribute to our understanding of cyber deterrence, we can explore the following research question:

1. How can we adapt the principles of traditional deterrence theory to overcome the unique challenges posed by cyber warfare, including attribution difficulties, managing

perceptions, asymmetry, and balancing defensive and offensive capabilities, to create a strong, credible, and effective cyber deterrent posture?

By investigating this research question and examining the various aspects of cyber deterrence, we can gain a deeper understanding of how to address the challenges of applying deterrence to cyber warfare. This will help us develop new strategies and policy recommendations for preventing and deterring cyber attacks, ultimately leading to a more secure and stable cyberspace for everyone involved. In order to achieve this, the research will introduce the concept of "Contingent Deterrence" which is highlighted in the theoretical background part of the thesis.

In the rapidly evolving landscape of cyber warfare, the literature review underscores the pressing issue of attributing cyber attacks to specific actors, which poses a considerable challenge to the establishment of effective deterrence strategies. Traditional deterrence theories, although invaluable for understanding conflict dynamics, are ill-suited to address the unique intricacies and challenges of the cyber domain. Cyber attacks often involve anonymous, covert actions, and rapidly evolving techniques that can obfuscate the attribution process. Consequently, there is an urgent need to develop a more comprehensive and interdisciplinary understanding of attribution and deterrence in the realm of cyber warfare.

The Q-Model by Rid and Buchanan and the MICTIC Framework by Steffens serve as methodological foundations for this research, providing comprehensive frameworks that elucidate the complexities of cyber attacks and the attribution process. By integrating these frameworks with traditional deterrence theories, the research aims to provide a more holistic understanding of the

cyber domain, fostering more effective deterrence strategies and improving the capacity to attribute cyber attacks to specific actors.

The research problem at the core of this investigation is the arduous task of accurately attributing cyber attacks to specific actors and the subsequent impact of this challenge on deterrence strategies in cyber warfare. This difficulty arises from the distinct characteristics of cyber warfare, which frequently involve anonymous, covert actions, and rapidly evolving tactics. Traditional deterrence models may not be appropriate for addressing the complexities of cyber warfare, and an interdisciplinary approach is necessary to develop effective deterrence and attribution strategies. The research problem is further compounded by the fact that many academic and policy discussions tend to focus on either the political or technical aspects of cyber warfare, creating a fragmented understanding of the issue at hand. In light of the identified research problem, the following research question emerges:

2.1 How can the MICTIC Framework be applied to a case study and enhance the attribution process?

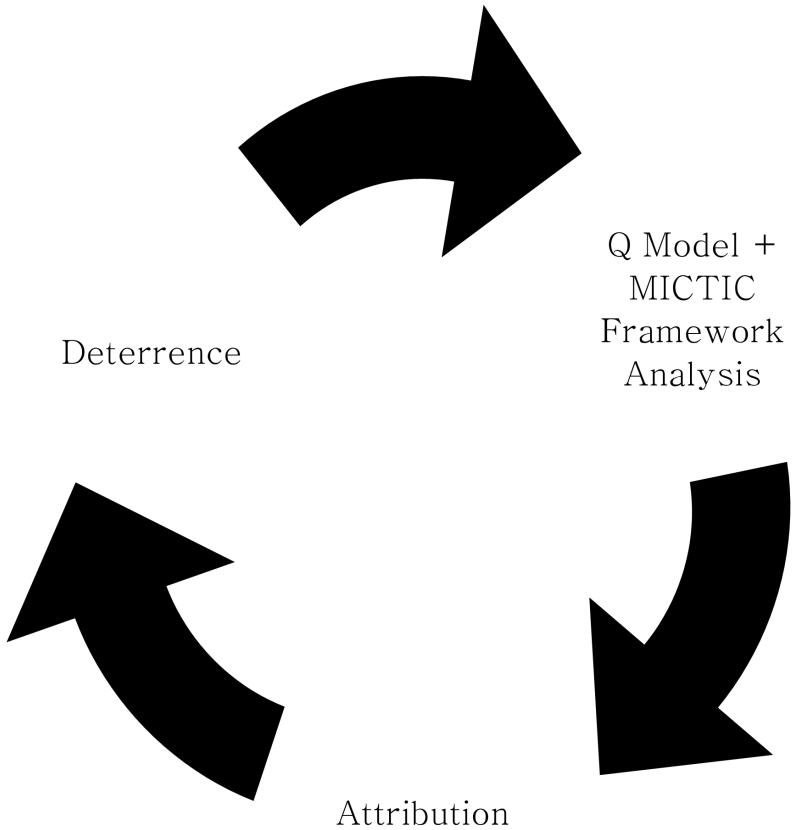
After having collected data related to an attack and categorized it with the MICTIC framework in order to enhance the attribution process, the study is able to make use of the Q Model to analyze the attribution process itself. As a way to circle back to the problem of deterrence, the research will analyze the political outcome of the attribution and how policymakers reacted to an attack. This could be in the form of indictments, economic sanctions, or announcing new laws and commitments that either boost cyber capabilities or decide to increase spending regarding offensive and defensive cyber proficiency. Therefore, the last research question is as follows:

2.2 What was the reaction of policymakers to a cyber attack, and how did their reaction contribute to the enhancement of contingent deterrence?

Addressing these research questions will involve not only a thorough examination of the existing literature on deterrence theory and cyber warfare but also the identification of case studies that exemplify the challenges of attribution in real-world scenarios. By exploring the intersections of political science and cybersecurity studies, this research will contribute to the development of a more comprehensive understanding of cyber conflict dynamics and the role of deterrence in shaping state behavior in cyberspace. Ultimately, the findings of this research will pave the way for more effective and nuanced policy discussions, fostering collaboration between the academic and practitioner communities in the pursuit of a safer and more secure cyber environment.

The following graphic will highlight the importance of this research. Since the discussion about deterrence is pointless without concrete attribution, it is absolutely necessary to mingle cyber security knowledge regarding malware analysis and resulting indicators of compromise and an adversary's tactics, techniques, and procedures with geopolitical knowledge. When it comes to the attribution of cyber adversaries, the process of attribution is a team sport that needs different specialists.

Figure 1: Attribution and Deterrence Process



1.3 Research Design

As elucidated heretofore, despite preliminary endeavors to postulate on deterrence and attribution in the realm of cyber warfare, empirical investigations incorporating an analytical framework remain conspicuously absent. The present research endeavors to address this lacuna by employing a political science framework, the Q Model, in conjunction with a cybersecurity

framework employed for attribution, the MICTIC framework. Through this integrative approach, the study seeks to attribute a cyber attack to a potential adversary with a high degree of probability, thereby paving the path for efficacious deterrence. The selection of cases adheres to the contingent deterrence model, opting for a case that aligns with each subdivision within the pyramid. Nonetheless, given the absence of a cyber-attack explicitly targeting harm to the general population, the application of a case to this particular dimension remains an unattainable objective at present. To effectively harness the insights provided by the dual frameworks underpinning this research, reliance on the specialized knowledge accumulated by cybersecurity firms is indispensable. Such entities possess unparalleled access to their clients' networks, granting them unique insights into the nature of cyber attacks. However, it is crucial to acknowledge the inherent challenges in obtaining such data for research purposes, as the information amassed by cybersecurity firms constitutes commercially valuable trade secrets. Consequently, data gleaned from an incident may be subject to confidentiality agreements as it is derived from the client's network. This caveat may potentially impact the generalizability of the findings and raises the question of whether the conclusions drawn in this research can be extrapolated to other contexts beyond the purview of this specific investigation. A myriad of variables holds significance in examining the efficacy of deterrence efforts and the ensuing outcomes between nations. One such pivotal variable pertains to a state's cyber capabilities, as expounded in the "National Cyber Power Index" (refer to p.35). The analytical portion of this research reveals that a state's response to a cyber attack varies considerably in accordance with its capabilities. Moreover, a state's geopolitical standing is of equal importance. For instance, a superpower such as the United States possesses a diverse range of response options, encompassing public attribution to garner public support for retaliation, the

imposition of economic sanctions, or even a display of kinetic military might. Furthermore, states with weaker cyber capabilities or fear of retaliation and escalation by the other party might tend to "deter by proxy," making use of "cyber guerilla" groups or "hacktivists" in order to divert suspicion from themselves to groups that are harder to attribute to a government.

Chapter 2. Deterrence and Cyber Warfare

To illuminate the distinctions between these two spheres and enable a thorough analysis, this literature review will undertake a methodical examination of classical deterrence literature. Following this, it will delve into contemporary academic research that aims to incorporate this theoretical framework into the rapidly changing cyber landscape. This approach will help create a more human-sounding text while maintaining an intellectual and academic tone.

As this research effort strives to critically appraise and amalgamate the knowledge obtained from both foundational and contemporary academic works on deterrence, it becomes increasingly clear that extrapolating and adapting the classical principles of deterrence theory to the highly dynamic and intricate domain of cyber warfare demands a diligent and refined approach. Considering the numerous challenges that emerge during this process, this research aims to not only pinpoint and analyze the critical points of departure between traditional and cyber deterrence realms but also to offer an exhaustive examination of the scholarly efforts that have endeavored to bridge these divides and create novel avenues for successfully applying deterrence theory in the era of cyber conflict.

By carefully reviewing and evaluating the current body of literature on deterrence, as well as investigating the groundbreaking theoretical and practical advancements made to expand the reach of this concept within the cyber domain, the literature review ultimately aspires to contribute to the ongoing academic dialogue on deterrence in the digital age. The conclusions and insights derived from this wide-ranging analysis will not only help enhance our comprehension of the complex relationship between deterrence theory and cyber operations but will also offer invaluable direction for devising more resilient and effective strategies and policies

aimed at addressing the risks and challenges associated with cyber warfare in the 21st century.

2.1 Classic Deterrence Theory

The well-established work on deterrence is further expounded by Michael J. Mazaar (2018)

who offers an extensive exploration of the multitude of strategies within deterrence, including the concepts of "Deterrence by denial" and "Deterrence by punishment." The notion of deterrence by denial investigates how a defending party can effectively undermine a potential attacker's confidence in achieving its objectives by rendering the anticipated outcome impossible or, if that cannot be achieved, significantly reducing the likelihood of a successful outcome. A relevant example within a military context might involve a meticulously orchestrated invasion by an aggressive force against a defending nation. If the defending nation can mobilize an adequate level of military resources, it could impose a prohibitive cost on the invasion of the aggressor. As a result, the aggressor would have to thoroughly weigh the potential for extensive losses, which might ultimately deter them from initiating the attack due to the heightened risks and stakes involved.

Conversely, the concept of deterrence by punishment (Snyde, 1959) encompasses the warning of imposing severe consequences, such as the escalation of nuclear conflict or the imposition of wide-ranging economic sanctions, in the event of an attack. However, unlike deterrence by denial, where a defending nation has the opportunity to demonstrate its military strength, the mere act of threatening to enforce harsh punishments could prove to be insufficient. The reason for this inadequacy is that the attacker might either engage in irrational behavior or express skepticism regarding the defender's commitment to implementing the punitive measures. This doubt arises from the potential that enacting severe

punishments could exacerbate the conflict further. This perspective aligns with Schelling's (1960, 123) argument concerning the nature of threats, where he contends: "Like an ordinary commitment, a threat can constrain the other player only insofar as it carries to the other player at least some appearance of obligation; if I threaten to blow us both to bits unless you close the window, you know that I won't unless I have somehow managed to leave myself no choice in the matter." This insightful analysis of deterrence strategies furnishes a more profound understanding of the complexities involved in deterring potential aggressors in various contexts.

An intriguing and multifaceted field of inquiry within the realm of deterrence that can be fruitfully applied to the domain of cybersecurity is the concept of "General" and "Immediate" deterrence. Signorino and Tarar (2003) elucidate the notion of "Immediate Deterrence" as a more short-term oriented form of deterrence that seeks to prevent a specific, imminent attack, such as during a crisis. Immediate deterrence involves rapid, decisive action to thwart the attacker's plans and forestall any destructive activity. In contrast, general deterrence is a longer-term, preventive approach aimed at dissuading would-be attackers from initiating hostile actions. One primary objective of general deterrence should be the reduction of the demand for immediate deterrence by making an attack an unappealing option for the aggressor. The overarching goal of general deterrence should be to discourage potential attackers from engaging in hostile acts by emphasizing the high costs they would incur if the defending country chose to retaliate. A robust, credible deterrent posture can help avert attacks and forestall potential conflicts in cyberspace, thereby fostering international stability and security in the digital age.

