FROM THE SHADOWS TO THE FRONT PAGE: STATE USE OF PROXIES FOR CYBER OPERATIONS

A THESIS

SUBMITTED TO THE

INTERSCHOOL HONORS PROGRAM IN INTERNATIONAL SECURITY STUDIES

Center for International Security and Cooperation

Freeman Spogli Institute for International Studies

STANFORD UNIVERSITY

By:

Samantha V. Feuer

May 2020

Advisors:

Dr. Amy Zegart
&
Professor Andrew Grotto

Abstract

The cyber threat environment is increasingly complex due to the proliferation of capabilities and diversity of threat actors. This thesis explores the growth of non-state entities executing cyber operations against foreign targets on behalf of Russia, China, North Korea, and Iran, and why these states elect to use them. These "cyber proxies" further obscure the environment and are utilized to conduct significant cyber-attacks, exploitations, and influence operations. Furthermore, they pose several risks to sponsoring states. Through the delegation of authority from centrally controlled government agents to non-state actors, the likelihood of information asymmetries and failures increases. I propose a framework containing four hypotheses: cyber proxies offer economic cost savings, enhanced plausible deniability benefits, greater access to skills and specializations, and finally those states that can credibly threaten cyber proxy misbehavior will be more likely to use them. Through analyzing a wide array of data sources including US government reports, statements, research from industry, think tank analyses, and notable journals, I find that the use of cyber proxies is widespread and converging among all these states. I ultimately conclude that economic costs and skills and specializations may motivate proxy use. However, the evidence does not suggest that these proxies provide enhanced plausible deniability benefits compared to government agents. Furthermore, these states all have larger degrees of internal versus external punitive power. It indicates that they may select cyber proxies within their territories to credibly threaten them for failures or mission creep, thus reducing risks. This work offers an overview of cyber capabilities within these four states and their use of cyber proxies, providing preliminary findings to suggest why they adopted cyber proxy strategies. During this period of global uncertainty, much of our everyday lives have been forced online. It is even more critical to protect our infrastructure from cyber threat actors and increase awareness of the source of intrusions within our networks. As data in this field improves, this thesis hopes to serve as a framework for future researchers to test, with more certainty, the causal links between these explanations and the use of cyber proxies within these four states.

Acknowledgments

I am immensely grateful to all those who have supported me throughout this journey. Whilst I cannot name everyone within just one page, there are a few individuals that deserve a special mention.

In particular, I want to express my gratitude to my two thesis advisors Dr. Amy Zegart and Professor Andrew Grotto for their unwavering care and guidance. It is their constant mentorship throughout my academic career that inspired me to undertake this challenge. An early engagement with Dr. Zegart in my freshman year introduced me to the area of international security studies and prompted to pursue topics within this fascinating field. Our weekly meetings during this project were instrumental in streamlining my thoughts and analysis. Professor Grotto was a driving force in my interest in the intersection of cybersecurity and national security. His assistance not only encouraged me to examine the topic discussed within this thesis, but also strengthened my analytical rigor and clarity of thought. I cannot fully find the words to express my gratitude to them.

Dr. Ewing provided helpful feedback on various drafts of this thesis. His instruction forced me to closely examine my methods and sharpen my analysis. I also want to thank Dr. Asfandyar Mir for his responsiveness and encouragement during moments of doubt. Dr. Zegart, Dr. Ewing and Dr. Mir also led the wonderful CISAC Honors Seminar which provided both enriching group discussion and many unparalleled opportunities. I will greatly miss this element of my Thursday afternoons.

I also want to thank Ambassador Pifer, Dr. Felter and Marisa MacAskill for organizing and leading the unforgettable Honors College trip to Washington DC. It is not lost upon me the work that went into coordinating such a richly engaging ten days, nor the unique experiences contained within it.

To the CISAC cohort and friends, thank you for the discussions, words of wisdom, and loyalty. It is your support and encouragement that allows me to achieve my goals.

Lastly, to my parents for inspiring me to pursue feats that I never could have imagined. Despite our geographical distance over the last four years, their support and love has been unfaltering. I could not be where I am today without you.

Table of Contents

List of Figures

List of Abbreviations

APT Advanced Persistent Threat

CCP Communist Party of China

CI Critical Infrastructure

DDoS Distributed Denial of Service

DNC Democratic National Committee

DoJ US Department of Justice

GRB North Korean General Reconnaissance Bureau

GRU General Staff of the Armed Forces of the Russian Federation

GSD North Korean General Staff Department

IRA Internet Research Agency

IRGC Iranian Revolutionary Guard Corps

MOIS Iranian Ministry of Intelligence and Security

MSS Chinese Ministry of State Security

PLA People's Liberation Army

RAT Remote Access Trojan

SFA Security Force Assistance

TTPs Tactics, Techniques and Procedures

Chapter 1. Introduction

1.1 What 2016 Taught Us

2016 represented a turning point. For the first time, the US fell victim to a widespread and coordinated cyber operation to influence the Presidential election.[1] Subsequent reporting followed Special Counsel Robert Mueller and his efforts to bring those involved, including US officials, to justice. Of particular note was the Russian-attributed hack into the Democratic National Committee (DNC) by several General Staff of the Armed Forces of the Russian Federation (GRU) agents.[2] However, after the dust had settled, the presence of cyber-enabled influence campaigns upon major social media sites, entered mainstream commentary. A non-state entity by the moniker of the Internet Research Agency (IRA) became synonymous with a coordinated attempt to "sow discord in the U.S. political system" during the 2016 elections.[3] Estimates suggest that IRA content reached "126 million people on Facebook, at least 20 million users on Instagram, 1.4 million users on Twitter, and uploaded over 1,000 videos to YouTube."[4]

Whilst this event signified a pivotal moment in public understanding of the diverse cyber threats leveraged by adversarial states, cyber activity by non-state actors on

[1] Eric Lipton, David E. Sanger, and Scott Shane, 'The Perfect Weapon: How Russian Cyberpower Invaded the U.S.', *The New York Times*, 12 December 2016.
[2] Department of Justice, 'United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleskey Alesandrovich Potemkin, and Anatoliy Sergeyevich Kovalev, Defenandts.', United States District Court for the District of Colombia (July 2018),.
[3] 'Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements', *U.S. House of Representatives Permanent Select Committee on Intelligence*.
[4] Renee DiResta, Jonathan Albright, and Ben Johnson, 'The Tactics & Tropes of the Internet Research Agency', *New Knowledge*, 2019, 6.

behalf of state sponsors is not new and certainly not unique to Russia. Some of the most prolific nations in cyberspace also include China, Iran, and North Korea as detailed by every US Threat Intelligence Report since 2014. The current coronavirus pandemic is only highlighting this fact. Both the UK and the US released statements in May 2020 condemning cyber "attacks by state and non-state actors seeking to undermine the global response" to COVID-19.[5]

Cyberspace is unique in that nearly every industry is reliant upon digital infrastructure for its operations. In geophysical domains, such as air, land, and sea, it may be possible to circumscribe what is considered a militarized or state-initiated attack. However, cyber is not constricted in the same way. The weaponization and militarization of the domain by state actors infiltrates military and government targets, but also commercial and private sector industries in the pursuit of national interest goals.[6] Not only have the attack vectors multiplied, but also the threat actors. As noted by Joseph Nye, states will find the threat landscape "far more crowded and difficult to control" due to the low barriers to entry that the cyber domain presents.[7] He further argues that "non-state actors and small states can play significant roles at low levels of cost."[8] Tool sophistication is also no longer a method to rely upon when considering the differences between a nation-state and non-state attack. Before 2015, zero-day exploits[9] were considered the gold standard for state cyber forces and often signaled sophistication.

[5] 'UK Condemns Cyber Actors Seeking to Benefit from Global Coronavirus Pandemic', *Foreign & Commonwealth Office*, 5 May 2020.
[6] 'Cyber Threat Source Descriptions', *Cybersecurity & Infrastructure Security Agency*.
[7] Joseph S. Nye, 'Cyber Power' (Belfer Center for Science and International Affairs, 2010), 1.
[8] Nye, 4.
[9] Zero-day exploits are previously undiscovered software vulnerabilities that an attacker can use to infiltrate, disrupt or destroy systems and networks

However as stated by Rob Joyce, Senior Advisor to the Director NSA for Cyber Security Strategy, there are "so many more vectors that are easier, less risky and quite often more productive than going down that [use of zero-days] route."[10] Using technical sophistication to distinguish between non-state and state activity is not always effective.[11] The result of this proliferated capability is the expansion of non-state actors and states looking to utilize them - particularly Russia, China, Iran, and North Korea[12]- to conduct cyber operations on their behalf.

1.2 The Puzzle of delegating executory authority to non-state agents

Relationships between non-state and state entities present many risks. States must consider that non-state entities may not always have the same interests, thus resulting in misalignment. Divergent interests may involve prioritizing personal gain, such as financial benefit, over national security. Cyberspace is a constantly evolving environment, the challenges of consistent monitoring and restriction of these non-state actors represent significant costs to a state. If inadequately managed, failures can occur as actors stray from the expressed intent of nation-state direction or interest. Furthermore, all the states of focus have made considerable efforts to build up their respective cyber commands. Therefore, in the presence of risks and the ability to conduct cyber operations from central military commands, this thesis asks:

[10] Janus Rose, 'NSA's Hacker-in-Chief: We Don't Need Zero-Days To Get Inside Your Network', *Vice*, 29 January 2016.
[11] 'Orpheus Data Shows Downward Trend in Zero-Day Use in Nation-State Operations', *Orpheus*.
[12] Note: North Korea's distinction between non-state and state is very difficult to ascertain. Whilst, I am moderate in my assessment of North Korea's non-state activity throughout this thesis, there are some indications that non-state activity and reliance may occur.

Why do states use cyber proxies for conducting cyber operations against external targets?

1.3 Argument and Contribution

When the Pentagon announced cyberspace as a new operational domain in 2011 the rhetoric surrounding the pervasiveness of cyber operations by state and non-state actors increased.[13] Whilst a myriad of private cybersecurity companies have tracked state-sponsored actors and how these groups are utilized, there is less attention given to why these countries have chosen to rely upon them for cyber operations. The limited literature within this space focuses heavily upon the nature of these state-non-state relationships, with some attempts to understand the motivations behind the use of these non-state actors.[14] However, there have been fewer attempts to explore these reasons in the context of the activity we see today. It is difficult to structure conditions to limit the use of state-sponsored non-state actors in cyberspace without a robust understanding of why nations might elect to use them. This thesis builds upon frameworks developed within the virtual and non-virtual proxy literature and explores prevailing motivations for using cyber proxies across China, Russia, Iran, and North Korea. This thesis aims to explain why states use cyber proxies through qualitative evaluations of four hypotheses:

1. **Cost Savings Hypothesis:** Cyber proxies provide states with avenues through which to limit both the operational and ex-post retributive economic costs of cyber operations.