One final essential component of deterrence that necessitates attention is the aspect of perception. As the other chapters of this study will illustrate, perception occupies a central role in the realm

of cyber warfare, and to grasp how it can be employed effectively in this domain, this research will shed light on the most pertinent aspects of this notion. According to Robert Jarvis (1982–1983) perception serves as the critical variable in appraising the efficacy of a deterrence endeavor. Consequently, deterrence by perception hinges on the ability to foster a subjective perception within the minds of potential adversaries. The capacity to influence an adversary's perception can be a potent instrument in precluding hostile actions and circumventing conflict. However, it is crucial to acknowledge that historical examples have demonstrated that an overly aggressive attacker may choose to act irrationally and perceive an attack as the most viable option because they discern no alternative, fear domestic backlash, or are otherwise persuaded that the costs of inaction surpass the potential benefits. The Japanese decision to strike Pearl Harbor in 1941 exemplifies how a nation may misjudge the risks and miscalculate the costs associated with a military campaign. Thus, the significance of perception in the context of deterrence underscores the importance of strategic communication and the crafting of a lucid, credible message that accurately conveys the state's capabilities and intentions within cyberspace.

2.2 Cyber Warfare

Upon examining the theory of deterrence in its "classical" sense and highlighting the different types of deterrence applicable to the realm of cyber, the subsequent portion of the literature review will focus on the implementation of deterrence theories within cyberspace.

Martin C. Libicki's seminal work, "Cyberdeterrence and Cyberwar," (2009) stands as a trailblazer in the domain of cyber deterrence. Though the book predates the current cyber age, it persists as an indispensable resource for researchers endeavoring

to comprehend how traditional theories of deterrence apply to the novel battleground of the internet. Libicki identifies three critical and six ancillary questions that are essential for understanding deterrence within the context of cyber warfare.

The first and foremost question, as per Libicki, pertains to the challenge of attribution, which presents a substantial obstacle in the sphere of cyber warfare. If the defender cannot accurately pinpoint the origin of the attack, deterring the assailant becomes problematic. The inherent difficulty of attribution necessitates that the defender possesses high confidence in attributing the attack before any retaliation occurs (Gourley, 2018). To exemplify, the case of Japan and Pearl Harbor demonstrates how striking the incorrect target can result in catastrophic consequences and undermine the logic of deterrence by estranging potential allies. Moreover, this predicament poses a significant challenge for countries operating within transnational coalitions, such as NATO (NATO, 2018), as they must convince their allies of the attack's source to adhere to treaty obligations. However, the likelihood of persuading allies and political constituencies wanes as the question of "Who is the attacker?" considerably reduces the chances of identifying the perpetrator. This dynamic gives rise to the issue of false-flag operations, wherein an attacker masquerades as another entity to deflect blame and evade retaliation. In accordance with game theory, if the threat of retaliation is sufficiently high, executing a false-flag operation could be a judicious move for the attacker.

The second crucial question pinpointed relates to the defender's ability to jeopardize the attacker's assets (Lindsay, 2013). The severity and impact of an attack are contingent on the defender's capacity to accurately evaluate its effects. For example, assessing a kinetic attack on a refinery is more manageable than evaluating malware that subtly modifies control systems' properties. The challenge of gauging the severity of a cyber attack might complicate the defender's capacity to respond proportionately, particularly if

the retaliation risks alienating allies and partners. The Stuxnet virus, allegedly developed by the American NSA and Israel's Mossad to target Iran's nuclear facility in Natanz, exemplifies this quandary (Kesan et al., 2012).

Lastly, the final question that Libicki raises concerns the attacker's ability to execute attacks repeatedly. In order to launch an attack, the assailant must identify software vulnerabilities that are either unpatched or have no known patch, making them zero-day vulnerabilities, or socially engineer their entry into the target. However, crafting exploits for vulnerabilities demands considerable time and effort, and ultimately exposes the possibility of human error in the exploit's code. This vulnerability in the attacker's capacity to repeatedly initiate attacks serves as a significant challenge to conducting successful cyber operations.

Cyber warfare signifies a notable departure from conventional conflicts, as it encompasses not only combatants but also noncombatants, including allies and neutral third parties, as observed by Lewis (2009). This dynamic, coupled with the anonymity inherent in cyberspace, presents formidable challenges in governing the cyber domain. The complexities in distinguishing between friend and foe within the cyber realm amplify the risk of inadvertent harm, rendering the management of cyber warfare an arduous undertaking. Furthermore, Lewis notes that, during the Cold War, a symmetry of vulnerabilities existed, wherein each side possessed cities and populations that the other could target and threaten. However, this symmetry is absent in the context of cyber warfare. The lack of conventional targets and the relative ease with which assailants can operate in cyberspace make determining an appropriate response highly challenging. To address this, Lewis advocates for the establishment of norms and thresholds that can delineate a line, the crossing of which could escalate a conflict. This approach endeavors to instill greater predictability and control in the administration of the cyber domain.

In summation, Lewis's insights accentuate the intricacies and challenges associated with managing cyber warfare. The involvement of noncombatants, combined with the anonymity of cyberspace, complicates the task of discerning friend from foe. Additionally, the absence of traditional targets raises questions regarding the proper response to a cyber attack. As a solution, Lewis suggests the incorporation of norms and thresholds to furnish increased predictability and control in the governance of the cyber domain.

Attaining deterrence in the domain of cyber warfare is a vital concern for both policymakers and scholars. A significant body of political science research has concentrated on the diverse approaches to realizing deterrence in cyberspace. Two primary strategies have emerged: bolstering defensive capabilities and actively investing in offensive capabilities.

Scholars like Schutte (2012) and Buchanan (2014) have championed the construction of defensive capabilities as a means to achieve deterrence. However, Fischerkeller and Harknett (2017) have proposed an alternative approach, advocating for investment in offensive capabilities, which is also the favored method of the US Cyber Command that is responsible for offensive operations in cyberspace (United States Cyber Command, 2018). They contend that the absence of established norms in cyberspace makes the establishment of deterrence through defensive capabilities challenging. According to them, norms must materialize through behavior and international discourse, but this process has been hindered by disagreements among countries. Consequently, the actors that actively operate and dominate cyberspace will be in the most advantageous position to argue for norms they perceive as "correct" and most beneficial to their interests.

Fischerkeller and Harknett recommend that the United States concentrate on offensive cyber operations to dominate cyberspace and shape future norms. They argue that this approach would

enable the US to dissuade adversaries from engaging in cyber hostilities with the US as the target and persuade allies to consider a course of action that aligns with its own cyber strategy.

In contrast, the defensive approach emphasizes building capabilities through collaboration and geographically unrestricted security communication among nation-states employing similar technologies. While proponents of this approach acknowledge that societies with extensive IT infrastructure tend to produce tech-savvy individuals and invest more in research and development of offensive tooling, they also recognize the downsides of having a large IT infrastructure. One significant drawback is the heightened vulnerability of countries with larger IT infrastructures. As more nodes are connected throughout a country, the potential for cyber attacks increases. Although this vulnerability may not apply to technically isolated countries like North Korea, nations with extensive IT infrastructures must prioritize defensive measures to thwart cyber attacks. In addition to vulnerability, the defensive approach also underscores the importance of cooperation among nation-states to build a collective defense against cyber threats. Through collaboration and unrestricted security communication, countries can develop a shared understanding of potential threats and collectively build capabilities to counter them.

In summary, achieving deterrence in cyberspace remains a multifaceted issue. While some researchers advocate for enhancing defensive capabilities, others suggest investing in offensive capabilities as a means of dominating cyberspace and shaping future norms. The lack of established norms in cyberspace further complicates the process of achieving deterrence. As a result, policymakers and scholars must continue to investigate various approaches to accomplishing deterrence in cyberspace.

2.3 Attribution Problem

As stated in the above literature review, a significant problem that attribution faces in cyberspace is the question of who is behind an attack. Balita et al. (2020) in their work on how deterrence can be applied in a world with imperfect attribution the authors delve into the complexities of establishing deterrence strategies in contexts where attributing malicious actions to specific actors is challenging, such as in cyber warfare. Utilizing a game-theoretic model, the author investigates the delicate equilibrium between effectively deterring potential aggressors and the increased possibility of mistakenly retaliating against innocent parties due to imperfect attribution. There is also a need for emphasis on the importance of recognizing and addressing the potential risks associated with being the target of a false-flag operation in the realm of cyber warfare (McKenzie, 2017). By examining the authors' logic in relation to false-flag attacks and incorporating the subsequent example of the Olympic Destroyer attack presented in the research, a noteworthy observation can be deduced. Specifically, given that North Korea is predominantly responsible for the majority of cyberattacks directed towards South Korean government institutions and private sector entities, the South Korean government is compelled to focus its deterrence capabilities with North Korea as the primary adversary in mind. Ironically, this concentrated focus on North Korea may inadvertently create an environment in which other nations harboring geopolitical or espionage interests in South Korea are encouraged to launch their own cyberattacks and adopt more aggressive postures. This is primarily due to the reduced likelihood of suspicion being cast upon them, as the attention remains primarily on North Korea. In more concise terms, this dynamic suggests that other potential aggressors may take advantage of the cover provided by a known and persistent attacker that routinely targets the defending country,

thus further complicating the landscape of cyber deterrence and defense.

The methodological foundation of this research employs Thomas Rid and Ben Buchanan's Q-Model (Rid et al., 2015), which serves as a comprehensive framework to elucidate, facilitate, and refine the intricate process of attributing cyber attacks with precision. The authors contend that the complexities and vast scope of the attribution process necessitate the division of labor, as it is unrealistic to expect a few individuals to make comprehensive and accurate attributions independently. As a result, it is imperative for researchers to recognize the immense value of domain-specific insights offered by cybersecurity firms.

This paper demonstrates that relying solely on political science knowledge and theories is insufficient for making cogent attribution claims. The acquisition of technical evidence, the conduct of follow-up investigations, and the implementation of cyber forensics are all vital components of the attribution process. Moreover, the authors emphasize that there is no single "correct" approach or overarching methodology for attribution. Effective integration of attribution into policy demands a profound understanding of diverse disciplines, encompassing geopolitical knowledge and political science, as well as technical and forensic expertise obtainable through collaboration with cybersecurity firms.

However, because Rid and Buchanan focus a lot on the political considerations of whether an attribution result should be made public, a comprehensive framework that strives to combine political science and cyber security knowledge is still missing. Therefore, the following research will make use of the MICTIC Framework as described by Steffens (2020) to bridge the above-mentioned gap and contribute to the enhancement of the interconnected field of political science and cyber security. The MICTIC Framework is described as follows in Steffens's work.

	Aspect	Example evidence
M	Malware	Language settings, timestamps, strings
I	Infrastructure	WHOIS data, links to private websites
C	Control server	source code or logs on seized hard drives
T	Telemetry	working hours, source Ips, malware generation
I	Intelligence	intercepted communication
C	Cui bono	geopolitical analysis of strategic motivation

As the above table shows, the MICTIC framework mainly focuses on extracting technical information related to an attack conducted by an adversary. The malware aspect encompasses the creation and configuration of backdoors, trojans, and exploits. Developers are responsible for this on the attacker's side, while reverse engineers and malware analysts handle it on the information security side. The infrastructure aspect covers the process of leasing and managing servers utilized for downloading malicious code and exfiltrating data. Many Advanced Persistent Threat (APT) groups are thought to have dedicated members overseeing the infrastructure. Researchers tracking and monitoring Command and Control (C&C) servers through publicly available services mirror this on the analysis side. The control server aspect comprises individual servers and artifacts found on them, serving as the primary resources for operators executing cyber-espionage

operations. Seizing a control server typically falls under the purview of law enforcement agencies. Telemetry refers to data regarding the (predominantly manual) activities of operators within a victim's network, which can be analyzed by security companies. Government agencies have access to additional intelligence sources as part of the intelligence aspect. Lastly, the cui bono aspect corresponds to the tasking requested by the group's state sponsor, typically a non-technical department. Within the information security community, this aspect is addressed through geopolitical analysis, which examines the strategic motivations of countries aligned with the observed attacker activity.

In summary, the literature review underscores the traditional deterrence theories and their applicability in the realm of cyberspace. The examination of cyber warfare and deterrence accentuates the limitations inherent in conventional deterrence theory when addressing cyber-attacks, particularly by elucidating the challenges of attribution, a fundamental component of deterrence, in the context of malware campaigns. Unlike missile attacks or troop movements, which can be detected through satellite imagery, the act of sending a malicious email attachment is not easily observable. This raises the critical question of how political scientists and cybersecurity researchers can identify the individuals or entities orchestrating cyber offensives. The ensuing research endeavors to answer this question by integrating traditional deterrence models with whitepapers from specialized cybersecurity firms, in conjunction with the Q Model and the MICTIC framework. This approach will allow the present research to bridge the existing gap in the fields of political science and cybersecurity studies, thereby advancing these disciplines. Although there are existing theoretical frameworks and game-theoretic approaches, they remain primarily theoretical and have yet to be applied in empirical case studies. By employing the aforementioned frameworks and theories in a case study, this research will make a valuable

contribution to the understanding and practical application of deterrence, and attribution strategies in the cyber domain, thus enriching the collective knowledge in this increasingly critical area of study.

3. Theory and Frameworks

As shown in the literature review, the research will make use of the MICTIC Framework and the Q Model. In order to make use of the Q Model, the research will focus on the MICTIC framework first because doing attribution without technical detail and evidence is a moot endeavor.

3.1 MICTIC Framework

Malware, as a comprehensive term, encompasses the intricate process of creating, developing, and customizing various malicious elements, including but not limited to backdoors, trojans, and exploits. On the side of the attacker, the responsibility for this complex process primarily lies with the adept and skilled developers, while on the information security side, the equally proficient reverse engineers and malware analysts are actively involved in counteracting these malicious efforts.

The multifaceted aspect of infrastructure includes the leasing, management, and operation of servers that are specifically employed for the distribution of malicious code and the extraction of sensitive data from targeted systems. It is widely believed that several Advanced Persistent Threat (APT) groups have designated members within their ranks who possess the responsibility of meticulously managing the infrastructure. On the analysis side of this particular aspect, researchers are engaged in the persistent

tracking and monitoring of Command and Control (C&C) centers, utilizing various publicly accessible services to achieve this task.

The control server component, another essential aspect, is comprised of individual servers and the diverse artifacts that can be identified within them. These servers and their contents serve as the primary resources for the operators who are directly involved in the execution of cyber-espionage operations. The task of securing control servers and thwarting their malicious objectives generally falls under the purview of law enforcement agencies, who are entrusted with the responsibility of maintaining cybersecurity.

Security companies undertake the crucial analysis of telemetry data, which constitutes information about the predominantly manual activities of operators infiltrating a victim's network. This valuable data provides insights into the malicious activities being conducted within compromised systems. The intelligence component, on the other hand, includes an array of additional sources that are exclusively accessible to government agencies for the purpose of enhancing their cybersecurity measures and strategies.

Lastly, the cui bono aspect is of significant importance as it pertains to the specific objectives and directives requested by the sponsoring state of the group. These directives are typically assigned by a non-technical department within the state's administration. In the information security community, this aspect is addressed through a comprehensive geopolitical analysis, which aims to ascertain the nation's strategic motivations that align with the observed attacker activities. This analysis enables a deeper understanding of the potential motives and ultimate goals of cyber-espionage operations.

Cybersecurity companies like Kaspersky, CrowdStrike, and others can significantly contribute to assisting political scientists in their efforts to attribute Advanced Persistent Threat (APT) attacks. By combining their technical prowess with the analytical acumen of political scientists, these collaborations can deepen the

understanding of the motives, origins, and potential targets of cyber-espionage operations. For example, Mandiant's famous report on APT 1, which describes the Chinese People's Liberation Army's Unit 61398, was used by the US government to indict five members of that Unit while openly naming the Chinese government as the culprit behind the attack (U.S. Department of Justice, 2014).

These companies possess a wealth of technical knowledge and experience with attack vectors, malware types, and attacker methodologies. They can supply political scientists with detailed technical information and analysis about APT attacks, including tools, techniques, and procedures (TTPs) used by specific threat actors. This insight allows political scientists to identify patterns that may suggest the involvement of particular nation-states or groups. Furthermore, cybersecurity companies have access to extensive threat intelligence data, which can be shared with political scientists to enhance their understanding of the cyber threat landscape. This information may encompass data on prior APT campaigns, victim distribution, targeted sectors, and exploited vulnerabilities.

By examining the technical indicators and artifacts discovered in APT attacks, cybersecurity companies can offer valuable insights into the likely origins of these attacks. They may pinpoint specific code or infrastructure elements previously connected to known nation-state threat actors. Sharing this information with political scientists can lead to a more precise and informed attribution process. Political scientists can also benefit from the expertise of cybersecurity companies to better comprehend the geopolitical context surrounding APT attacks. These experts can shed light on the strategic motivations of various nation-states and how their cyber capabilities align with broader political and military goals. Such information helps political scientists develop a nuanced understanding of the factors driving APT campaigns and the potential consequences for global security. Collaboration on

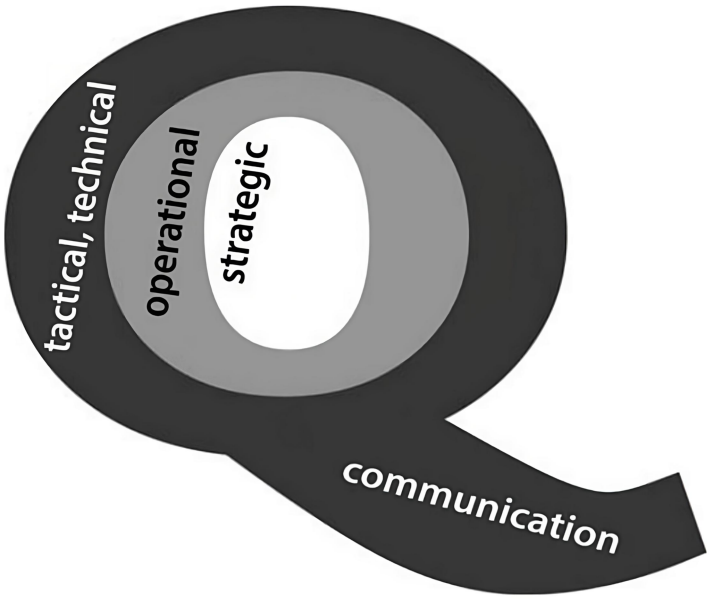
research projects and publications can advance the understanding of APT attribution, as both cybersecurity companies and political scientists combine their respective areas of expertise to produce more comprehensive and robust analyses. Additionally, joint training and workshops provided by cybersecurity companies can enhance the technical knowledge of political scientists, enabling them to incorporate technical evidence more effectively into their analyses.

In conclusion, by leveraging their respective strengths and working together, cybersecurity companies and political scientists can enhance the overall understanding of APT attacks and contribute to more accurate and reliable attribution efforts.

3.2 Q Model

The Q Model introduces a design that aims to aid researchers in their pursuit of explaining, guiding, and improving the attribution process by asking relevant questions which put an investigation of an attack into the correct political context.

Figure 2: Q Model



(Source: Rid & Buchanan 2015, p.9)

The model focuses on the different levels of analysis researchers need to cover. According to the authors, the trigger of an investigation and the resulting attribution process starts with indicators of compromise which refers to any piece of evidence or data that suggests a computer system or network has been breached, compromised, or targeted by a cyber attack. Indicators of compromise are usually only available to computer forensic analysts or malware researchers that actively try to detect and monitor attacks, thus highlighting the importance of attribution being a “team sport.” The tactical objective encompasses comprehending the incident primarily from a technical perspective, focusing on the methods employed. The operational aim involves grasping the attack's overarching framework and the assailant's characteristics – the nature of the incident. At the strategic level, the goal is to ascertain the party accountable for the attack, and evaluate the underlying motives, importance, and suitable reactions – the identification and rationale of the aggressor. This multi-faceted approach allows for a comprehensive analysis of cyber incidents, taking into account the various elements that contribute to their

occurrence and impact. Consequently, the most crucial component of the Q Model could be considered its final aspect, which pertains to communication. The authors assert that public attribution of a cyber attack to a specific adversary has the potential to enhance both attribution and defense capabilities, thereby bolstering deterrence measures. Nonetheless, the majority of whitepapers and publicly accessible reports are authored by corporations rather than governments. This fact underscores the imperative for political scientists to integrate technical knowledge within their theoretical frameworks and arguments.

Drawing upon insights garnered from cybersecurity establishments, such as Tactics, Techniques, and Procedures (TTPs), Indicators of Compromise (IOCs), and examinations of the geopolitical landscape, decision-makers can attain an augmented degree of conviction in their attribution, leading to informed policy adjustments. The Q Model emphasizes the necessity for a collaborative approach to attribution, incorporating the expertise of malware analysts, political experts, and policymakers. This framework's essence can be distilled into three key inquiries:

1) What constitutes the technical dimensions of an assault, and what is the structure of the particular malware operation? This step also includes the comparison of the TTPs and IOCs found with other malware and clusters them.

2) By evaluating the significance of the attack, the assailant's capabilities, and the political or geographical context, we can deduce the responsible party for the aggression.

3) Synthesizing the insights derived from 1) and 2), we can address the ultimate question of motivation. Identifying the adversary behind an attack and discerning the fundamental impetus allows the defender to convert these findings into strategic measures. Such actions may involve publicly ascribing the assault to a foreign entity or

implementing novel legislation to enhance defensive or offensive capacities. Moreover, by responding to the underlying rationale, adversaries may be compelled to terminate their operations, modify their strategies, or issue public rejoinders to allegations, thus influencing the targeted party's broader reaction. The most important part of the Q Model's communication part is The manner in which attribution ought to be conveyed is a significant aspect to consider. The theoretical framework suggests that sharing comprehensive information, employing approximate terminology, and acknowledging the constraints of the evaluation can enhance collective protection measures, bolster the legitimacy of the attribution, and refine the attribute ion process.

3.3 Contingent Deterrence

In the preceding sections, which encompassed an extensive literature review and delineation of the research problem, it has been established that traditional conceptions of deterrence are ill-suited to the rapidly evolving dynamics of 21st-century warfare. Consequently, the ensuing discussion will endeavor to recontextualize deterrence theories, giving rise to a novel conceptualization termed "Contingent Deterrence." Deterrence by denial, a strategy wherein state endeavors to forestall acts of aggression by rendering it exceedingly challenging or unattainable for adversaries to accomplish their objectives, exhibits minimal efficacy in the context of deterring offensive cyber operations. With respect to such operations, an effective implementation of deterrence by denial would necessitate that the defending party fortifies all internet-connected systems, thereby precluding even a single breach. A cursory examination of the modus operandi underlying offensive cyber-attacks elucidates the futility of this

pursuit. The majority of network intrusions originate from either a social engineering attack, wherein an unsuspecting employee of the target organization inadvertently activates malicious software by engaging with a seemingly innocuous document, or the exploitation of zero-day vulnerabilities. In the absence of awareness regarding the potential weaknesses inherent in the software or hardware utilized, the defending party confronts a nearly insurmountable challenge in repelling intruders. Compounding this issue is the fact that software and hardware development is predominantly the purview of third-party entities, underscoring the defender's reliance on external parties to address vulnerabilities that, if left unchecked, may precipitate catastrophic attacks.