[13] David Alexander, 'Pentagon to Treat Cyberspace as "Operational Domain"', *Reuters*, 14 July 2011.
[14] See: Tim Maurer, 'Cyber Mercenaries'; Jamie Collier, 'Proxy Actors in the Cyber Domain'; Justin Key Canfil, 'Honing Cyber Attribution: A Framework for Assessing Foreign State Complicity'; Erica Borghard & Shawn Longergan, 'Can States Calculate the Risks for Using Cyber Proxies?'.

2. **Plausible Deniability Hypothesis:** States hope to obtain distance from cyber operations enacted upon adversarial states to avoid legal recourse and escalation. Cyber proxies allow states to adopt an arms-length approach in achieving national interest goals and therefore enhance the benefits attained from plausible deniability.
3. **Skills and Specialization Hypothesis:** Cyber proxies can conduct focused operations with skills that states may not be privy to due to bureaucratic constraints.
4. **Punitive Power Hypothesis:** States use cyber proxies when they possess the ability to pose credible threats for proxy misbehavior or failure - thus limiting principal-agent dilemmas.

1.4 Methodology

1.4.1 Methods and Sources

This thesis examines four explanations for cyber proxy use within China, Russia, Iran, and North Korea. I select these states because they represent the highest priority threat actors to the US within the cyber domain. The timeframe of interest was from 2010 to present day, and utilizes a within-case, process tracing approach of qualitative data sources to parse the hypotheses. I provide a constrained definition of cyber proxies to account for a multitude of uncertainties.

All these states appear to employ cyber proxies as defined in Chapter 2. I decided to select on the dependent variable (the existence of cyber proxies) to explicitly answer the question of why these countries use cyber proxies, noting that all are authoritarian

regimes. Other researchers may invoke a comparison approach by analyzing those that do use cyber proxies and those that don't. The reason I chose not to approach this question in this manner is due to data limitations and bias in reporting. I primarily have access to reporting that focuses explicitly on external threats to Western nations. To maintain secrecy around the intelligence communities and US CYBERCOM activity,[15] reporting of cyber operations conducted by the US is mostly handled by secondary sources, such as journalists, rather than official government statements. Selecting on the dependent variable prevents further bias entering into this project as it allows consistent examination of a variety of data sources that provide qualitative data across all these four states.

Another reason that I have chosen to select upon the dependent variable is that I am analyzing extreme cases where the impact of the cyber operation was enough to warrant inclusion within industry analysis, government statements, and US Department of Justice indictments (DoJ) or Department of Treasury sanctions. Many of the cyber proxies examined within this project are also labeled as Advanced Persistent Threat (APT) groups by industry. The definition of an APT is a threat actor that "gains and maintains unauthorized access to the targeted network and remains undetected for a significant period,"[16] with the potential to pose destructive impacts. This definition exemplifies the extreme nature of these actors in that they pose a "significant" departure from the norm. Furthermore, these states are widely considered to be the most aggressive towards the US. These aspects demonstrate that these cases are extreme. William Starbuck posits that "studies of exceptional performance are inevitably concerned with

[15] USCYBERCOM is the United States' Department of Defense agency tasked with cyber operations and activity.
[16] "What Is an Advanced Persistent Threat (APT)?," *CISCO*.

extreme cases, and to understand the requirements of exceptional cases, one must study extreme cases, not averages." An analysis of "extreme cases can expose overlooked cause factors and make one aware of the complexity of phenomena."[17] Throughout this thesis, I utilize previous explanations of proxy use and examine them with intensified attention to understand nuances that the prevailing literature may have ignored.

Before analyzing the hypotheses, I provide a synthesis of qualitative data sources to demonstrate trends within the cyber threat environment. I consult private industry evaluations, think tank analysis, and governmental agency reports to illustrate how these states built up their central cyber capabilities and integrated proxies into their cyber strategy. I provide a snapshot of how proxies are used today across all four countries, indicating key convergences but also the existence of both cyber proxies and centralized capability. In doing so, this chapter further prompts the question of why do states use cyber proxies.

I evaluate cost, plausible deniability, skills and specializations and state punitive power as motivations, relying upon limited open-source data to provide a framework with an initial exploration of China, Russia, Iran, and North Korea.

I assess both operational and economic punishment costs and explore whether cyber proxies can provide cost savings for states within these areas. My primary within-case was Russia because it represents the only country where a DoJ indictment/criminal complaints explicitly detailed the expenses of a cyber operation. I further this analysis through open-source data collection of private versus public sector salaries to determine the ability of Russia to augment its in-house cyber agents. I conduct a similar analysis

[17] William Starbuck, *The Production of Knowledge: The Challenge of Social Science Research* (New York: Oxford University Press, 2006), 149-150.

with China. To assess the threat of punitive economic costs in motivating cyber proxy use, I consider trends in sanctions for cyber operations conducted by foreign nationals/state entities. I utilize a dataset produced by the Foundation for Defense of Democracies that tracks the number of US sanctions enacted upon these four states between 2013-2020. In doing so, I consider whether using cyber proxies increases or reduces the risk of incurring punitive economic costs.

To assess plausible deniability as a motivator I explain whether it is truly attainable and whether utilizing cyber proxies enhances plausible deniability benefits. I approach this concept from an international audience standpoint, demonstrating whether proxies afford states reduced legal liability for cyber operations conducted on their behalf. I consult international agreements to demonstrate the lacking legal structures which promote conditions through which cyber proxies, and their state sponsors, can act with impunity. I continue this discussion by evaluating whether cyber proxies can enhance key plausible deniability benefits such as limiting conflict escalation. To do so, I utilized qualitative data from DoJ indictments and criminal complaints, and New York Times reports to collect a medium-N dataset of 28 cases of alleged cyber proxy activity within these four nations. I coded these cases as explicit or discrete. Discrete describes cases where there was mention of how the targets of the cyber operations could aid militaries or governments of another state. Explicit describes cases where the phrase "behalf of [insert state]" was used within the report or indictment. Through this, I track how many are indicted with a state sponsor explicitly mentioned to assess whether concepts of limited war are upheld.

To explore skills and specializations, I examine how bureaucratic structures may motivate the use of cyber proxies. I focused my analysis on Iran's state cyber entities and their interaction with non-state agents. I conduct a qualitative analysis of US think tank reports and industry analysis of Iran's cyber agencies. In doing so, I present a case for outsourcing in the presence of structural inefficiencies inherent within their state apparatus.

The last hypothesis is distinct in that rather than considering benefits as motivation, it assesses the ability of these states to control risks. Whilst, I consider this hypothesis independently, it is clear that alone it is not sufficient to motivate the use of cyber proxies. I evaluate the ability of these states to create deterrents to misalignment through their ability to wield credible punitive power, thus threatening cyber proxies should they misbehave. I elect to view the ability to control cyber proxies through the lens of coercive deterrence because such mechanisms are already established and, therefore, do not present additional effort or cost on behalf of the state. Additionally, through considering how credibly nations can threaten its citizens, we can infer to what extent cyber proxies would feel these threats and thus self-regulate their behavior to align with state wishes. I do this by developing a matrix of four sources of state punitive power; internal, external, formal, and informal. To assess formal, internal power I consult the World Justice Project 'Rule of Law Index' and supplement with an analysis on the use of travel bans within these countries to indicate the level of state interference within the criminal justice sector. Informal, internal power involved an analysis of extrajudicial systems that are publicly unacknowledged by the state, such as black jails and assassinations. To do so, I conduct a qualitative analysis of Freedom Rights Watch

reports, government statements, and news sources. Formal, external power was assessed through evaluating extradition efforts on behalf of these nations against the US. Using news sources I generate a small-N dataset of competing extradition cases between the US and Russia, concerning cyber operations to assess Russia's ability to threaten its cyber proxies beyond its borders. Lastly, I evaluate informal, external power through a qualitative cross-case analysis of assassinations conducted abroad, using news reports, official statements.

1.4.2 Limitations

As demonstrated above, I use an array of methods and data sources to explore my hypotheses. The reason for doing so lies in the severe data limitations inherent in the study of cyberspace and this topic in particular. Conclusively proving that an actor is, in fact, non-state is extremely difficult and subject to change. Therefore, whilst this thesis explores these hypotheses and arrives at some preliminary findings, the main contribution is a framework which future researchers, with better access to data, can utilize to answer the question more robustly. The issues within this project are:

1. The states under focus are authoritarian and some are incredibly closed regimes, thus access to information was difficult. North Korea and China for example proved particularly problematic .
2. The intersection of cybersecurity and national security is an extremely challenging field to penetrate, even in the US.
3. The lack of concrete data generates a number of uncertainties.

In the case of the lack of data, I used private cybersecurity company reports as primary sources as these firms usually are the first to publicly discover and continuously track

cyber threat actors. However, there is no systematic reporting standard among these firms, and much of their data is customer-provided. As a result the conclusions they draw can be slightly different. Even within one firm, methods can change year on year as intelligence and technical analysis improves. Another primary data source utilized was government reports and indictments. Although these documents are more systematic than private sector reports, secrecy and lag-time between incident and response distorts the reality of the cyber threat profile.

This project relies heavily on secondary sources, such as mainstream media sources, journals, think tank analyses. However, most of these are US-centric therefore introducing bias.

1.5 Scope

As mentioned in section 1.4.1, I use a very specific definition of cyber proxies that I define with more clarity in Chapter 2. The reason for doing so is that it allows focus on cases that are most puzzling because they entail the most risk. However, as a result, I cannot reasonably include US use of contractors or similar examples because it is not clear that these entities are entrusted with the degree of authority to execute that I layout within my definition. I also chose to select China, Russia, Iran, and North Korea for two main reasons:

1) They present the highest policy relevance and immediate threat.

2) They display similar regime types. Therefore, I can control for this variable, lowering the possibility of false positives or negatives.

1.6 Roadmap

Chapter 2 opens by defining two terms that will be used extensively throughout this thesis: cyber operations and cyber proxies. State use of non-state entities to achieve national interest goals is not a new phenomenon and exists both during wartime and peacetime. Therefore, I examine the richer literature on the use of physical proxies as a base to develop my hypotheses. I also combine this with the limited literature on cyber proxies, noticing some overlaps between motivations in the physical and virtual spaces. Subsequently, three key benefits of using cyber proxies and physical proxies emerge; costs, plausible deniability, and skills and specializations. However, these benefits are accompanied by several risks that are intensified when delegating to non-state entities.