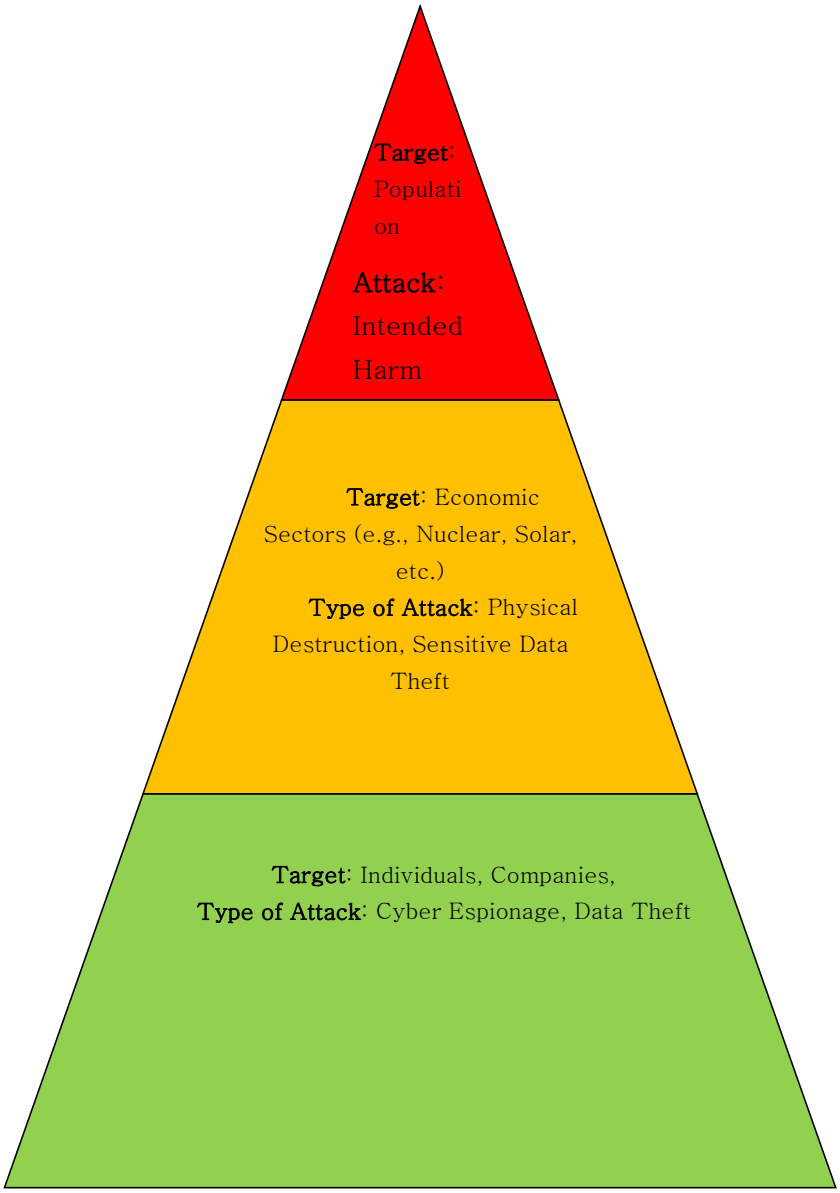
The concept of deterrence by punishment faces difficulties as well. When applied to the rapidly evolving realm of cyber warfare, however, this principle encounters a series of challenges that undermine its effectiveness. In particular, issues related to proportionality, collateral damage, and escalation expose the limitations of deterrence by punishment in the context of cyber conflict. The inherently complex nature of cyber warfare complicates the determination of an appropriate and proportional response to a cyberattack. The boundaries between state and non-state actors, as well as civilian and military targets, are often blurred in the digital realm. This ambiguity makes it difficult to assess the level of retaliation that would conform to international norms and be deemed just, thus impeding the effectiveness of deterrence by punishment. Furthermore, the nature of cyberspace exacerbates the risk of unintended consequences and collateral damage during retaliatory cyber operations. Countermeasures directed at an adversary may inadvertently impact innocent third parties or disrupt critical infrastructure, potentially resulting in significant harm to civilians and strained diplomatic relations. Moreover, the prospect of retaliation in the context of cyber warfare carries the risk of escalating tensions and inadvertently

provoking further hostile actions. Deterrence by punishment may inadvertently contribute to a spiral of increasingly aggressive cyber operations as both the original attacker and the retaliating party strive to outmaneuver one another in the digital domain. This dynamic complicates the control of a cyber conflict's intensity and duration, potentially leading to unintended and severe consequences.

Prior to proposing a framework for the implementation of "Contingent Deterrence," it is imperative to delineate several key variables, foremost among which is the critical issue of "attribution." Engaging in a discourse on deterrence without clear and precise attribution renders the conversation futile. Another pivotal variable pertains to the thresholds that may escalate a cyber conflict, as not every nation-state attack necessarily reaches the level that could precipitate an escalation. Moreover, both parties must possess a lucid understanding of the actions and potential targets that may breach these thresholds. Consequently, to establish a shared threshold, the development of international norms is essential. Given the relatively nascent state of cyber warfare as a dimension of conflict, the current landscape may be characterized as one of "mutual palpation," wherein states—some more than others—endeavor to discern their adversaries' respective thresholds. Nevertheless, this exploratory approach carries with it the ever-present risk of unintended escalation. The threshold for escalation may vary between countries, contingent upon specific values held in high regard. For instance, a democratic nation, in which politicians must be accountable to their constituents, may exercise greater caution in avoiding the loss of civilian lives potentially associated with a deterring cyberattack. This necessitates that any retaliatory action be grounded in public support. To achieve this, policymakers must be unequivocal about the thresholds and corresponding responses that ensue when a foreign adversary crosses the established boundary. Ambiguity must be eschewed in determining what constitutes an overtly hostile action.

To establish thresholds in the context of cyber warfare, nation-states must initially conduct an "inventory assessment" to determine the assets that warrant protection and the value these assets hold. Additionally, the intended target of a potential cyberattack should be taken into account. The subsequent diagram delineates three distinct components to be considered in relation to "Contingent Deterrence." It is worth noting, however, that not every offensive cyber operation will align exclusively with one component of the diagram. Some components may overlap, resulting in a Venn diagram-like representation. Furthermore, an attack may evolve from a mere information-exfiltration campaign to one with more destructive intentions. The green segment of the diagram represents targets and types of attacks that are least likely to provoke escalation, denoted by the segment's expansive breadth. In this context, the defending state possesses the broadest range of deterrent options, which may include economic or diplomatic sanctions. The subsequent stage encompasses data theft as well, with the distinction that the targeted information is of a more sensitive nature, such as military intelligence, research in critical domains like nuclear or energy, or details concerning military personnel or agents deployed abroad. The apex of the pyramid represents the narrowest portion, signifying that the defending party has limited options for deterrence and faces a high likelihood of escalating the conflict to include a kinetic component. Targets in this category may include a nation's civilian population with the objective of inflicting physical harm or, in other words, producing lethal outcomes.

Figure 3: Contingent Deterrence Model



Other important variables to consider when talking about "Contingent Deterrence" are a state's capabilities and resources. For example, a state with a strong economy, like the United States,

can retaliate with economic or diplomatic sanctions, while a nation like Iran, which is also known actively conduct offensive cyber operations, is not in a position to do so.

4. Case Studies

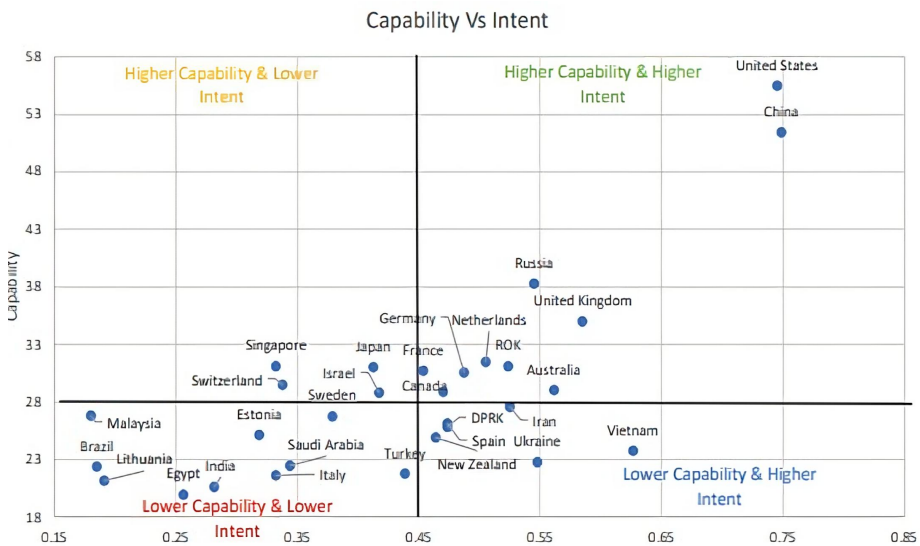
4.1 United States vs. China: Deterring Cyber Espionage and Computer Network Attacks

For an extended period spanning multiple decades, China has been recognized for its persistent efforts to develop formidable cyber warfare capabilities, which not only rival those of the United States but also surpass them in several aspects. The foundation of China's vision for cyberspace supremacy is deeply rooted in the People's Liberation Army (PLA) concept that the victor in future conflicts will be determined by the side more adept at generating and exploiting data and information (Mallick, 2022). This vision perfectly aligns with Xi Jinping's opinion "that without cybersecurity, there is no national security, the economy and society will not operate in a stable manner, and the broad popular masses' interests will be difficult to guarantee." (DigiChina, 2018)

This long-standing aspiration for dominance in cyberspace can be traced back to the Chinese phrase "wǎngluò qiángguó" (网络强国), which translates to "Internet strong country" or "Cyberpower." The term began to gain significant momentum in 2014 when it started to encompass policies related to cyberspace and other cutting-edge technologies, such as artificial intelligence. In its relentless pursuit of ascending to the status of a cyber superpower, China has strategically concentrated its efforts on several crucial areas: technological innovation, digital infrastructure development, and the establishment of a comprehensive legal and regulatory framework

governing cyberspace. Substantial efforts have been directed towards enhancing internet accessibility, investing in next-generation technologies, and nurturing domestic innovation. Particular emphasis has been placed on breakthrough areas such as artificial intelligence, big data, and quantum computing. The substantial growth and expansion of Chinese cyber capabilities are exemplified in the National Cyber Power Index (Cyber Project, 2022), as calculated by the Belfer Center for Science and International Affairs. This index serves as a testament to China's unwavering commitment to asserting its position as a global leader in the realm of cyberspace, thereby solidifying its influence in the digital domain for years to come.

Figure 4: National Cyber Power Index



(Source: National Cyber Power Index 2022, p.26)

Additionally, evidence presented in front of the "U.S.-China Economic and Security Review Commission" underscores the remarkable progress achieved under the guidance of 网络强国 (wǎngluò qiángguó). It is widely held that China is rapidly emerging as a formidable adversary for the United States in the realm of cyberspace, continuously developing and refining its offensive capabilities in a bid to accomplish strategic objectives while

simultaneously possessing sophisticated defensive capacities. The testimony further accentuates the prevailing notion that, in comparison to the advanced offensive cyber capabilities of China, the United States' current cyber defense measures appear insufficient. This discrepancy underscores the urgency for the United States to reassess and bolster its cyber defense strategies in order to effectively counteract and mitigate the risks posed by the ever-evolving Chinese cyber capabilities (DeSombre, 2022). One example of the constant strive for enhancement regarding offensive capabilities is the yearly Tianfu Cup held in Chengdu, China, where hackers try to find "zero-day"[1] vulnerabilities in products like Windows 10, Apple IOS, Safari, Chrome, and other products that are used all over the world. The outcome of the 2021 Tianfu Cup was thirty previously unknown, zero-day vulnerabilities (Cimpanu, 2021). While a similar event takes place every year in the US, called DEF CON[2], the Tianfu came under scrutiny because one of the zero-day vulnerabilities against Apple IOS was used by the Chinese government for an espionage campaign against the Uyghurs (O'Neill, 2021). Another irresponsible usage of zero-day vulnerabilities by the Chinese government was the Log4j (LunaSec, 2021) debacle that unfolded in early December 2021. Alibaba researchers decided to disclose the vulnerability responsibly, to

---

[1] A zero-day vulnerability is a previously unknown security flaw in software or hardware that has not yet been identified or patched by the vendor. Attackers can exploit this vulnerability to compromise a system or gain unauthorized access, often without the knowledge of the software or hardware developer, until it is discovered and a patch is released.

[2] DEF CON is an annual hacking conference held in Las Vegas, Nevada, which brings together cybersecurity professionals, ethical hackers, researchers, and enthusiasts from around the world. The event features presentations, workshops, and competitions focused on various aspects of cybersecurity, hacking, and emerging technologies, providing opportunities for learning, networking, and collaboration within the cybersecurity community.

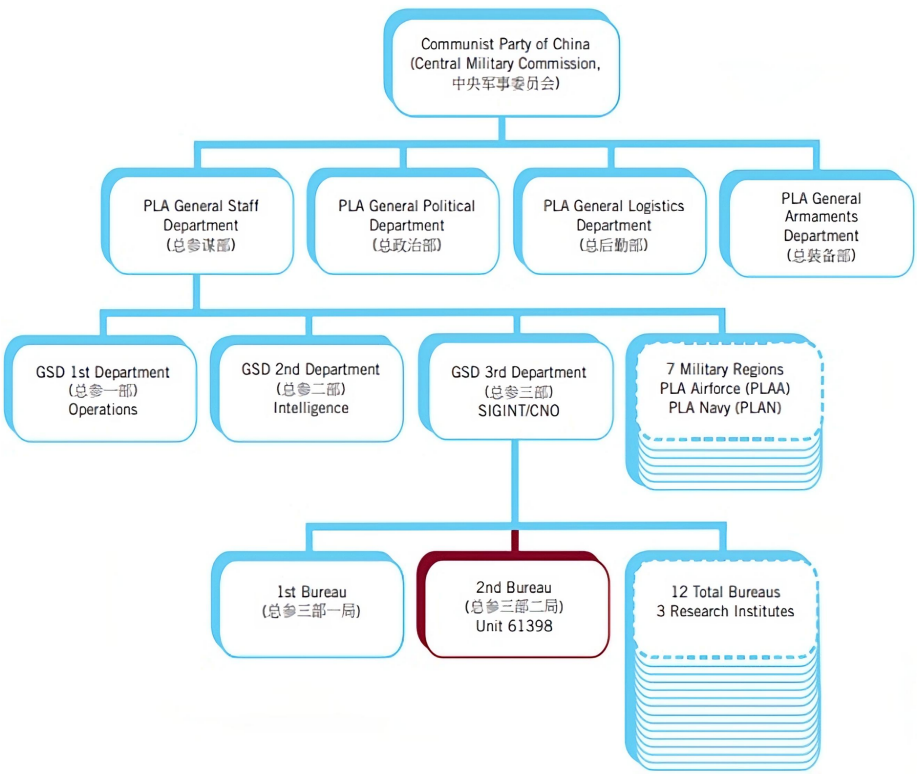
which the Chinese Ministry of Industry and Information Technology answered with a suspension of cooperation for six months (Townsend, 2021).

The United States government has been cognizant of the pressing issue of cybersecurity, with a particular focus on this matter since the early years of the twenty-first century(The White House, 2003). Recognizing that China is well aware of America's strategic vulnerability in the form of its fragile cyberinfrastructure, the US government took decisive action. The first instance of a public indictment against a foreign Advanced Persistent Threat group, henceforth referred to as APT, was directed at China's People's Liberation Army (PLA) Unit 61398 for its alleged engagement in cyberespionage activities targeting American corporations (U.S. Department of Justice, 2014). This landmark indictment identified five officers who were purportedly associated with Unit 61398, which operates under the aegis of the PLA's third department. The accused individuals were held accountable for overseeing the infrastructure employed to execute the cyberattacks. Furthermore, they were charged with a multitude of offenses, including conspiracy to commit computer fraud and abuse, unauthorized access to protected computer systems, the transmission of information with the malicious intent to inflict damage on secured computers, aggravated identity theft, economic espionage, and theft of trade secrets. This multifaceted indictment serves to underscore the gravity of the situation and the need for a persuasive and comprehensive response to such threats in order to protect the “underbelly” of the United States (Phys.org, 2009).

The following part of the research will incorporate the MICITC framework and analysis done by cybersecurity companies in order to enhance the attribution process and, as a result, make use of the Q Model in order to show how policymakers reacted to the cyber-attack and how deterrence can be achieved.

The most famous analysis of APT1's activities against US companies is Mandiant's report called "APT1: Exposing One of China's Cyber Espionage Units" (Mandiant, 2013), which is the first-ever report a private security company published about a government-funded hacking group. According to the report, the second Bureau is part of the General Staff Department's third department, which is estimated to have a personnel of roughly 130,000, with twelve additional bureaus and three research institutions responsible for different operations, such cryptology, intelligence analysis, and the interception of radio and satellite communications. Furthermore, different bureaus are responsible for different countries or continents. Unit 61398 does not only have its focus on the USA but also on other English-speaking countries like Canada (Stokes et al., 2011).

Figure 5: PLA Organization Structure



(Source: Mandiant, 2013, p.8)

APT1, has a well-documented history of using spear phishing attacks to infiltrate targeted companies (Fischer, 2013). In these attacks, the group impersonates real individuals and sends emails containing a malicious link that, when clicked, downloads a ZIP file containing a backdoor executable. This backdoor is part of the WEBC2 (Fraunhofer FKIE, 2023) family of backdoors and enables the attackers to gain access to the targeted system and control it remotely. Interestingly, the names of the malicious ZIP files used by APT1 range from military to diplomatic themes, indicating the group's broad targeting of various industries. APT1's activity dates back at least nine years prior to the public release of Mandiant's report in 2013, with the earliest known compile time of a malicious executable dating back to January 23, 2004. The attackers' use of hop servers to hide their location is notable, but their use of Microsoft's Remote Desktop Protocol provided investigators with valuable evidence. Specifically, the attackers selected the "Chinese (Simplified) – US Keyboard" layout, suggesting that they were native Chinese speakers and providing further evidence of the group's attribution to the Chinese government. While the MICTIC framework analysis does not yield significant results in the context of this attack, the investigation of the "I" (Infrastructure) and "C" (Control Server) elements provides stronger evidence linking APT1 to Unit 61398. Furthermore, of the 832 IP addresses observed by Mandiant, a vast majority were registered in the Pudong New Area of Shanghai, where PLA Unit 61398 has its headquarters (Mandiant, 2013, p. 38-42).

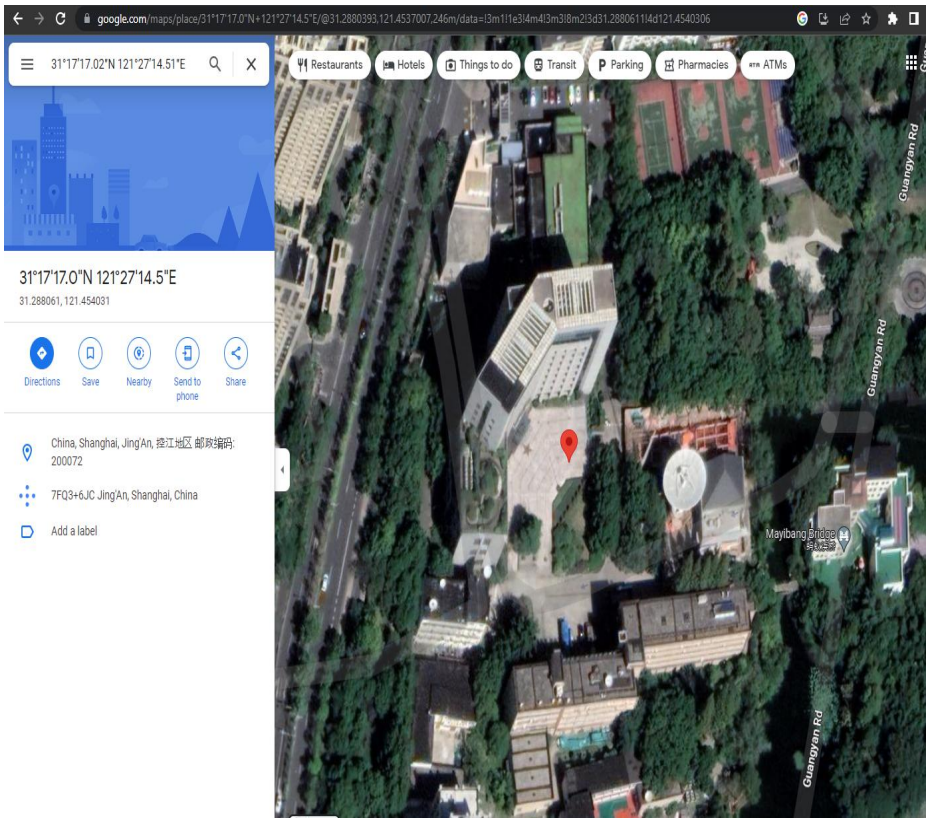
Number	Net block	Registered Owner
445	223.166.0.0 – 223.167.255.255	China Unicom Shanghai Network
217	58.246.0.0 – 58.247.255.255	China Unicom Shanghai Network
114	112.64.0.0 –	China Unicom

	112.65.266.266	Shanghai Network
12	139.226.0.0 – 139.227.255.255	China Unicom Shanghai Network
1	114.80.0.0 – 114.95.255.255	China Unicom Shanghai Network
1	101.80.0.0 – 101.95.255.255	China Unicom Shanghai Network
27	Non-Shanghai Chinese IPs	

(Source: Mandiant 2013, p.40)

In examining the Command and Control (C2) infrastructure employed by the assailants, a recurring identifier, "cpyy.chen," emerged as a notable feature. Domains associated with this handle revealed "Chen Ping" as the registrant. Delving deeper into this identifier, researchers discovered a personal blog authored by an individual born on May 25, 1979, who was employed in the military and policy sectors. The blog included images of the individual's "workplace," showcasing an array of satellite dishes and adjacent buildings. These visual clues facilitated the process of tracing the photographer's location back to the headquarters of the 12th Bureau, 3rd Department of the PLA's General Staff Department. The conclusive piece of evidence materialized in the form of a specific malware sample. The Command and Control domain corresponding to this sample was registered to an IP address situated at latitude 31°17'17.02" North and longitude 121°27'14.51" East (Crowdstrike, 2014). Intriguingly, these coordinates correspond precisely to the location of the 12th Bureau's headquarters, which houses Unit 61486. Previous observations have indicated that this unit collaborates closely with Unit 61398. The discovery of this connection added substantial weight to the case, further bolstering the argument that the attackers were indeed operating under the aegis of these military units.

Figure 6: Coordinates from an Attack leading back to PLA Buildings

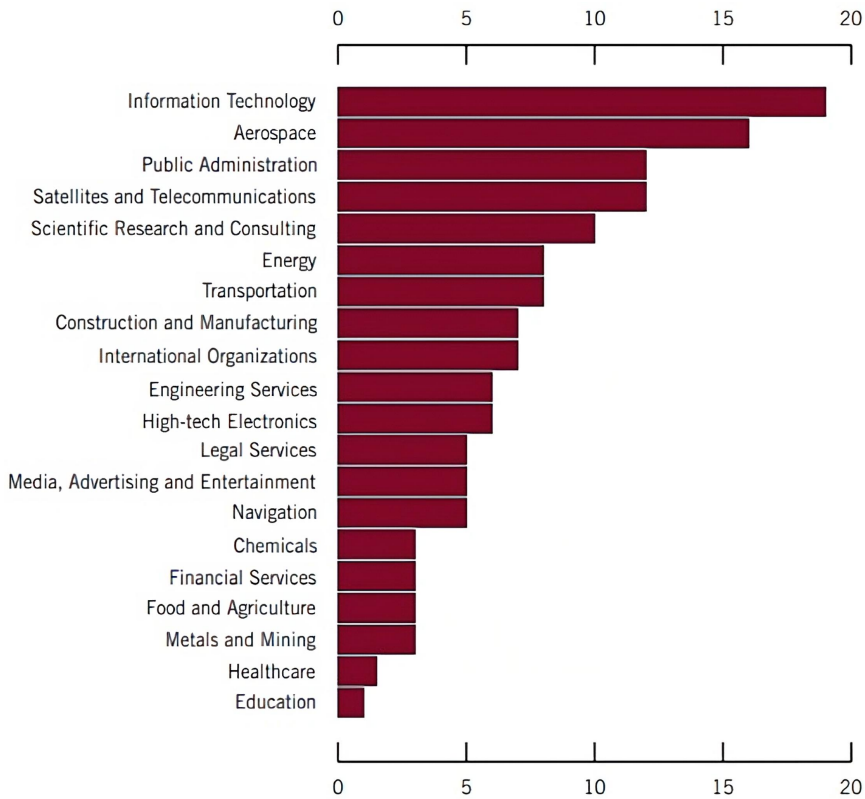


(Source: Google Maps)

The geopolitical and strategic incentives (cui bono) inherent in the MICTIC framework are further elucidated upon examining the correlation between China's Five-Year Plans and the targeted victims detailed in Mandiant's report. Among the nearly 150 victims identified, a significant majority are involved in sectors including Information Technology, Aerospace, Satellite and Telecommunications, Scientific Research and Consulting, and Energy. The 10th Five-Year Plan, spanning from 2001-2005 (International Energy Agency, 2021), underscores the significance of hydropower, nuclear power, renewable energy, and other energy sources, which is a reoccurring theme in the following Five-Year Plans as well. Although the indictment does not enumerate all victims, several mentioned are engaged in areas emphasized by the

10th Five-Year Plan. For instance, Westinghouse, which constructed four power plants in China, and SolarWind, which is developing solar power solutions, exemplify such cases. Furthermore, a recurring theme in China's Five-Year Plans is the commitment to enhancing its military capabilities and modernization efforts. During the period when APT1 was suspected to be operational, specifically from 2004 to 2013, China faced accusations in 2009 of purloining plans for the F-35 Lightning II (Clarke, 2011), which were stored on defense contractor networks and subsequently exfiltrated to foreign territories. Furthermore, the Pentagon reported that its defenses had been breached by attackers, who downloaded several terabytes of data, including information about a $300 billion-dollar stealth fighter project (Gross, 2009).