Chapter 3 provides some necessary background to the buildup of cyber capabilities in China, Russia, Iran, and North Korea, demonstrating that central cyber units, commands, and bureaucratic organizations exist within all these countries and have benefitted from significant investment within the last ten years. I also detail the build-up of domestic cyber capabilities generally and the continuum between cybercriminal activity and cyber proxy use within some of these states.

Chapter 4 builds upon the explanations laid out by the literature and examines them, using a process-tracing approach within and across the cases of China, Russia, Iran, and North Korea. This chapter finds that operational costs could potentially motivate cyber proxy use despite the literature discussing the 'cheapness' of cyber operations. However, it does not find evidence to support ex-post economic retribution costs as a motivator. Much of the literature within this space cites that cyber proxies provide states

with plausible deniability.[18] However, an analysis of attribution, legal frameworks, and escalation risks in cyberspace suggest that there is no clear evidence that cyber proxies enhance plausible deniability benefit over state agents. Through an analysis of bureaucratic institutions, these states demonstrate a highly complex structure that is competitive and subject to change based upon political leadership. As such, cyber proxies may provide a method through which to sidestep the inefficiencies within these centralized entities. Lastly, I evaluate punitive power to demonstrate that states use cyber proxies when they can pose credible deterrent threats, discouraging misbehavior. Through an analysis of internal, external, formal, and informal sources of state punitive power, this section assesses that all these states possess strong internal punitive power. As a result, I conclude that states may predominantly employ cyber proxies within their territories to bring them under their umbrella of effective control.

Finally, Chapter 5 discusses the conclusions and implications of this work – both for policy and scholarship.

[18] See: Tim Mauer, 'Cyber Proxies and their Implications for Liberal Democracies', *The Washington Quarterly* 41, no. 2 (July 2018); Tim Maurer, 'Cyber Mercenaries', Joseph Nye, 'Cyber Power'; Erica Borghard and Shawn Lonergan, 'Can States Calculate the Risks of Using Cyber Proxies?

Chapter 2. Balancing Outsourcing Benefits and Principal-Agent Dilemmas

Cross-Domain Theories of State-Proxy Relationships

2.1 Why Now?

The state-centric model of international relations is being tested. Nation-states no longer have a monopoly over the threat environment. Non-state actors now have the capabilities to both defend and attack adversaries in foreign locations with increasing success. Today's world is populated by international organizations - both political and military – and private organizations with the ability to wield significant power and influence.[19] States themselves are not blind to this change. Even within the United States, the government is recognizing the challenges associated with the modern era and is increasing reliance upon non-state entities to solve them.[20] This thesis examines why states use cyber proxies for conducting cyber operations against external targets on their behalf.

Much of the focus on proxies has centered around the physical domain and still along the lines of state-centric conflicts. However, proxy actors have been "chronically under-analyzed" in the physical space let alone the virtual.[21] The nature of proxies is that their relationships, and sometimes their actions are usually secret,[22] leading to very few

[19] Nye, 'Cyber Power', 1.
[20] John R. Mills, 'What Ever Happened to the Front Company? Resurrecting Lost American National Security Tradecraft for an Asymmetric World', *Georgetown Journal of international Affairs*, International Engagement on Cyber III: State Building on a New Frontier(2013-14), 125-133, 127.
[21] Andrew Mumford, "Proxy Warfare and the Future of Conflict.", The RUSI Journal 158, no.2 (2013): 40-46, 40.
[22] Candace Rondeau, and David Sterman, 'Twenty-First Century Proxy Warfare', *New America,* 2019, 11.

empirical studies. Nonetheless, some key scholars within the space attempt to answer this very question, which I shall outline in subsequent sections.

Why is this important? Cyber-proxies exist at the confluence of three trends:

1) The **mounting dangers** that non-state actors pose in terms of asymmetric conflict are unclear and require new risk calculi when formulating a response.
2) **Rising great power competition** is prompting nations to find novel ways in which to achieve strategic aims without direct confrontation. Many countries throughout the world are known to be using proxies to achieve strategic goals outside of their physical boundaries. Whilst no direct acknowledgment of this has been made within cyberspace, there is reasonable evidence to believe such tactics will translate into the virtual space.
3) The **issue of cyber warfare** itself is becoming more and more common in international relations discussions. It is unclear how cyber warfare will be conducted in the future, but cyber conflict is increasingly recognized as an alternative or complement to kinetic conflict.[23]

As more proxies enter the cyber domain, the US must adopt more nimble responses through an understanding of the diverse nature of these threats. By allowing proxies to take on what is considered by the US as "inherently governmental functions," the threat landscape has expanded.[24] To successfully mitigate the threats posed by

[23] Herbert Lin, 'Escalation Dynamics and Conflict Termination in Cyberspace', *Strategic Studies Quarterly* 6, no. 3: CYBER SPECIAL EDITION (2012): 46–70, 53; Patrick Lin, Neil Rowe, and Fritz Allhoff, 'Is It Possible to Wage a Just Cyberwar?', *The Atlantic*, 5 June 2012.
[24] 'Policy and Procedures for Determining Workforce Mix', *Department of Defense*, no. Department of Defense Instruction 1100.22 (12 April 2010), 19.

adversarial states in the cyber domain, it is important to first understand the actors used to leverage these attacks, and why states elect to use them.

To answer this question, I first define cyber operations and cyber proxies, two terms that are used extensively throughout this thesis. Then I examine the richer literature detailing the benefits of using physical proxies and compare with the limited literature surrounding cyber proxies. Next I consider the drawbacks of using proxies both within the physical and virtual spaces.

2.2 Definitions

2.2.1 Cyber Operations

Within this project, I focus on cyber operations that threaten the national interests of the US and its allies. I borrow Herb Lin's definition of cyber offensives - "actions taken against an adversary's computer systems or networks that harm the adversary's interests."[25] The picture of the cyber threat landscape today and what actions can "harm the adversary's interests," extends beyond just actions defined within cyber offensives. Three types of operations are frequently examined:[26]

1) Cyber Network Exploitation (CNE)
2) Cyber Network Attack (CNA)
3) Cyber-enabled Influence Campaign

From the vantage point of the victim the lines between these operations are unclear. They can evolve across these three types. This thesis considers all of these categories within

[25] Lin, 'Escalation Dynamics and Conflict Termination in Cyberspace', 46.
[26] CNE refers to espionage and reconnaissance whilst CNA intends to "damage, disrupt or destroy". See: Kim, Zetter 'Hacker Lexicon: What are CNE and CNA?', *Wired*, July 6 2016.

the analysis to ascertain a full-spectrum view of cyber proxy use. Technical assets required for success in these operations vary significantly and therefore allows this thesis to comprehensively consider how specific scenarios warrant cyber proxy use over others. Even more pertinently, all of the operation types appear to be conducted by cyber proxies acting on behalf of China, Russia, Iran, and North Korea.

2.2.2 Cyber proxy

The existing literature on proxies contains some competing definitions. The word proxy, despite its use for many years, is still hard to define. The reason is that proxies are defined not by how they came to be as an organization, individual or rebel group, but rather how they are operationalized/weaponized for state use. Therefore proxies can have varying organizational structures, conduct many different operations, have varying relationships with the state, and follow multiple motivational paradigms. In the physical space, proxies are often defined as an "agreement between a state and a non-state group that involves the exchange of military resources in furtherance of a political objective",[27] between two, typically asymmetrically capable countries.[28]

There are some clear gaps in the literature on why states use proxies that are particular to cyberspace. Reasons for this are that cyber warfare between states is difficult to define as international law and norms have not caught up with the rapid inclusion of cyber into conflict spaces and because the term "cyber proxy" is relatively new and lacking in clear definition. As explained by Borghard and Lonergan, "it is difficult to

[27] Erica Borghard, and Shawn Lonergan, 'Can States Calculate the Risks of Using Cyber Proxies?', Foreign Policy Research Institute 60, no.3 (May 7, 2016): 395-416, 404.
[28] Erica Borghard, 'Friends with Benefits? Power and Influence in Proxy Warfare' (Colombia University, 2014), 17.

define these actors because they do not operate consistently under state control."[29] As laid out within Tim Mauer's *Cyber Mercenaries*, upon which much of this thesis is built, the nature of relationships between state and the cyber proxy can differ in degrees explicit direction.[30] Nonetheless, consistent across the literature is that a proxy is non-state, such that authority is delegated from outside of the formal governmental apparatus. Beyond this, scholars approach the topic from varying standpoints, utilizing the definitions of other state contractual relationships as a guide, as well as focusing on the underlying strategy of these relationships– such as target and motivation – to add definitional weight.

Using target and motivation as a method to define cyber proxies can be misleading. Borghard and Lonergan assess that physical and virtual military spaces differ because the line between national interest motivation and personal motivation is less transparent. For example, many have focused on attacks upon national critical infrastructure (CI) to assess state involvement.[31] Yet, due to the proliferation of capability, and weak defenses within the underlying systems of conventional CI, non-state actors can successfully target these sectors out of personal motivation.[32] Furthermore, the current conception of attacks on CI as the most damaging to society, and therefore indicative of state motivation, misrepresents the ability to exploit alternative threat vector to cause significant damage. As explained by Borghard and Lonergan:

---

[29] Borghard and Lonergan, 'Can States Calculate the Risks of Using Cyber Proxies? ', 396.
[30] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018).
[31] Borghard and Lonergan, 'Can States Calculate the Risks of Using Cyber Proxies? ', 398.
[32] For a more comprehensive review of the vulnerabilities of underlying CI systems consult Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (John Wiley & Sons Inc, 2019), 208.

Amazon is estimated to make roughly $1,996/second ... if an attack similar to that which occurred against Amazon.com in 2000 were to occur today, being down for 60 minutes could cost the company over $7 million in lost revenue."[33]

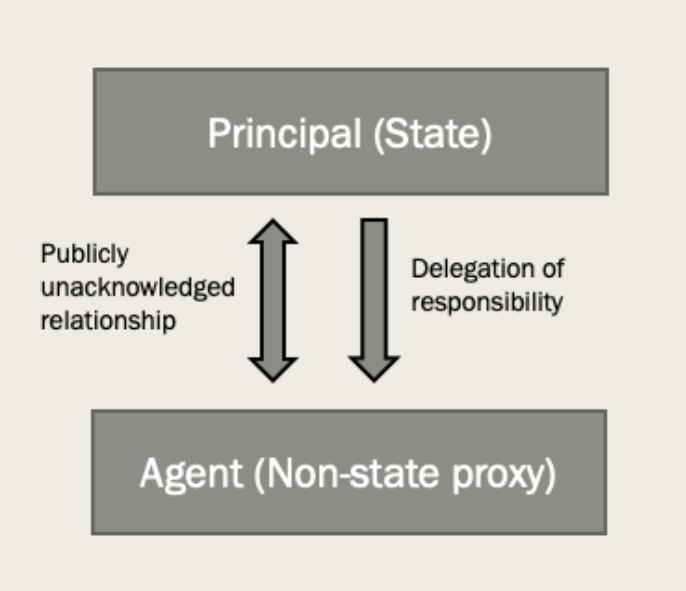
Large private sector companies are targets that could serve both personal financial motivation but also state economic advantage. Therefore, using targets or motivation as a delineating line does not adequately define what a cyber proxy is.