Figure 7: Victims of Chinese Cyberespionage as per Sector



(Source: Mandiant: 2013, p.24)

One critical aspect of successful deterrence is the ability to articulate one's course of action precisely in order to convey the message that the defender is willing to undergo a certain amount of "trouble" in order to dissuade adversaries from conducting further offensive operations. However, before taking action, the defender must always carefully assess the risks and benefits of its response to an attack. China is a nation with more than just a "capable" military, which decreases the range of possible deterrence actions that do not have the possibility of escalating a conflict. Even though the Obama White House said in its "International Strategy for Cyberspace" that: "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests." (The White House, 2011) Clearly, even military action is not off the table when it comes to targeted cyber attacks that might become a national threat to the United States. However, the United States decided to take the route of "Public Attribution," starting with the indictment of five Chinese military personnel thought to be responsible for attacks on several American companies. While the involvement of the Chinese Government was strictly refuted by the Chinese Ministry of Defense, calling Mandiant's report "groundless both in facts and legal basis," (Herald, 2013) further tracking of APT1 and 72 other hacking groups' infrastructures that are thought to have their origins in China, by the FireEye iSIGHT Intelligence (FireEye, 2017) team resulted in " a notable decline in China-based groups' overall intrusion activity against entities in the U.S. and other 25

countries." While it is unknown if the United States has responded to Chinese intrusions with attacks on Chinese networks on their own, the indictment seemed to have an "escalatory" effect with Xi Jinping establishing a new Cyber Intelligence Center which has the mission of improving cyber warfare capabilities by focusing on cyber reconnaissance, cyber defense, and the development of cyber weapons (Gertz, 2016). Not long after, The State Council Information Office of the People's Republic of China released a strategy paper (USNI News, 2015) in May 2015 outlining China's approach to national defense and military modernization, highlighting its strategic goals of safeguarding national sovereignty, territorial integrity, and development interests while promoting global peace and common development. To support its rise as a world power, China aims to build a strong military with a focus on modernizing its armed forces and improving combat capabilities. The strategy includes a shift from a purely defensive orientation to a combination of offense and defense, emphasizing the importance of air and maritime power. It also highlights the need for China to enhance its nuclear deterrence and counterstrike capabilities, develop advanced missile defense systems, and prioritize information warfare and cyber operations, including intelligence gathering and countering enemy cyberattacks. China's military seeks to play a more active role in international security cooperation, forming partnerships with other nations and participating in global peacekeeping missions. The document acknowledges potential threats to China's security, such as territorial disputes, separatist movements, and foreign intervention, and underscores the need for China to be prepared to respond to a wide range of security challenges. In reaction to this, the Obama White House prepared sanctions in September 2015 ahead of Xi Jinping's state visit to the United States (Liptak, 2015) The result of the meeting between President Obama and Xi Jinping resulted in the "2015 United States–China Cybersecurity Agreement (The

White House, 2015). The United States and China have reached a consensus on several key cybersecurity issues. Both nations have agreed to provide timely responses to requests for information and assistance concerning malicious cyber activities and to cooperate within the framework of their national laws and relevant international obligations. This includes investigating cybercrimes, collecting electronic evidence, and mitigating malicious cyber activities originating from their territories. Furthermore, the two countries have agreed that neither government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. In addition, both sides are committed to identifying and promoting appropriate norms of state behavior in cyberspace within the international community. They welcomed the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, which addresses norms of behavior and other crucial issues for international security in cyberspace. A senior experts group will be created for further discussions on this topic. The United States and China have also agreed to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues, with representatives from both countries' relevant ministries and agencies. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance concerning malicious cyber activities. Furthermore, both sides have agreed to establish a hotline for the escalation of issues that may arise in the course of responding to such requests. The first meeting of this dialogue will be held by the end of 2015, with biannual meetings thereafter.

However, even after the agreement between Obama and Xi, further indictments were made regarding cyber espionage and hacking attempts (Department of Justice, 2016,2018,2023). The

ongoing cyber espionage attacks led the House of Representatives to introduce new legislation (H.R.5576 – 115th Congress, 2018) which imposes financial and travel-related sanctions on individuals, entities, and foreign governments designated as critical cyber threat actors. Financial sanctions under the discussed legislation encompass asset freezing, transaction prohibition, and denial of access to financial institutions for individuals identified as critical cyber threat actors within the specified subsection. Travel-related sanctions render designated foreign nationals ineligible for admittance into the United States, visa acquisition, or receipt of entry documentation, as well as preclude them from obtaining any benefits under the Immigration and Nationality Act. Effective immediately, existing visas or entry documentation for these individuals shall be revoked. Furthermore, the President possesses the authority to impose various sanctions on foreign governments found to have supported, facilitated, or directed a critical cyber threat actor. Potential sanctions include limitations on non-humanitarian or non-trade-related aid, security assistance, opposition to loans or financial assistance from international financial institutions, and restrictions on the export of items listed on the United States Munitions List or Commerce Control List. The President may employ the authorities granted under sections 203 and 205 of the International Emergency Economic Powers Act to enact these sanctions. Coordination with US allies and partners is advised, and the Secretary of State is mandated to spearhead an international diplomatic initiative to deter cyber threat actors and offer mutual support to allied nations. Specific activities and transactions are exempt from sanctions, including authorized US intelligence activities and transactions necessary for compliance with international obligations.

The President has the discretion to waive sanctions imposition for up to one year if doing so serves national interests, law enforcement purposes, or humanitarian reasons. Moreover, the

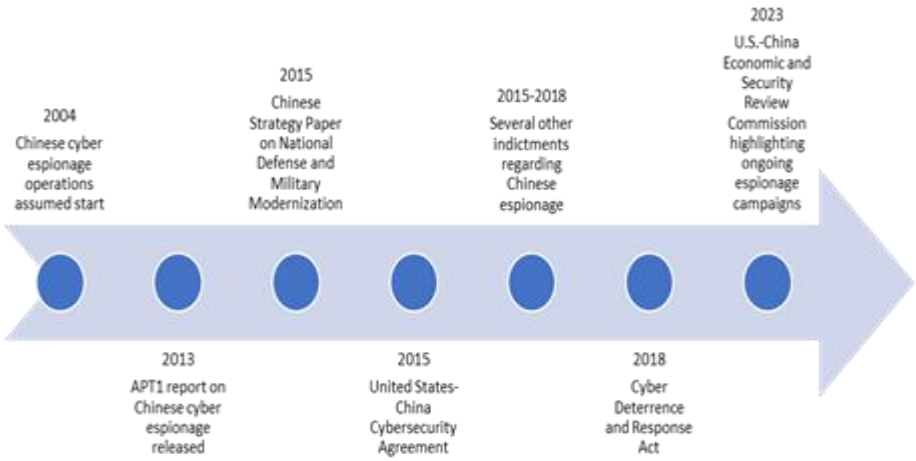
President may rescind sanctions and designations if the foreign entity can verifiably demonstrate cessation of involvement in the sanctioned conduct and provide assurances against future participation in such activities.

Lastly, this section clarifies that the legislation does not constrain the President's authority under the International Emergency Economic Powers Act or any other legal provision to impose sanctions addressing critical cyber threat actors and malicious state-sponsored cyber activities.

However, Chinese cyber espionage and ambitions to further enhance current technology and offensive capabilities have not diminished, as the hearing on "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States" (U.S.-China Economic and Security Review Commission, 2022) has shown.

The case study highlighted the threat of Chinese cyber espionage and offensive cyber operations while highlighting policy reactions that took the forms of public statements, indictments, and new legislation with the intent of deterring further Chinese cyber aggressions. However, as the case study has also highlighted, public attribution, indictments, and even bilateral agreements are not adhered to, and states are ready to disobey them at any time when they feel they are "played" by the other faction. Another possible reason for not following promises and mutual agreements is the foggy characteristic of cyber warfare. It seems that without international norms or guidelines, states are not willing to surrender to advantageous positions on the battlefield of the 21st century.

Figure 8: United States. vs China Cyber Confrontation



4.2 United States vs. Iran: Deterrence by Proxy

The Stuxnet worm, discovered in 2010, represents a turning point in the field of cybersecurity and international relations. As the first known cyberweapon specifically designed to target industrial control systems, Stuxnet not only demonstrated the potency of digital attacks on critical infrastructure but also revealed the potential for significant geopolitical ramifications. This event has had profound implications on the discourse surrounding cyber deterrence, as it exposed vulnerabilities and raised concerns about the potential escalation of cyber warfare into physical conflict. Stuxnet, therefore, has become a focal point in the evolving landscape of digital warfare and continues to shape both offensive and defensive cyber capabilities.

Tensions in the Middle East have persisted for decades; however, the revelation by the National Council of Resistance of Iran (NCRI) on August 14, 2002, during a conference at the Willard Hotel in Washington, D.C., evoked heightened apprehensions surrounding the potential expansion of Iran's nuclear program (Jafarzadeh , 2002). The report alleged that the Iranian government

was constructing a heavily fortified, subterranean facility in proximity to the town of Natanz. Moreover, the facility was purportedly situated 70 feet below ground, with multiple layers of defense, anti-aircraft weaponry, and surface-to-air missiles to safeguard against aerial assaults – a tactic for which Israel has established a precedent, not only within Iranian territory (1981) but also in Syria (2007) (Katz et all., 2017).

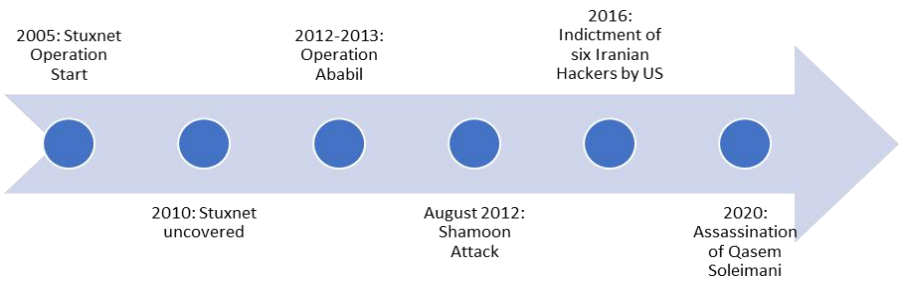
While China is known to be a fierce competitor in the realm of cyber capabilities, Iran, according to the National Cyber Power Index, ranks considerably low in capability but still much higher than average in intent. The following analysis of Iranian deterrence efforts regarding the Stuxnet attack highlights this finding.

As with the Chinese espionage case, private cyber security companies played a significant role in the attribution of the Stuxnet virus as well, highlighting once more how important it is for political science theory to incorporate domain knowledge generated by specialized companies that have access to data and knowledge public entities do not. While the Stuxnet attack did not leave as many traces in their code as the Chinese espionage attacks, the amount of sophistication combined with a geopolitical analysis shrinks the amount of parties that could have been responsible for an attack that has been called the world's first cyber weapon and the start of a new era of warfare.

According to Symantec (Broadcom, 2013), who were one of the first cybersecurity companies to have analyzed the Stuxnet samples, the malware started operations as early as 2005, five years before its uncovering. Furthermore, the malware made use of eight exploits, for of them being zero-day exploits. While it is not unheard of that nation-state actors, and even cybercriminals, make use of zero-days in order to achieve the goal of their offensive campaign, the usage of four zero-days in one piece of malware is unprecedented and hints towards the high sophistication of the threat actor. The malware also introduces a user mode and kernel

mode rootkit that is responsible for “hiding” its malicious code from the eyes of the victim. Kernel mode rootkits are particularly challenging to program due to several factors, including their complexity, the need for in-depth system knowledge, and the potential for catastrophic consequences if errors are made. These rootkits operate at the lowest level of the operating system, directly interacting with the system's kernel, which demands an intricate understanding of the internal workings and architecture of the targeted platform. Additionally, errors in kernel mode rootkit development can result in severe system instability, crashes, or even irreversible damage to the targeted system, making the margin for error extremely narrow and thus highlighting the high sophistication of the adversary. Furthermore, unlike most malware that targets Windows, Linux or Internet of Things (IoT) devices, Stuxnet was on the hunt for specific programmable logic controllers (PLC) manufactured by the German company Siemens. Not only that, but the malware was searching for specific versions of that PLC: S7-315 and S7-417 (Zetter, 2014, chap. 10). This fact, however, bears the question of how that specific information was obtained. The intel had to come from an inside source that knew exactly what components were used in the Iranian centrifuges. Furthermore, complex malicious code such as Stuxnet’s needs to be tested rigorously before “shipping” it to the target. It is alleged that the testing of Stuxnet was conducted with Libyan centrifuges from their own nuclear program the United States managed to shut down successfully (Langner, 2017).

Figure 9: United States vs Iran Cyber Confrontation



According to the contingent deterrence model, the attack carried out, allegedly by the NSA and Israel's Mossad, ranks higher than the cyber espionage attacks conducted by China against the United States, leaving Iran with fewer options for retaliation and higher in their possible chance for escalation. One might assume that Iran might retaliate by attacking Israel through their connections to the Hamas organization, supporting terror attacks against foreign personnel in the region, or taking the route of economic sanctions and closing the Strait of Hormuz, especially considering that Iran ranks significantly lower in cyber warfare capabilities compared to China, and thus, does not possess the means retaliating through cyber.

However, Iran not only did not take the route of economic sanctions but used smaller cyber "rogue" groups in order to carry out retaliation attacks. Under the codename "Operation Ababil" the Iranian government contracted a group called "Cyber fighters of Izz Ad-Din Al Qassam" in order to conduct denial of service attacks against American financial institutions like Bank of America, JPMorgen Chase, Walls Fargo, Capital One and others. The group responsible for the attack (QASSAMCYBERFIGHTERS, 2012) did so, citing a "sacrilegious movie insulting all the religions not only Islam." While denial of service attacks are not uncommon and can

even be conducted by individuals with software available on the internet, the attacks against American banks were hit with traffic that was around sixty times higher than typical attacks (Gonsalves, 2012).

Similar to the Chinese cyberespionage case, the United States reacted to the hacks on private American entities with an indictment against seven Iranians who were hacking on behalf of the Islamic Revolutionary Guard Corps, accusing them of attacking forty-six US financial companies. The attacks disabled bank websites prevented customers from accessing their accounts and collectively cost the banks tens of millions of dollars in remediation costs (Department of Justice, 2016).

However, rather than attacking the United States directly and risking an escalation the Iranian government decided to flex its cyber weapons against Saudi Arabia, demonstrating the growing capabilities of Iranian cyber forces and their potential to use such attacks as a deterrent against the United States and its allies. The attacks, which utilized the notorious Shamoon malware, targeted two major energy companies in the Persian Gulf region, disrupting their operations and causing considerable damage to their computer systems. Saudi Aramco, the world's largest oil company, and RasGas, a leading liquefied natural gas (LNG) producer, both fell victim to the Shamoon malware, which wiped data from thousands of computers and replaced it with an image of a burning American flag. The scale and sophistication of the attacks underscored the evolving nature of Iranian cyberwarfare capabilities, which had previously been seen as relatively limited in comparison to other state-sponsored cyber actors. The timing and targets of the Shamoon attacks are indicative of Iran's strategic intent in cyberspace. The attacks on Saudi Aramco and RasGas occurred amidst rising geopolitical tensions in the Persian Gulf, including the ongoing conflict in Syria and concerns over Iran's nuclear program. By targeting these critical energy infrastructure companies, Iran

sought to demonstrate its ability to retaliate against economic sanctions and military threats from the United States and its regional allies. Moreover, the use of the Shamoon malware in these attacks served as a potent symbol of Iran's growing cyber prowess. The malware, which is believed to have been developed by Iranian state-sponsored hackers, is notable for its capacity to evade detection and spread rapidly through networks, causing significant disruption and damage in the process. The successful deployment of Shamoon in the attacks against Saudi Aramco and RasGas served as a stark warning to the United States and its allies of Iran's ability to retaliate in cyberspace.

In this context, the Shamoon attacks can be seen as an Iranian effort to establish deterrence against the United States and its regional partners. By demonstrating its capability to inflict substantial harm on critical infrastructure targets, Iran sought to signal its resolve to defend its interests in the face of external pressure. The attacks also served as a message to the international community that Iran's cyber capabilities were not to be underestimated, potentially discouraging further aggression against the Islamic Republic.

While not attributable to the escalation of the cyber conflict between the United States and Iran, the United States has shown that they are willing to make use of kinetic force by assassinating Qasem Soleimani, an Iranian major general, in 2020 near Baghdad.

The comparative analysis of the Stuxnet attack and Iran's subsequent response elucidates a stark divergence from the Chinese cyberespionage incidents, necessitating a deeper examination of the underlying factors and strategic implications. It is imperative to acknowledge that the Stuxnet malware exhibited a significantly more destructive nature, characterized by a highly sophisticated and targeted approach. Moreover, its potential for lethal consequences, such as the disruption of critical infrastructure, renders Stuxnet a conceivable "red" cyberattack within the context

of the contingent deterrence model. Iran's subsequent reaction, however, presents a rather anomalous case that invites further scholarly inquiry. Effective deterrence theory dictates that a counterstrike should possess an equal or at least commensurate magnitude in order to convey a powerful message of strength and resolve. Nonetheless, the Iranian denial-of-service (DoS) attacks appeared relatively feeble, targeting private organizations rather than the U.S. government directly. While the assault on critical financial institutions is undeniably disruptive and inconvenient, the inflicted damage is neither acute nor enduring, thereby limiting its long-term strategic value.

Furthermore, the choice to target private institutions as opposed to well-secured government networks underscores Iran's nascent cyber capabilities at the time. This strategic decision highlights the inherent limitations of Iran's cyber arsenal, as well as their recognition of the vastly superior cyber defenses possessed by the United States. Although Iran could have opted for kinetic force against United States' personnel in Iraq or Afghanistan, or even assailed Israeli targets as a means of showcasing their military prowess and regional influence, they refrained from such actions. The closure of the Strait of Hormuz, a critical global chokepoint for oil transportation, also appeared to be dismissed as a viable option, perhaps due to the potential for severe international repercussions and economic consequences. Instead, the Iranians elected to retaliate by attacking their regional adversary, Saudi Arabia, and impairing the nation's oil industry through the deployment of pernicious wiper malware. The rationale underlying this decision is rather transparent and merits further exploration. Although Saudi Arabia maintains close ties with the United States, the nation does not boast the same level of cyber prowess, with their capabilities being on par with or even inferior to those of Iran. This strategic calculus enabled Iran to exploit a more vulnerable target without directly confronting the United States. Furthermore, the wiper

malware utilized against Saudi Arabia was not equivalent to the DoS attacks against the U.S., representing a clear distinction in the severity and long-term impact of the retaliatory measures.

While DoS attacks endeavor to incapacitate a website or network temporarily, rectification is generally swift, and the overall consequences are limited in scope. In contrast, wiper malware is engineered to annihilate data or render a computer entirely inoperable, leading to more significant disruptions and potential long-term damage. Had Iran pursued such a course against United States institutions, the Iranian government would have undoubtedly found itself at a considerable disadvantage, potentially escalating the conflict and inviting even more devastating countermeasures. Conversely, targeting a United States' ally with destructive malware still conveys a discernible message of defiance and resolve, albeit in a more indirect and measured manner. Drawing from this case, it can be inferred that states cognizant of their cyber inadequacies vis-à-vis a formidable adversary may resort to "deterrence by proxy," employing third-party actors to execute attacks on their behalf. This strategy enables weaker states to project power and influence without directly provoking a more powerful adversary. Furthermore, this case demonstrates that the target of a retaliatory strike need not be the initial aggressor, broadening the scope of potential targets and complicating strategic calculations. A rational actor, fully aware of their subordinate position on the global stage relative to the aggressor, would be better served targeting another rival state, albeit one with significant ties to the initial aggressor. This approach allows the weaker state to demonstrate its capabilities and send a message without incurring the wrath of the primary adversary. As evidenced by the Iranian attacks on Saudi Arabian oil companies, this strategy can be employed with relative success. By selecting a target that is both geographically and politically relevant, the retaliating state is able to make a bold statement while simultaneously avoiding a direct confrontation with

the more powerful adversary. In this particular case, Iran managed to inflict considerable damage on the Saudi Arabian oil industry, thereby sending a clear message to the United States and its regional allies.

In conclusion, the examination of the Stuxnet attack and Iran's subsequent response sheds light on the intricacies and nuances of statecraft in the cyber domain. The divergent nature of this case from Chinese cyberespionage incidents emphasizes the need for a comprehensive understanding of the various strategies employed by states in the cyber arena. Moreover, it highlights the importance of considering the broader geopolitical context when assessing cyber conflicts, as well as the potential for deterrence by proxy and the targeting of third-party actors. As cyber capabilities continue to evolve and proliferate, understanding the motivations and strategies of state actors in this domain will become increasingly critical to maintaining global stability and security.

7. Conclusion

In the realm of cyber warfare, understanding and addressing the challenges of attribution is not merely a technical hurdle. Rather, it's an intricate puzzle that intertwines technology, law, diplomacy, and geopolitics. When talking about attribution, scholars and policy makers not only deal with the 'who' of the attack but also the 'why,' 'how,' and 'when.' To tackle this, a comprehensive approach needs to be multidimensional, focusing not just on the technological aspects but also on understanding the motive behind the attack, the modus operandi used, and the timing of the operation. This approach allowed this research to discern patterns and behaviors that can guide the investigation towards the true perpetrators, bringing an investigation closer to the goal of effective deterrence.

The study further emphasizes the value of frameworks such as the Q Model and the MICTIC framework. When employed in tandem, these frameworks serve as powerful tools that provide us with a methodical and robust approach to the analysis of cyber incidents. The Q Model, deeply rooted in the field of political science, offers an opportunity to view cyberattacks through the lens of international relations, enabling research to decipher the possible motivations behind the attack. On the other hand, the MICTIC framework offers a more technical perspective, focusing on the means employed to execute the attack, thereby allowing to identify the unique signatures that the attackers might have left behind.

But technology and frameworks have limitations. The study recognizes that human expertise plays an equally significant role in the process of attribution. Cybersecurity companies, due to their direct involvement in the cyber landscape, possess a wealth of real-time data and experiences. This firsthand knowledge and understanding, when amalgamated with academic research and political insights, can drastically improve the accuracy of attribution, thereby enhancing deterrence capabilities. The role of international

alliances and cooperation in cyberspace is yet another cornerstone that needs to be emphasizes. As cyberattacks continue to blur the traditional boundaries of conflict, it becomes even more critical to establish international norms and rules that govern cyber warfare. An internationally agreed-upon set of norms not only sets a precedent for what constitutes a cyberattack but also outlines the appropriate response measures, thereby adding another layer of deterrence. An international approach to defining these norms can also bring about a mutual understanding and collective action against the shared threat of cyberattacks.

Delving into the real-world examples of state responses to cyber threats, the study presents two intriguing cases – the United States' response to Chinese cyber espionage and Iran's reaction to a cyber-first-strike against its nuclear program. The contrasting strategies employed by these nations underline the notion that there is no one-size-fits-all approach to deterring cyber threats. Instead, each state, depending on its geopolitical standing, technical capabilities, and the nature of its relationships with other states, may employ a different strategy to deter cyberattacks.

This study serves as a testament to the fact that effective deterrence in cyberspace is not the responsibility of a single actor but a collective effort. In this digital age, where the lines between physical and cyber conflicts are becoming increasingly blurred, it is imperative that governments, cybersecurity companies, academic institutions, and the public work hand in hand. Each stakeholder brings something unique to the table – governments with their ability to enact laws and policies, cybersecurity companies with their technical expertise and real-time data, academic institutions with their research capabilities and peer-reviewed knowledge, and the public with their sentiment and support.

In conclusion, addressing the challenges of cyber warfare requires a holistic approach, combining technological advancements, political insights, academic research, and public sentiment. The

study calls for unity, cooperation, and collective action against the invisible enemy in the digital battlefield. This study's findings reiterate the importance of addressing attribution in cyber warfare, which is fundamental to ensuring effective deterrence. It urges further development and adaptation of methods that enhance attribution accuracy, bringing the cyber realm closer to established conflict and deterrence paradigms. However, it must be noted that such endeavors are intricately complex, requiring harmonization between technological advancements, data interpretation, and geopolitical insights.

Analyzing specific instances of state reactions to cyber threats, the study lays bare the intricacies and subtleties of cyber warfare. The United States' calibrated response to Chinese cyber espionage and Iran's recourse to proxy retaliation against cyber aggression underscores the necessity of tailored, context-specific deterrence strategies. These strategies are contingent on several factors such as the state's geopolitical standing, technical prowess, nature of its relationships with other states, and its available alternatives for retaliation. In examining the diverse responses, this study introduces a crucial variable – the concept of 'deterrence by proxy.' This is an avenue that requires extensive exploration and analysis in future research. A better understanding of this concept can potentially broaden the perspectives on state behavior in the cyber warfare landscape and lead to more refined strategies for cyber deterrence. The significance of a concerted, multilateral approach to addressing cyber threats is underlined in this study. International cooperation, in the form of global norms and rules governing cyber warfare, can provide a sense of mutual security and deterrence. This collective front against cyber threats is integral to maintaining global cyber peace. The role of public sentiment and national unity is another crucial aspect this study brings into focus. Ensuring transparency about cyber threats and government responses can foster a sense of shared responsibility among citizens. This human

element, often neglected in the technocentric discussions of cyber warfare, can enhance deterrence efforts and build a resilient national front against cyber threats.

To summarize, this study presents a comprehensive exploration of the multi-dimensional challenges of cyber warfare. It recognizes the need for diverse stakeholders to come together, each contributing their unique insights and expertise, to create effective cyber deterrence strategies. It calls for enhanced accuracy in attribution, more refined deterrence strategies, international collaboration, and engagement of public sentiment for a more robust defense against cyber threats. The battle in the cyber realm is evolving and complex, but armed with these insights, we stand a better chance of safeguarding nations' digital future. By acknowledging these complexities and intricacies, academia and policymakers can embark on a more informed journey toward mitigating cyber threats and securing our digital environments. The path towards a resilient and secure cyber ecosystem is not easy but armed with these findings, this new terrain can be navigated more efficiently.