Nonetheless, any cyber proxy acting on behalf of a state must attempt to do so based on national interest goals. As stated by Tim Maurer, the decision of non-state actors to take up arms in defense of this communication could be both directly authorized, or non-state initiated and tolerated by the state.[34] He, therefore, defines cyber proxies as "intermediaries that conduct or directly contribute to an offensive cyber action that is enabled knowingly, whether actively or passively, by a beneficiary."[35] This definition encompasses a wide range of non-state actors but excludes those that only conduct activity for non-state purposes. I will further clarify this definition through the use of the principal-agent framework. The framework suggests a hierarchical relationship in which the principal sits atop the agent, thus making the agent reliant on the continuation of need by the principal. Within this thesis, the principal would be the state apparatus, including political leadership or national security agencies. Whilst the agent would constitute a non-state actor, for example a hacktivist or a private entity. Therefore, a cyber proxy would be a non-state entity that carries out cyber operations (as defined earlier) on behalf of the state. This thesis considers that the distinguishing factor between

[33] Borghard and Lonergan, 'Can States Calculate the Risks of Using Cyber Proxies? ', 401.
[34] Maurer, *Cyber Mercenaries: The State, Hackers, and Power.*
[35] Ibid*, 20.*

a cyber proxy and a state agent usually lies in the level of recognition by one another. (Figure 2.1)

Figure 2.1: Diagram of State-Proxy interaction Based on the Principal-Agent Framework



For example, a GRU agent indicted for his role in a hack and leak operation is recognized by the state due to his status as a GRU agent. However, a cyber proxy would not be. The relationship is also vice versa, where the cyber proxy should not acknowledge direct employment by the state. Direct employment does not, for example, include entities that pledge allegiance to political leadership.

Furthermore, cyber proxies do not include entities that may engage in software development or technical R&D for cyber operations. Rather, this thesis focuses on those that are delegated operation executory authority, whether "actively or passively."[36] It appears that the US differs in that it does not grant non-state actors executory authority that I define here, and relies on US CYBERCOM agents for pressing the 'proverbial red

[36] Maurer, *Cyber Mercenaries*, 20.

button' on its cyber operations.[37] Whereas, Russia, Iran, China, and North Korea all appear to purposefully diffuse power to non-state actors both under direct and indirect instruction.[38] My question is why certain nations would elect to use cyber proxies instead of relying on their respective cyber commands.

2.4 Why Do States Use Physical Proxies?

There is limited literature discussing cyber proxies. To counter this restriction, I consult the more expansive literature on the use of physical proxies to generate hypotheses. States have used physical proxies for multiple years, existing literature cites three primary reasons: Limiting costs – both physical and monetary, efficiency gains created through specialization, and plausible deniability.

2.4.1 Cost

A well-documented reason as to why states use proxies in the physical space centers around minimizing the costs associated with state-on-state conflict. There are two main costs that proxies help states avoid: economic and political.

The US is the world's strongest military power.[39] However, theories of asymmetric conflict explain that weaker countries can pose credible threats against strong nations, challenging realist theories of warfare.[40] Since the end of WWII major wars

[37] 'Policy and Procedures for Determining Workforce Mix', 19.
[38] Madison Creery, 'Hacker Militias or Cyber Command? The U.S. and Russian Institutionalization of Cyber Warfare', *Georgetown Security Studies Review*, 7 March 2019.
[39] '2020 Military Strength Ranking', *Global Firepower*, 2020.
[40] Ivan Arreguín-Toft, "How the Weak Win Wars: A Theory of Asymmetric Conflict," *International Security* 26, no. 1 (2001): 93–128.

diminished, indicating a preference for indirect confrontation and limited wars.[41] After the Cold War there was an increasing trend, at least domestically within the US, for retrenchment and "burden-sharing."[42] Additionally, direct confrontation within today's nuclear and technologically developed world, presents high consequences for escalatory action.

Economic Costs

Yaacov Bar-Siman-Tov underscores that using proxies within war "offers the possibility of achieving objectives more economically."[43] Proxies provide a cost-saving paradigm to states because direct confrontation incurs higher economic costs. This is both in the form of start-up costs and ex-post economic costs.

Start-up costs

Deploying national armies, even in peacetime, can incur significant economic costs.[44] Andrew Mumford argues that paramilitary corporations experienced a resurgence in the post-Cold War world due to a reduction in national armies and the transference of trained personnel to the private sector.[45] However, this push to reduce direct military expenditure does not mean that states ceased to pursue political influence in foreign territories and disengage from regional conflicts. As a result, the role of private military companies increased within both Western and non-Western nations. Clive Walker and

[41] John Mueller, "The Obsolescene of Major Wars," *Bulletin of Peace Proposals* 21, no. 3 (1990): 321–28.; Rondeaux and Sterman, 'Twenty-First Century Proxy Warfare', 16.
[42] Richard N. Haass, *War Of Necessity, War of Choice* (New York: Simon & Schuster, 2009), 86.
[43] Yaacov Bar-Siman-Tov, 'The Strategy of War by Proxy', *Cooperation and Conflict* 19, no. 4 (1984): 263–73, 266.
[44] 'Inquiry into U.S. Costs and Allied Contributions to Support the U.S. Military Presence Overseas', *United States Senate Committee on Armed Services*, April 15, 2013, 6.
[45] Mumford, 'Proxy Warfare and The Future of Conflict', 42.

Dave Whyte argue that these entities were able to provide cheap warfare due to their "lower start-up and running costs" compared to national military deployments.[46]

Direct Confrontation Costs

Direct confrontation with the US or one of its allies is likely to generate high economic costs, especially in the presence of nuclear-armed nations.[47] Utilizing proxies minimizes direct confrontation whilst still achieving national interest goals at an arm's length. In doing so, states may avoid ex-post costs, such as direct retribution, internationally imposed sanctions, and condemnation, as well as the "governance costs" associated with annexation.[48] For example, Byman and Krebs argue that Iran's use of terrorist organizations such as Hezbollah is in recognition of the fact that "Tehran's weak military forces could not" effectively persist in an attack on Israel themselves.[49]

The use of proxies also enables the state greater flexibility in deciding to enter into and remove itself from conflicts. This contrasts with alliance-based relationships which are reciprocal, whereby if one alliance member is attacked, the other members of the alliance are obligated to respond. These formal, contractual relationships are less appealing to states, especially under the realist model of international relations. Glenn Snyder explains how alliance commitments can lead to entrapment, where countries are compelled to enter into a "conflict over an ally's interests that [the other state] does not

[46] Cliver Walker and Dave Whyte, 'Contracting out War?: Private Military Companies, Law and Regulation in the United Kingdom', *The International and Comparative Law Quarterly* 54, no. 3 (July 2005): 651–89, 659.
[47] "5-7% of [Ukrainian] government spending each year is still devoted to Chernobyl-related benefits and programs." "Economic Impacts of Nuclear Weapon Detonation," *Article 36*, March 2015, 3.
[48] Idean Salehyan, 'The Delegation of War to Rebel Organizations', Journal of Conflict Resolution 54, no.3 (2010): 493-515, 504.
[49] Daniel Byman and Sarah E. Kreps, 'Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism', *International Studies Perspectives* 11 (February 2010): 1–18, 4.

share, or shares only partially."[50] Proxies by comparison are often temporal and informal arrangements.[51] They allow politics elites to choose their conflicts on a case by case basis, avoiding direct military engagement.

Political Costs

As proxies are often characterized by more informal relationships, they are considered "less public and hence less subject to domestic constraints"[52] Political costs can be incurred both domestically and externally but appear to have a similar calculus. According to Borghard, in the presence of "domestic veto players", elites may utilize more secret forms of action to circumvent what would be considered an unpopular course of action.[53] This presupposes that the state-proxy relationship is clandestine within domestic or international circles. Therefore, in states with weak or highly accountable political leaders, it may be beneficial to use proxies to avoid decreasing public support.[54] For example, according to Mueller's causality hypothesis, as human causalities increases, support for war decreases.[55] Using proxies can allow political leaders to achieve strategic goals in the presence of domestic constraints and anti-war sentiment.

---

[50] Glenn H. Snyder, 'The Security Dilemma in Alliance Politics', *World Politics* 36, no. 4 (July 1984): 461–95, 467.
[51] Major Amos Fox, 'In Pursuit of a General Theory of Proxy Warfare', *The Institute of Land Warfare (123)*, 2019, 5.
[52] Glenn H. Snyder, *Alliance Politics* (Cornell Universtiy Press, 1997), 15.
[53] Borghard, 'Friends with Benefits? Power and Influence in Proxy Warfare', 14; The presence of domestic veto players is discussed primarily in the context of democracies as a reason for slow responses to threats. Randall L. Schweller, 'Unanswered Threats: A Neoclassical Realist Theory of Underbalancing', *International Security* 29, no. 1 (2004): 159–201.
[54] Borghard, "Friends with Benefits? Power and Influence in Proxy Warfare.", 38.
[55] John E. Mueller, *War, Presidents and Public Opinion* (John Wiley & Sons Inc, 1973).

Both Schelling and Fearon explain how backing down in the face of explicit commitments can result in reducing domestic and international credibility.[56] This was displayed through Obama's red line on the use of chemical weapons by Assad. He ultimately reneged on his commitment saying that he understood that "press(ing) the pause…would cost [him] politically.[57] However as state-proxy relationships are not always clear, this allows leaders to circumvent appearing weak in the international system.

2.4.2 Efficiency

Hawkins et al. argue that "without some gains from specialization, there is little reason to delegate anything to anybody."[58] Specialized proxy forces can create efficiency gains for states that may not have familiarly with certain conflict zones. The sponsoring state can skirt geographical boundaries as well as informational asymmetries through the use of domestically-based actors who know the terrain and national character.[59] In doing so, states present a legitimate "face" to the campaign, resulting in less domestic resistance.[60] [61] For example, the US assisted the Mujahideen in Afghanistan, which contributed greatly to their victory over the Red Army. Through this strategic relationship, the US was able to maintain an "arm's length"[62] presence in Afghanistan

---

[56] James D. Fearon, "Domestic Political Audiences and the Escalation of International Disputes," *American Political Science Review* 88, no. 3 (1994): 577–92.; Thomas Schelling, *Arms and Influence* (Yale University Press, 1966).
[57] Jeffrey Goldberg, 'The Obama Doctrine', *The Atlantic*, April 2016.
[58] Darren Hawkins et al., *Delegation and Agency in International Organizations* (Cambridge University Press, 2006), 13.
[59] Salehyan, 'The Delegation of War to Rebel Organizations', 504.
[60] Ibid.
[61] Daniel Byman, "Why Engage in Proxy War? A State's Perspective," *Brookings*, May 21, 2018.
[62] Salehyan, 'The Delegation of War to Rebel Organizations', 502.

using a local force that understood the region and its people. However, although the Mujahideen may have needed US support then, they have since become stronger and found other sources of support. In fact, the Mujahideen case demonstrates how proxies can "bite the hand that feeds them" as "only a small portion of the Stingers the US supplied to proxies in Afghanistan were ever recovered."[63] This misalignment and growing strength of the proxy highlights the multiple risks that states must shoulder in such relationships.

2.4.3 Plausible deniability

Using proxies is thought to provide states with "plausible deniability", such that the command and control link between is blurred to an extent that it is difficult to determine the ultimate sponsor of a proxy, allowing for the state to deny involvement. Gregory Treverton, a member of the first Senate Select Committee on Intelligence, stated that plausible deniability "enable(s) the US government to argue plausibly that it, and failing that, at least the President, had not been involved."[64] Much of the literature surrounding plausible deniability argues that it is de facto desirable and attainable, based upon an assumption that states "lack awareness of the hidden hand behind successful operations."[65] However, as recently demonstrated by Russian involvement in the 2016 US elections, attribution to the origin is possible. Even in the Cold War – "the (so-called) age of plausible deniability" – proxy "operations were apparent but not acknowledged."[66]

---

[63] Pfaff and Granfield, 'The Moral Peril of Proxy Wars', *Foreign Policy, April 5, 2019*.
[64] Gregory F. Treverton*, Covert Action* (I.B. Tauris & Co Ltd (1988), 5.
[65] Rory Cormac, and Richard Aldrich, "Grey Is the New Black: Covert Action and Implausible Deniability", International Affairs 94, no.3 (2018): 477-94, 481.
[66] Cormac and Aldrich "Grey Is the New Black: Covert Action and Inplausibel Deniability", 480, 483.

However, today the cost-benefit analysis appears to have shifted as non-virtual proxies are tracked and explicitly connected to their state sponsors.[67] As a result, we might expect states to use more transparent, formal methods of proxy relationships to impose greater control, and avoid potential issues associated with agency slack and adverse selection. Yet, this has not been the case and proxies are continuously used in the covert action space. This indicates that the detachment between proxies and the state is considered valuable, even with the absence of true plausible deniability.

Recent analyses of this concept argue that plausible deniability is not a binary condition but rather exists on a spectrum and has "multiple audiences."[68] According to Michael Poznansky, there are two types of plausible deniability a "state model" and an "executive model."[69] The state model is defined by the entire government entity seeking plausible deniability, whilst the executive model is defined by an attempt to disaffiliate an action from the chief executive, rather than the entire state apparatus. The model suggests that plausible deniability is used to appease domestic audiences and/or international audiences. (Figure 2.2) The use of proxies further separates the action from government structures, allowing some semblance of deniability, resulting in limited escalation opportunities for adversarial states. As stated by Daniel Byman, Israel has been struck by Iran-sponsored Hezbollah multiple times but has not directly felt "compelled to strike Iran itself."[70] There could be many reasons for this but key among them is that it is not always clear to what extent Hezbollah is acting on behalf of Iran.[71] This indicates that the

[67] See: 'Terrorist Designations and State Sponsors of Terrorism', *U.S. Department of State, Bureau of Counterterrorism*.
[68] Cormac and Aldrich, "Grey Is the New Black: Covert Action and Implausible Deniability", 487.
[69] Michael Poznansky, 'Revisiting Plausible Deniability', *Journal of Strategic Studies*, 2020.
[70] Byman, "Why Engage in Proxy War? A State's Perspective."
[71] Kimberley N. Trapp, *State Responsibility for International Terrorism* (OUP Oxford, 2011), 35.

proxy's separation from the state infrastructure makes it difficult for adversaries to respond directly, thus limiting escalation.

Figure 2.2: Two models of state plausible deniability

Model	Relevant actor	The How	The Why	Threat to exposure	Relation to democracy
State	The government	Conceal support	International concerns	Leaks, rival states, ICTs	Harmonious
Executive	The chief executive	Distance from operators	Domestic concerns	Tightly-held sources	Conflictual

Source: Michael Poznansky, 'Revisiting Plausible Deniability', *Journal of Strategic Studies*, 2020, 18.

Another example is US intervention into Afghanistan between 1979-1986. The US provided covert assistance to Pakistan which was transferred to Afghan rebels, yet by 1985 such action was an open secret within both domestic and foreign state circles. However, the US continued to deny their involvement. As posited by Austin Carson, this strategy was adopted to provide the USSR with "face-saving space to continue to abstain from retaliation."[72] If the US had publicly admitted their involvement, it may have forced the USSR to respond directly to either Pakistan or the US. The deniability kept the conflict within the specter of limited war.

2.5 Drawbacks of Using Proxies

As demonstrated from the above, there are several reasons why states may use physical proxies, including costs, efficiency, and plausible deniability benefits. However, an analysis of the principal-agent framework demonstrates that there are multiple risks in delegation. These risks are enhanced when traversing the boundary between state and

[72] Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton University Press, 2018), 268.

non-state actors. The question is not just simply 'why do states use cyber proxies when they could build up their own central capabilities?', but also 'why do they use them considering the risks?' In this section I will explain the unintended consequences that can arise as documented within the physical space. I will then go onto explain how these drawbacks might apply to cyberspace.

2.5.1 Drawbacks of using physical proxies

In understanding the risks of outsourcing to proxies, political scientists reference the principal-agent framework. It was first utilized in the field of economics as a model through which to understand how decentralizing authority can generate backlash. Principal-agent dilemmas include Adverse Selection and Agency Slack.

Adverse Selection

Adverse Selection occurs because "the principal cannot completely verify [the] skills or abilities [of an agent] either at the time of hiring or while the agent is working."[73] As a result, the principal risks underperformance or overperformance, both of which create uncertainty as to the efficacy of the agent in achieving the principal's goals. The result of this uncertainty is that the principal could pay a high price for a low-quality agent. Using Akerlof's theories of quality uncertainty, principals typically offer prices that are too low for "high-quality applicants," meaning that only low-quality agents apply. (Akerlof 1970) For example, the "US spent millions training various Syrian opposition-group members, but in the end only a handful showed up for the fight".[74]

[73] Kathleen M. Eisenhardt, 'Agency Theory: An Assessment and Review', *The Academy of Management Review* 14, no. 1 (January 1989): 57–75, 61.
[74] Byman, 'Why Engage in Proxy War? A State's Perspective'.

Agency Slack

Agency Slack occurs when the interests of the agent diverge from those of the principal, resulting in what Hawkins et al. describe as "independent action by an agent that is undesired by the principal."[75] Idean Salehyan highlighted the Rwandan state support of the armed ADFL (Alliance of Democratic Forces for the Liberation of Congo) rebels as an example. Within Joseph Kabila's (former President of the Congo) campaign to overturn the Congolese government led by Mobutu Sese Seko in the 1990s, Rwanda hoped that Kabila would install a Congolese government that was more friendly to Rwanda. However, he would later expel all Rwandan advisors and arm Rwandan insurgents.[76] Such relationships lead "ex-ante to uncertainty" which results "ex-post to concrete disadvantages"[77] For the principal, the tension exists between the risk of delegating authority and the benefits of indirect conflict.

The problem of Agency Slack is most acute in the face of ideological misalignment, such that the goals of the state and the proxy are – in some capacity- no longer synergistic. As assessed by D. Roderick Kiewiet and Matthew McCubbins, "there is almost always some conflict between the interests of….principals and agents."[78] In discussing the value of proxies, Stephen Biddle uses the lens of Security Force Assistance (SFA) to show that providing arms and training to local proxies does not necessarily produce any strong military benefits. The purpose of SFA within the US military strategy

[75] Hawkins et al., *Delegation and Agency in International Organizations, 8*.
[76] Salehyan, 'The Delegation of War to Rebel Organizations', 501.
[77] Patrick Keil, 'Principle Agent Theory and Its Application to Analyze Outsourcing of Software Development', ACM SIGSOFT Software Engineering Notes 30, no.4 (July 2005): 1-5, 1.
[78] D. Roderick Kiewiet and Matthew D. McCubbins, *The Logic of Delegation* (University of Chicago Press, 1991), 5.

was to "limit the US footprint" within foreign conflicts.[79] However, Biddle argues that the same security dilemmas that occur within principal-agent dilemmas are present in US SFA agreements. He also speaks to an inverse relationship between interest alignment and SFA provision by the US. For example, SFA partners have included many corrupt states with known divergent moral and ideological standpoints, such as Pakistan, "which provides a haven for Al-Qaeda's global headquarters and for Taliban militants who have killed thousands of US soldiers in Afghanistan."[80] Somewhat paradoxically, the "governance problems that give rise to the US interest in SFA often simultaneously promote interest divergence between the United States and its partner."[81] The question remains as to why states continue such a strategy when finding an aligned partner is so unlikely, thus resulting in moral hazards.

Beyond ideological alignment, states may use proxies when they know the proxy's survival is dependent on their support. There are multiple benefits for non-state actors to enter into these relationships. It allows non-state actors to overcome power asymmetries, evade repression, and augment their capabilities. However, these benefits are highest within conflicts where the non-state actor is a minority in another country which would falter without external support. This dynamic, at least at the outset, forces the agent's reliance on the principal. However, this reliance also has its limits because the more a state is successful in its operation, so is the proxy itself.[82] Success often entails an expanded capability or regional presence leading to decreased reliance upon a sponsor as

[79] Stephen Biddle, 'Building Security Forces and Stabilizing Nations: The Problem of Agency', *Daedalus (146)*, no. 4 (2017): 126-138, 129.
[80] Biddle, 'Building Security Forces and Stabilizing Nations: The Problem of Agency', 128.
[81] Ibid.
[82] Byman and Kreps, 'Agents of Destruction?', 8.

the proxy reaches self-sufficiency. Ultimately, the possibilities of Agency Slack can still occur even if not apparent at the outset.