8. Bibliography

Alireza Jafarzadeh, "Remarks by Alireza Jafarzadeh on New Information on Top Secret Projects of the Iranian Regime's Nuclear Program," Iran Watch, accessed April 12, 2023, https://www.iranwatch.org/library/ncri-new-information-top-secret-nuclear-projects-8-14-02.

Baliga, Sandeep, Ethan Bueno de Mesquita, and Alexander Wolitzky. "Deterrence with Imperfect Attribution." *American Political Science Review* 114, (2020): 1155-1178.

Broadcom, "Stuxnet 0.5: The Missing Link," Symantec, accessed April 12, 2023, https://docs.broadcom.com/doc/stuxnet-missing-link-13-en.

Buchanan, Ben. "Cyber Deterrence Isn't MAD; It's Mosaic." *Georgetown Journal of International Affairs*, (2014): 130-140.

Cimpanu, Catalin. "Windows 10, iOS 15, Ubuntu, Chrome fall at China's Tianfu hacking contest." The Record. November 15, 2021. https://therecord.media/windows-10-ios-15-ubuntu-chrome-fall-at-chinas-tianfu-hacking-contest/.

Clarke, Richard. "Obama's Challenge in Cyberspace." HuffPost. Last modified May 25, 2011. https://www.huffpost.com/entry/obamas-challenge-in-cyber_b_199926.

Crowdstrike. "Hat-tribution to PLA Unit 61486." Last modified June 2014. http://contagio.deependresearch.org/APT/China/APT1_Comm

entCrew_CommentPanda_PLAUnit61398_TG8223/Reading/2014_06_Crowdstrike_Hat-tribution%20to%20PLA%20Unit%2061486%20%C2%BB.pdf.

Cyber Project. "National Cyber Power Index 2022." Belfer Center for Science and International Affairs, Harvard Kennedy School. September 22, 2022. https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.

Deccan Herald. "China rejects US hacking allegations." February 20, 2013. Accessed March 25, 2023. https://www.deccanherald.com/content/313639/china-rejects-us-hacking-allegations.html.

Department of Justice. "Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies." Office of Public Affairs, July 23, 2018. https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading.

Department of Justice. "Chinese National Charged for Stealing Source Code from Former Employer with Intent to Benefit Chinese Government." Office of Public Affairs. June 14, 2016. https://www.justice.gov/opa/pr/chinese-national-charged-stealing-source-code-former-employer-intent-benefit-chinese.

Department of Justice. "FBI Employee Pleads Guilty to Acting in the United States as an Agent of the Chinese Government." Office of Public Affairs. August 1, 2016.

https://www.justice.gov/opa/pr/fbi-employee-pleads-guilty-acting-united-states-agent-chinese-government.

Department of Justice. "Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities." Office of Public Affairs. Accessed April 12, 2023. https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated.

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

DeSombre, Winnona. "Testimony before the U.S.-China Economic and Security Review Commission: Hearing on 'China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States.'" February 17, 2022. https://www.uscc.gov/sites/default/files/2022-02/Winnona_DeSombre_Testimony.pdf.

DigiChina. "Lexicon: 网络强国 Wǎngluò Qiángguó." Stanford University. Last modified September 10, 2018. https://digichina.stanford.edu/work/lexicon-%E7%BD%91%E7%BB%9C%E5%BC%BA%E5%9B%BD-wangluo-qiangguo/.

DigiChina. "Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference." New America. Last modified May 31, 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/.

FireEye. "Red Line Drawn: China Recalculates Its Use of Cyber Espionage." Accessed March 25, 2023. http://web.archive.org/web/20170714005607/https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

Fischerkeller, Michael P., and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis* 61, no. 3 (2017): 381-393.

Fisher, Dennis. "Spear Phishing Campaigns Use Fake Mandiant APT1 Report as Lure." Threatpost. Last modified February 21, 2013. https://threatpost.com/spear-phishing-campaigns-use-fake-mandiant-apt1-report-lure-022113/77552/.

Fraunhofer FKIE. "WebC2-Table." Malpedia. Accessed March 25, 2023. https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_table.

Gertz, Bill. "Chinese Military Creates High-Level Cyber Intelligence Center." Free Beacon. June 1, 2016. https://freebeacon.com/national-security/chinese-military-creates-high-level-cyber-intelligence-center/.

Gonsalves, Antone. "Bank attackers more sophisticated than typical hacktivists, expert says." CSO Online. Accessed April 12, 2023. https://www.csoonline.com/article/2132319/bank-attackers-more-sophisticated-than-typical-hacktivists--expert-says.html.

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102-135.

Gourley, Bob. "Towards a Cyber Deterrent." (May 29, 2008), SSRN, https://ssrn.com/abstract=1542565.

Gross, Grant. "Hackers break into Pentagon's fighter jet project." Network World. Last modified April 21, 2009. https://www.networkworld.com/article/2267807/hackers-break-into-pentagon-s-fighter-jet-project.html.

H.R.5576 - 115th Congress (2017-2018): Cyber Deterrence and Response Act of 2018. Congress.gov. Accessed March 30, 2023. https://www.congress.gov/bill/115th-congress/house-bill/5576/text.

International Energy Agency. "THE 10TH FIVE-YEAR PLAN FOR ECONOMIC AND SOCIAL DEVELOPMENT OF THE PEOPLE'S REPUBLIC OF CHINA (2001-2005)." Accessed March 25, 2023. https://www.iea.org/policies/1736-the-10th-five-year-plan-for-economic-and-social-development-of-the-peoples-republic-of-china-2001-2005.

Jervis, Robert. "Deterrence and Perception." International Security 7, no. 3 (1982-1983): 3-30.

Katz, Yaakov, and Amir Bohbot. *The Weapon Wizards: How Israel Became a High-Tech Military Superpower*. New York: St. Martin's Press, 2017. Chap. 7, Kindle.

Kesan, Jay P., and Carol M. Hayes. "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace." *Harvard Journal of Law & Technology* 25, no. 2 (2012): 431-498.

Langner, Ralph. "STUXNET UND DIE FOLGEN: Was die Schöpfer von Stuxnet erreichen wollten, was sie erreicht haben, und was das für uns alle bedeutet." Accessed April 12, 2023. https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf.

Lewis, James Andrew. "The 'Korean' Cyber Attacks and Their Implications for Cyber Conflict," Center for Strategic and International Studies, October 2009, https://www.csis.org/analysis/korean-cyber-attacks-and-their-implications-cyber-conflict.

Libicki, Martin C. "Cyberdeterrence and Cyberwar," (Santa Monica, CA: RAND Corporation, 2009), https://www.rand.org/pubs/monographs/MG877.html.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365-404.

Liptak, Kevin. "White House readies cyber sanctions against China ahead of state visit." CNN. August 31, 2015. https://edition.cnn.com/2015/08/31/politics/china-sanctions-cybersecurity-president-obama/index.html.

LunaSec. "Log4Shell: RCE 0-day exploit found in log4j, a popular Java logging package." Last modified December 9, 2021. https://www.lunasec.io/docs/blog/log4j-zero-day/.

Mallick, Major General PK. "China's Developing Cyber Warfare Capabilities." *Centre for Land Warfare Studies, Manekshaw* Paper No. 323, 2022. https://indianstrategicknowledgeonline.com/web/IB-323_China%E2%80%99s-Developing-Cyber-Warfare-Capabilities.pdf

Mandiant. "APT1 Exposing One of China's Cyber Espionage Units." Accessed March 25, 2023. https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units.

Mazarr, Michael J. "Understanding Deterrence." RAND Corporation, 2018, https://www.rand.org/pubs/perspectives/PE295.html.

McKenzie, Timothy M. "Is Cyber Deterrence Possible?" Maxwell Air Force Base, Alabama: Air University Press, Air Force Research Institute. https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF.

NATO. "Cyber defence," North Atlantic Treaty Organization, last modified June 28, 2018, https://www.nato.int/cps/en/natohq/topics_78170.htm.

O'Neill, Patrick Howell. "How China turned a prize-winning iPhone hack against the Uyghurs." MIT Technology Review. May 6, 2021.

https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/.

Phys.org. "Cybersecurity starts at home and in the office." Last modified October 1, 2009. https://phys.org/news/2009-10-cybersecurity-home-office.html.

QASSAMCYBERFIGHTERS. "Bank of America and New York Stock Exchange under attack unt." Pastebin. Accessed April 12, 2023. https://pastebin.com/mCHia4W5.

Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1-2 (2015): 4-37.

Schelling, Thomas C. *Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1960.

Schutte, Sebastian. "Cooperation beats Deterrence in Cyberwar" Peace Economics, *Peace Science, and Public Policy* 18, no. 3 (2012): 1219-1240.

Signorino, Curtis S., and Ahmer Tarar. "A Unified Theory and Test of Extended Immediate Deterrence," *American Journal of Political Science* 50, no. 3 (2003): 586-605.

Snyder, Glenn H. *Deterrence by Denial and Punishment*. Princeton, N.J.: Woodrow Wilson school of Public and International Affairs, 1959.

Steffens, Timo. *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage*. Cham, Switzerland: Springer International Publishing, 2020.

Stokes, Mark A., Jenny Lin, and L.C. Russell Hsiao. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." Project 2049 Institute. May 2011. https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf, p.8.

The White House, Office of the Press Secretary. "FACT SHEET: President Xi Jinping's State Visit to the United States." September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-State-visit-united-States.

The White House. "International Strategy for Cyberspace." May 2011. Accessed March 25, 2023. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, p. 14.

The White House. "The National Strategy to Secure Cyberspace." February 2003. George W. Bush White House Archives. https://georgewbush-whitehouse.archives.gov/pcipb/.

Townsend, Kevin. "Chinese Government Punishes Alibaba for Not Telling It First About Log4Shell Flaw: Report." SecurityWeek. December 22, 2021. https://www.securityweek.com/chinese-government-punishes-alibaba-not-telling-it-first-about-log4shell-flaw-report/.

U.S. Department of Justice. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." Last

modified May 19, 2014. https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and.

U.S.-China Economic and Security Review Commission. "Hearing on 'China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States'." Accessed March 30, 2023. https://www.uscc.gov/hearings/chinas-cyber-capabilities-warfare-espionage-and-implications-united-states.

United States Cyber Command. "Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority," (April 2018), National Security Archive, https://nsarchive.gwu.edu/sites/default/files/documents/4421219/United-States-Cyber-Command-Achieve-and-Maintain.pdf.

USNI News. "Document: China's Military Strategy." May 26, 2015. https://news.usni.org/2015/05/26/document-chinas-military-strategy.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown, 2014. Chap. 10, Kindle.

국문 요약

사이버 전쟁의 출현은 정책 입안자들과 정치학 전문가들 모두에게 복잡한 도전을 제시한다. 이 새로운 전장에서, 전통적인 억제 방법은 그렇게 효과적이지 않을 수 있다. 이 석사 논문은 사이버 보안과 정치학 모두의 통찰력을 결합하여 사이버 공격을 귀속시키는 과정을 개선하기 위한 새로운 접근법을 제공한다. 이 논문은 사이버보안 백서와 정치학 개념을 융합함으로써 이러한 사이버 공격의 배후에 있는 원동력과 의도에 대한 더 나은 이해를 달성할 수 있다고 주장한다. 이론과 실제 응용을 연결하기 위해, 이 논문은 사이버 공격의 두 가지 구체적인 사례 연구를 검토한다. 이를 통해 내부 정치, 글로벌 규범, 전략 문화 등 디지털 영역에서 국가 행동에 영향을 미치는 다양한 요인을 분석한다. 이러한 사례 연구의 교훈을 적용함으로써, 본 논문은 보다 전체론적인 사이버 공간 억제 전략이 어떻게 만들어질 수 있는지를 보여준다. 이 연구는 사이버 전쟁의 독특한 과제를 해결하기 위한 학제간 협력과 혁신적인 해결책의 가치를 강조함으로써 사이버 억제에 대한 지속적인 논의에 기여한다. 또한 사이버 영역의 억제력이 개념화되는 방식을 바꾸는 것을 목표로 하는 "컨틴던트 억제력"이라는 새로운 개념을 소개한다. 실제 사건을 연구함으로써, 이 연구는 정책을 형성하고 사이버 공격의 배후에 있는 행위자들을 더 높은 정확성과 자신감으로 정확히 찾아내는 능력을 향상시키는 데 도움이 될 수 있는 실용적인 통찰력을 제공한다.

키워드: 사이버 전쟁, 억지이론, 귀속, 미국, 중국, 이란