States may also experience domestic political conflicts should a proxy's activity diverge from intention. Depending on how states present their connection to their proxies, much like alliances, there is a possibility that they will become bound to their proxies despite their informal relationship structure. If support is announced publicly by the state and is domestically supported, backing away from a proxy even if the relationship is no longer strategically advantageous may be met with domestic pushback.[83] Fearon assesses that this is most acute in democracies due to the electoral dependency of leadership.[84] However, Jessica Weeks argues that often in authoritarian nations, political leadership is highly vulnerable to domestic challenges by other elites and that this is often of paramount concern to leaders.[85] This therefore, could result in a state finding itself consistently connected to actions that it no longer supports.

Implications

Adverse Selection and Agency Slack, fueled by information asymmetries, can have dangerous consequences summarized by The Promethean Dilemma and The Inadvertent Crisis Dilemma. The Promethean Dilemma occurs when an agent retaliates against the principal through the use of the very tools that the principal provided for agent empowerment. The Inadvertent Crisis Dilemma, by comparison, occurs when a proxy has been empowered to such an extent that they take actions outside of their mandate, leading

[83] Byman, "Why Engage in Proxy War? A State's Perspective."
[84] Fearon, "Domestic Political Audiences and the Escalation of International Disputes."
[85] Jessica L. Weeks, 'Autocratic Audience Costs: Regime Type and Signaling Resolve', *International Organization* 62, no. 1 (2008): 35–64, 36.

to conflict escalation rather than containment.[86] In fact, Pfaff and Granfield argue that "once a proxy has a benefactor's support, they have a greater incentive to escalate conflict rather than resolve it."[87] This may negate potential cost savings and result in greater crises, especially when multiple principals are involved.[88] One such case is the crisis in Yemen which has incurred high costs but also resulted in ethical failures that challenge the conception of just war.[89]

Alongside restricting the mandates of agents, Nielson and Tierney's analysis of the principal-agent problems within international organizations argues that the existence of credible threats by the principle may "reduce the gap between the principal's demands and the agent's subsequent behavior"[90] However, others argue that there must also be a system of monitoring in place to reduce information asymmetries in the first place (McCubbins and Schwartz, 1984; Kiewiet and McCubbins, 1991).

2.5.2 Drawbacks of Cyber Proxies

The very real problems of using physical proxies, as outlined above, leads again to ask why states would elect to use cyber proxies?

In cyberspace some of the above problems appear even more acute. The circumstances for non-state groups or "rebels" have changed. The agents are not necessarily repressed or under-resourced in constant fear of physical attack from controlling political elites. In fact, they are often anonymous, and highly skilled without

[86] Borghard and Lonergan, 'Can States Calcualte the Risks of Using Cyber Proxies?', 415.
[87] Pfaff and Granfield, "The Moral Peril of Proxy Wars."
[88] Byman, "Why Engage in Proxy War? A State's Perspective."
[89] Rondeaux and Sterman, 'Twenty-First Century Proxy Warfare', 54.
[90] Daniel L. Nielson and Michael J. Tierney, 'Delegation to International Organizations: Agency Work and the World Bank Environmental Reform', *International Organization* 57, no. 2 (Spring 2003): 241–76, 251.

much need from a principal to augment their capabilities.[91] Furthermore, in such a world where proxies may comprise of ad-hoc, 'for-hire' services, they no longer limits themselves to states that share their political motivations. This leads to decreased dependence as proxies may threaten to turn to other nations "if they [feel] unsupported."[92] Therefore, there is a shift in power balance, where the state is in competition with others for the proxy's continued aligned behavior.

As a result, principal-agent problems such as the Inadvertent Crisis Dilemma may be more pronounced. For example, as cyber-attacks persist within an already global domain the capability to act against one state can also be leveraged against others. This compares to the physical space where the transference of a conflict beyond its borders may require a proxy to form relations with other proxies or build-up sophisticated capabilities – both of which take time. Cyber proxies can flexibly change targets without significantly altering their operational strategy.[93]

By the same coin, cyber proxies possess tools that can be used against the sponsor in a very direct fashion. For example, where physical proxies may volte-face and use their empowered position to undermine the sponsors strategic objectives within the foreign field of battle, cyber proxies can use their position to hack into the sponsoring state themselves. This indicates that cyber proxies can wield far more power than physical proxies to punish their sponsor. However, as cyber proxies do not need to travel

[91] Jamie Collier, 'Proxy Actors in the Cyber Domain', *St. Anthony's International Review* 13, no. 1 (May 2017): 25–77, 29,32.
[92] Byman, "Why Engage in Proxy War? A State's Perspective."
[93] As indicated by the use of one APT group to target multiple industries, or one vulnerability exploitation attempt on an Internet Service Provider (ISP) to target multiple entities.

extraterritorially to conduct operations, states may be able to limit these risks through control on the cyber environment within their borders.

2.6 Benefits of Using Cyber-Proxies

Maurer and many other scholars in this area discuss a multitude of reasons as to why states use cyber proxies, many of which reflect the same literature as in the physical space. Maurer argues that there is a degree of path dependency in this regard and that "proxy relationships are strongly tied to a country's political, economic, legal and cultural system, taking decades rather than years to transform."[94] He also gives three primary reasons why states enter into these relationships: first, nation-states are failing to attract "the quantity and quality of talent", second, non-state ability to achieve highly disruptive attacks quickly and third, a "revival of plausible deniability."[95] I find that each of these reasons can be translated into skills gaps, increased efficiency, and plausible deniability respectively.

In considering the skills gap argument, public sources of information often cite the battle between the private and the public sector to attract highly skilled workers.[96] However, this dynamic is mostly analyzed from a Western standpoint. A proxy's ability to achieve highly disruptive attacks appears to align with the specialization argument as reasoning for the use of physical proxies. Under my definition of cyber proxy, does this argument persist?

---

[94] Maurer, 'Cyber Proxies and Their Implications for Liberal Democracies', The Washington Quarterly 41, no. 2 (2018): 171-188, 182.
[95] Ibid, 172 .
[96] Ellen Nakashima and Aaron Gregg, 'NSA's Top Talent Is Leaving Because of Low Pay, Slumping Morale and Unpopular Organization', *Washington Post*, 2 January 2018.

Where some define the use of cyber proxies as the re-emergence of plausible deniability, others see it as a continuation of "implausible deniability". What is clear is that while not plausible deniability, we are acting in a time of useful deniability where the lack of regulation and clarity around the cyberspace and cyber-warfare, creates uncertainty as to appropriate responses. There is a lack of discussion around how the domain itself impacts the decision as to why states use proxies. Perhaps it is not attribution that countries fear but rather retribution. As large nations are constrained to certain appropriate retaliatory actions, cyberspace almost acts a clear path by which competing states can maneuver without fear of retaliation.

Cormac and Aldrich argue that the driving force behind today's use of "implausible deniability" is the ability to show resolve and strength against adversaries whilst also preventing escalation.[97] Archives from the Cold War, indicate that "many 'secret' western operations were in fact known to Soviet intelligence."[98] State secrecy through covert operations is under threat from its citizens who can act as whistle-blowers through multiple outlets, including the internet itself.[99] As such, no state can credibly rely on concrete plausible deniability but rather seek ambiguity as a means of confusing opponents. Cormac and Aldrich assess this approach in the context of today's hybrid warfare, which includes cyber operations in the form of influence campaigns. The lynchpin of hybrid warfare is "to generate a situation where it is unclear whether a state of war exists – and if it does, who is a combatant and who is not."[100] This is particularly

[97] Cormac and Aldrich, 'Grey Is the New Black: Covert Action and Implausible Deniability', 488.
[98] Ibid, 482.
[99] Ibid, 479.
[100] Rod Thornton, 'The Changing Nature of Modern Warfare', *The RUSI Journal* 160, no. 4 (4 September 2015): 40–48, 41.

present in cyber conflicts in which definitions around what constitutes an act of war over just an act of aggression are not clearly defined. NATO's faltering response to multiple suspected Russian hacks against European members displays a lack such a lack of coherency, and how to appropriately respond to it. By being unable to conclusively trace activity back to the Russian government, NATO is wary not to escalate or legitimize Russia's actions by pulling almost the entire European block into conflict.[101] Therefore, using cyber proxies may effectively obscure the origin of an attack, thus allowing states to act with impunity.

2.7 Conclusion

There are many risks posed through the use of cyber proxies as a result of principal-agent dilemmas. This leads to the question of why states would elect to use proxies in the presence of these risks. From analyzing the literature on the use of physical proxies and the limited literature on cyber proxies, I show that there are several potential advantages. The literature currently appears to assume that these benefits exist as explanations but there has not been a clear, concerted effort to assess them within the context of the current environment. Furthermore, as a result of principal-agent dilemmas, states must establish systems to adequately monitor their proxies to ensure mission alignment and success. There has, however, been limited analysis of the continuum between deterrent mechanisms and cyber proxies.

[101] David E. Sanger, 'As Russian Hackers Probe, NATO Has No Clear Cyberwar Strategy', *The New York Times*, 16 June 2016.

Within this thesis, I will examine how these explanations translate to the virtual space through evaluating the following hypotheses within my four countries of focus:

1) Cyber proxies provide economic cost-saving advantages

2) Cyber proxies afford states with enhanced plausible deniability benefits in comparison to state agents

3) The unique skills and specializations that exist outside the government apparatus motivate outsourcing

4) These states use cyber proxies because they are in the best position to control them

Chapter 3. Trends and Interactions

An Overview of State Cyber Capabilities and Proxy Agents

I have highlighted Russia, China, Iran, and North Korea because, as stated by the 2019 US Intelligence Threat Assessment, these four countries are major threat actors.[102] Before answering why these states use cyber proxies, I will first illustrate the existence of such relationships. I will detail a number of alleged cyber proxy use cases whose operations were focused on US targets. In the following sections, I will:

1) Synthesize trends of use through analyzing various cyber incidents and Advanced Persistent Threat (APTs) Groups.[103]

2) Demonstrate the existence of these cyber proxies across all four states, and

3) Provide some indication of how cyber proxies are used.

3.1 General Trends: State Activity Has Increased, but Tactics Have Stayed the Same

Much of this research is based upon unstructured data using analyses conducted by threat analysts at private cybersecurity firms. The threat intelligence industry as a whole is new and standardization is lacking. Open source cyber threat intelligence emerged as a result of private cyber defense companies setting up research arms to aid both their R&D and commercial success. However, as stated by JD Work, a cyber intelligence professional and chair for Cyber Conflict and Security at Marine Corps

[102] Daniel R. Coats, 'Worldwide Threat Assessment of the US Intelligence Community 2019', *Senate Select Committee on Intelligence, Office of the Director of National Intelligenc*e, January 29, 2019, 5.
[103] Crowdstrike defines APTs as "a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time.", 'APT Definition', *Crowdstrike*, 18 November 2019.

University, "differing intelligence shops typically rely on very different approaches to collection against cyber threat targets."[104] Even within commercially produced intelligence reports, providers admit their inability to maintain "the status quo".[105] Furthermore, much of their analysis is based on data generated from their customer base. As a result, most claims in regards to attribution are necessarily attached with a disclaimer and are susceptible to bias.

Despite these inherent limitations, there is no question that the number of cyber-attacks has increased year on year, and state activity is increasingly targeted a wide range of industries. According to the 2019 World Threat Assessment issued by the Office of the Director of National Intelligence, "The growing availability and use of publicly, and commercially available cyber tools is increasing the overall volume of unattributed cyber activity around the world."[106] Today's cyber activity is increasingly complex.

However, a few major trends persist. Yearly threat reports from major cybersecurity intelligence firms report a rise in the number of active APTs. These groups are often thought to be state or state-sponsored entities due to their targets, techniques, and continued activity.[107] Verizon has published its Data Breach Investigations Report (DBIR) every year since 2008, which tracks data breaches.[108] Between the 2018-2019 DBIRs, Verizon reported an 11% increase in "actors identified as nation-state or state-

[104] JD Work, 'Evaluating Commercial Cyber Intelligence Activity', *International Journal of Intelligence and CounterIntelligence 33*, no.2, 16 January 2020, 8.
[105] Verizon, "2014 Data Breach Investigation Report', 7.
[106] Coats, 'Worldwide Threat Assessment 2019', *7.*
[107] "What Is an Advanced Persistent Threat (APT)?," *CISCO*.
[108] Verizon defines a breach as "An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party." Verizon, '2019 Data Breach Investigations Report', 2019.

affiliated."[109] Other firms such as Crowdstrike made similar allegations of increasing state-sponsored activity. Their detection of influence campaign activity within Taiwan and Hong Kong on behalf of alleged Chinese APTs signals an increasing likelihood that such activity will be mimicked against other external targets, including the US.[110] Alongside this, Symantec and Crowdstrike have explicitly detected a decrease in malware attacks and an increase in "living off the land" (LOTL) techniques.[111] Symantec has also noted a continued decline of zero-day exploits utilized by APTs. Such trends, rather than indicating reducing sophistication, actually signal that attackers are shifting towards "defense evasion methods"[112] to "maintain a low profile by hiding their activity in a mass of legitimate processes."[113] Verizon also reports that these alleged nation-state or state-affiliated breaches mostly appear to be cyber-espionage, with phishing as the most widely used tactic.[114] This information indicates that targeted cyber operations at the behest of or by nation-states are on the rise, and that techniques employed whilst not necessarily state of the art, still achieve objectives.

To what extent however is this activity conducted by cyber proxies on behalf of China, Russia, Iran, and North Korea?

---

[109] DBIR 2018 reported 12% state/state-affiliated breaches, while DBIR 2019 reported 23%. Verizon, '2019 Data Breach Investigations Report', 5.
[110] '2020 Global Threat Report', *Crowdstrike*, 2020.
[111] '2020 Global Threat Report', *Crowdstrike*, 8; 'Internet Security Threat Report 2019', *Symantec* (February 2019), 18.
[112] Mark Goudie, 'Going Beyond Malware: The Rise of "Living off the Land" Attacks', *Crowdstrike Blog*, 2 May 2019. Living off the land attacks are non-malware exploits, utilized increasingly by APT groups. These exploits make use of "native tools already present" on the victim's system. In doing so, it can help attackers maintain a low profile by hiding their activity within "legitimate processes."
[113] 'Internet Security Threat Report 2019', *Symantec,* 18.
[114] Verizon '2019 Data Breach Investigations Report', 25.

The table (Figure 3.1) below represents a snapshot of how cyber proxy groups are used today. Much of this section is built upon the extensive analysis conducted by Tim Maurer within *Cyber Mercenaries*, and its supplemented through a qualitative analysis of multiple DoJ indictments, mainstream media sources, think tank analyses and industry reports. To gather this evidence, I relied heavily upon DoJ indictments between 2010-2020, accompanied by industry reports that track operations of specific state-affiliated APTs and publish annual threat reports. In recognition that the DoJ and private industry are constrained by political, legal, and commercial motivations, I also used Google search function to broaden my discussion and draw further insights from mainstream media and think tanks.

Figure 3.1: How cyber proxies used today by China, Russia, North Korea, and Iran[115]

Functions	China	Russia	North Korea	Iran
Front companies	Yes	Yes	Yes	Yes
Individual hackers	Yes	Yes	Yes	Yes
Dual-motivation operations	Yes	Yes	Unclear	Yes
State and proxy agents within one operation	Unclear	Yes	Unclear	Unclear
Influence campaigns	Yes	Yes	Yes	Yes
Economic advantage	Yes	Yes	Yes	Yes

In subsequent sections, I will examine cyber proxy use within all of these states, demonstrating the above functionalities.

[115] Definitions - Front companies: known and perhaps registered private companies that are used to cover state activity; Individual hackers: non-state individuals with no clear group affiliation; Dual-motivation operations: one group or individual conducting cyber operations that satisfy different goals. For example, national interest/personal interest, financial/political etc.; State and proxy agents within one operation: The explicit presence of a state agent and a non-state entity working cohesively within the same operation – usually conveyed through indictments; Influence campaigns: attempts to influence rhetoric around political events in a foreign nation through the use of online forums and media; Economic advantage: cyber-enabled operations to enhance economic advantage of one nation state against another – could involve ransomware attacks, attacks on the financial sector or intellectual property theft.

3.2 China's Use of State-Sponsored Cyber agents and their Pursuit of Independence

Back in 2001, a Foreign Affairs article stated that "it will be some time before the Internet becomes a political threat in China"[116], citing the low percentage of internet users and highly effective state regulations. China and other states appear highly concerned with controlling favorable domestic narratives, ensuring ideological alignment.[117] This concern appears to have mounted in response to the growth and accessibility of digital technologies. The Chinese conception of cybersecurity differs from the definition used within the US. According to the 2018 US National Cyber Strategy, cybersecurity is defined by the ability to identify, protect and ensure the resilience of online networks, systems, functions, and data as well as "recovering from incidents."[118] However, both China and Russia appear to define cybersecurity in terms of information security, intended to prevent the external influence upon domestic rhetoric.[119] An article first published in IPI Global Observatory suggests that China's build-up of its internet infrastructure is perhaps in response to its desire to make its "internal internet infrastructure more secure."[120]

Tim Maurer argues that China is an example of a state that has made its way from "sanctioning" to close "delegation" of its cyber proxies.[121] Maurer lays out a framework through which to assess the nature of state-cyber proxy relationships using three distinct

---

[116] Nina Hachigian, "China's Cyber Strategy," *Foreign Affairs* March/April (2001).
[117] Beina Xu and Eleanor Albert, 'Media Censorship in China', *Council on Foreign Relations*, February 17, 2017.
[118] 'National Cyber Strategy of the United States of America', *President of the United States*, September 2018, 2.
[119] Maurer, *Cyber Mercenaries, 6*.
[120] Lyu Jinghua, 'What Are China's Cyber Capabilities and Intentions?', *IPI Global Observatory*, 22 March 2019.
[121] Maurer, *Cyber Mercenaries, 20-21, 107*.

terms: Sanctioning, Orchestration, and Delegation. Sanctioning is the least tightly managed relationship with the state providing "passive support" through "turning a blind eye to their activities." Orchestration is defined through state support but without specific instruction or oversight. Delegation describes a relationship through which the state would have "overall or effective" control of the cyber proxy. He assesses that from 1994 to the present day, China has experienced a growth in not only its technical ability but also oversight upon its cyber proxy agents.[122] These proxies are thought to have originally formed within patriotic hacker communities and online forums that would frequently act to advance the "interests of the Chinese nation."[123] A notable example occurred in 2001 where a collision between a Chinese fighter jet and a US signals intelligence aircraft in disputed airspace lead to the death of the Chinese pilot. As a result, Chinese hacktivist groups initiated "Hack the US week".[124] However, in the past two decades, the Chinese government has sought to bring these groups and individuals under command and control through establishing "information warfare militias,"[125] and utilizing students within technical universities as cyber militias.[126] Agreements made with President Obama in 2015, primarily over commercial cyber espionage, seem to demonstrate that Xi Jinping is willing to take a harsher stance with domestic hacker groups. Whilst evidence suggests that no long term control over Chinese origin IP theft was attained as a result of the agreement, these public statements from Chinese leadership

[122] Ibid, 107-119.
[123] Ibid, 109.
[124] Daniel M. Creekman, 'A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China', *American University International Law Review* 17, no. 3 (2002): 641–81, 643.
[125] Maurer, 'Cyber Proxies and Their Implications for Liberal Democracies',181.
[126] Alexander Klimburg, 'Mobilising Cyber Power', *Survival* 53, no. 1 (2011): 41–60, 45-46.

may indicate a growing dissatisfaction with uncontrolled hacker groups.[127] According to Beijing Knownsec Information, "China suffered the highest rate of DDoS[128] attacks in the world in 2018," yet 97% were believed to have originated from domestic hackers.[129]

Despite this concern, China appears to utilize proxy groups in attaining larger political ends such as economic independence. The 2015 "Cyber Agreement" (The Agreement) between President Xi Jinping and President Obama was a response to the alleged widespread Chinese-origin, cyber-espionage campaigns to steal US IP. According to the US IP Commission Report, the annual cost to the US as a result of global IP theft is between $225-600 billion.[130] Among requests for information sharing, The Agreement heavily emphasized the creation of norms in cyberspace, including a commitment to refrain from "conduct(ing) or knowingly support(ing) cyber-enabled theft of intellectual property".[131] The inclusion of such a clause is a reflection of an increasing number of incidents of suspected IP theft originating from what appears to be Chinese actors.[132] Yet, beyond asking for control on Chinese state-conducted IP theft, The Agreement makes references to IP theft which government "knowingly supports". Such a statement indicates the existence of a relationship between a state and an independent entity. To what extent, therefore does China engage and utilize these "non-state actors"?

---

[127] Andy Greenberg, 'China Tests the Limits of Its US Hacking Truce', *Wired*, 31 October 2017.
[128] DDoS (Distributed Denial of Service) attacks are large-scale disruptive intrusions that prevent system performance as intended due to an overload of system requests.
[129] Jinghua, "What Are China's Cyber Capabilities and Intentions?"
[130] 'Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and the United States Policy', *The Commission on the Theft of American Intellectual Property*, February 2017, 12.
[131] 'Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference', *The White House, Office of the Press Secretary*, September 2015.
[132] United States Council of Economic Advisors. T*he Cost of Malicious Cyber Activity to the U.S. Economy,* 13.

Due to incomplete information, it is difficult to understand the degree of independence - or whether there is any independence at all - of discovered Advanced Persistent Threat (APT) groups to their alleged sponsoring state. For example, according to FireEye, a US cybersecurity company, APT1 also known as the Comment Crew, is actually Unit 61398 which is a branch of the 2nd Bureau of the People's Liberation Army (PLA) - a government agency.[133] Indeed, more recently APT17 thought to be a potential contractor conducting cyber operations on behalf of the Chinese Ministry of State Security (MSS), was later linked directly to the Chinese Ministry of State Security (MSS) by Intrusion Truth – an anonymous group that frequently doxes high profile APTs.[134] [135] Accordingly, APT1 and APT17 are not cyber proxies under my definition. Nevertheless, the degree of IP theft occurring from Chinese origins and the wording of The Agreement, suggests that there are non-state groups involved in state-cyber operations. To demonstrate, I shall use the example of APT3's activity.

3.2.1 APT3 in Focus

The 2019 DNI Threat Intelligence report states that the US is most concerned about China's cyber espionage and attacks on core military and critical infrastructure systems, which could last from "days to weeks" based on current sophistication.[136]

---

[133] 'APT1: Exposing One of China's Cyber Espionage Units', *Mandiant (FireEye)*, 2004, 3.; David Sanger, David Barboza, and Nicole Perlroth, 'Chinese Army Unit Is Seen as Tied to Hacking Against U.S.', *The New York Times*, 18 February 2013.
[134] Doxing is the process of internet-based investigation of an entity and publicly disclosing sensitive, identifying information. It is used both in cyber intelligence and malicious intent
[135] Catalin Cimpanu, 'APT-Doxing Group Exposes APT17 as Jinan Bureau of China's Security Ministry', *ZDNet*, 24 July 2019.
[136] Daniel Coats, 'Worldwide Threat Assessment of the US Intelligence Community 2019', 5.

APT3 was first identified as a suspected contractor for the Chinese Ministry of State Security on May 9 2017 by an anonymous cyber intelligence group called Intrusion Truth. Despite the anonymity of this group, their analysis tends to receive corroboration from major cybersecurity shops. Intrusion Truth claimed that it discovered the domain name purchasers of a compromised site that was receiving traffic as a result of successful spear-phishing emails. On this website was a Remote Access Trojan (RAT)[137] commonly known as Pirpi - a known APT3 tool.[138] The domain purchasers were linked to two men, both of whom were shareholders for a private company called Guangzhou Boyu Information Technology Company Ltd (Boyusec).[139] Previously in 2016, the Pentagon had exposed Boyusec as "a Chinese cybersecurity firm...covertly working with Beijing's Ministry of State Security intelligence service in conducting cyber espionage operations."[140] This existing information resulted in the conclusion that Boyusec was APT3. The claim was supported by the Inskit Group – the cyberthreat research arm of the well-known cybersecurity and intelligence firm, Recorded Future. Inskit Group conducted an open-source research effort that utilized academic works to trace cyber-related entities in China, website analysis, and posts related to Boyusec on Chinese job forums. They discovered that one of Boyusec's publicly advertised partner Guangdong ITSEC, "is subordinate to an MSS-run organization called China Information Technology Evaluation Center (CNITSEC) and that Boyusec has been working with

[137] A RAT is malware that allows attackers to remotely access and control a computer without detection.
[138] 'APT3 Is Boyusec, a Chinese Intelligence Contractor', *Intrusiontruth*, 5 September 2017.
[139] Ibid.
[140] Bill Gertz, 'Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service', *The Washington Free Beacon*, 29 November 2016.

Guangdong ITSEC on a joint active defense lab since 2014."[141] The number of entities allegedly involved in this interaction with APT3, indicates its complex relationship to the state, further obscuring the direct connection.

In November 2017, the US Department of Justice unsealed an indictment against three individuals linked to Boyusec for their role in "computer hacking, theft of trade secrets, conspiracy and identity theft" against three US firms.[142] Interestingly, although the indictment mentioned the hackers' connection to Boyusec, they did not make a connection to the Chinese state.[143] Considering the analysis previously done by Recorded Future, it may suggest that:

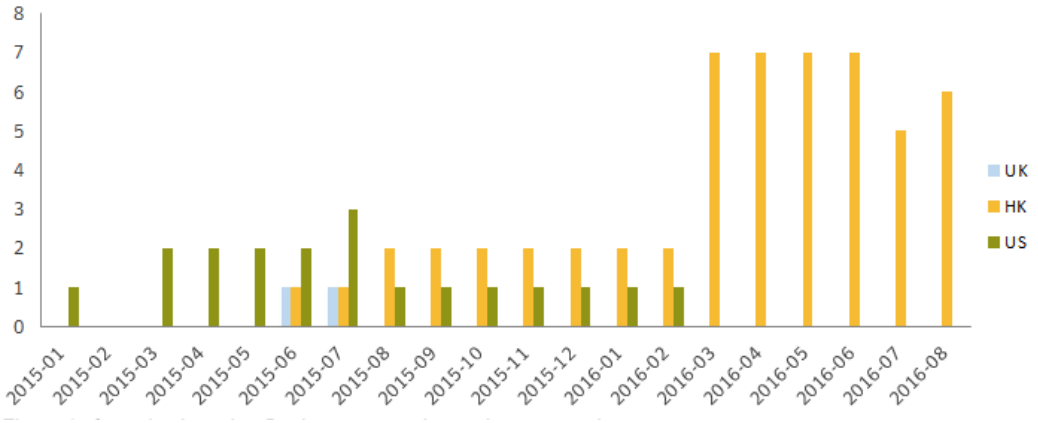
1) This particular activity was not considered to be state-sponsored, suggesting that Boyusec may engage in activity at the request of other entities beyond the states or,
2) Although such an operation may be state-supported or encouraged, the lack of direct naming in the indictment is a reflection of political or legal constraints, including a lack of evidentiary proof to meet legal thresholds.[144]

Another indication that APT3 may be state-linked is due to its change in activity during and post 2015. According to Symantec, APT3's targeting of the US peaked in July 2015, just two months before the Cyber Agreement meeting took place. (Figure 3.2) Afterward, it appears to significantly reduce and come to almost nothing in 2016, instead

[141] Insikt Group, 'Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3', *Recorded Future*, 17 May 2017.
[142] Victims were Moody's Analytics, Siemens AG and Trimble, Inc; Department of Justice, 'U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage', *Office of Public Affairs*, 27 November 2017.
[143] Tim Starks, 'Potential Rift with China over Hacking Charges', *Politico*, 28 November 2017.
[144] 'OSINT Isn't Evidence - InfoSec Needs to Take A Step Back & Breathe', *Secjuice*, 16 May 2018.

changing focus towards Hong Kong. The timing may suggest that the reduction in activity was due to the Cyber Agreement creating pressure for the Chinese government to reduce intrusions upon the US. That being said, there may be other confounding variables that explain this reduction of activity. The timing of increased attention on Hong Kong is reflective of political events calling for increased independence from Beijing in the form of the 2014 Umbrella Movement,[145] and the 2015 kidnapping of five Hong-Kong based publishers.[146] The potential political environment as a catalyst for APT3's shift is also evident in subsequent cyber-espionage campaigns discovered in 2016. (Figure 3.2) Ahead of Hong Kong parliamentary elections in September 2016, APT3 activity was detected within networks of two Hong Kong government departments. The Asia Pacific CTO of FireEye suggested the purpose was information collection before the upcoming elections.[147]

Figure 3.2: Change in APT3 targets over time



Source: A L Johnson, 'Buckeye Cyberespionage Group Shifts Gaze from US to Hong Kong', Symantec[148]

[145] Street protests broke out in Hong Kong in 2014 due to what was considered to be CCP interreference into political process.
[146] Andrew Nathan, 'How China Sees the Hong Kong Crisis', *Foreign Affairs*, 30 September 2019.
[147] 'Mainland Chinese Hackers Attack Hong Kong Government Departments: Security Firm', *The Straits Times*, 2 September 2016.
[148] A L Johnson, 'Buckeye Cyberespionage Group Shifts Gaze from US to Hong Kong', *Symantec Enterprise Community*, 6 September 2016.

Whilst APT3 was linked primarily to commercial espionage efforts, the timing of these shifts appear to be politically motivated and convey a higher degree of national interest motivation. It indicates that APT3 may be utilized for both financially and politically motivated operations.

3.3 Russia's Use of Non-State Actors and Their International Disruption Objectives

Russia is one of the most aggressive actors in cyberspace today. It is the only state suspected of systematically using cyber warfare concurrently with a physical offensive.[149] Yet, Russia has been slow in developing a comprehensive cyber central command. Only in 2013, did the Russian Ministry of Defense announce the development of a military arm dedicated to cyber operations.[150] However, according to James J. Wirtz, Dean of the School of International Graduate Studies at the Naval Postgraduate School and prolific writer in issues of international security, "Russia, more than any other nascent actor on the cyber stage, seems to have devised a way to integrate cyber warfare into a grand strategy capability."[151] The development of its civilian hacker force originally orientated itself towards personal financial gain, rather than ideological alignment.[152] Much like China, Russia's formal doctrine surrounding cyber activity has focused on information

[149] Michael Connell and Sarah Vogler, 'Russia's Approach to Cyber Warfare', CNA Analysis and Solutions, March 2017, 17-18.
[150] Ibid, 8.
[151] James J. Wirtz, 'Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy', *NATO CCDCOE*, 2015, 31.
[152] Winnona DeSombra and Dan Byrnes, 'Thieves and Geeks: Russian and Chinese Hacking Communities', *Recorded Future*, 2018, 3.

security rather than cybersecurity. The 2000 Information Security Doctrine framed threats to Russia as cyber-enabled information campaigns and influence facilitating the "degradation of spiritual values."[153] Such a statement suggests that Russia is more concerned with an power balancing against external actors rather than economic competition capability.

Russia is distinct in comparison to these other countries in that it has historically granted its civilians greater internet freedoms. Whilst Putin's regime introduced more domestic internet regulation, overall Russia adopts what Maurer assesses as a "laissez-faire approach" towards its cybercriminals.[154] This is consistent with comments from Misha Glenny, a Russian studies and cybersecurity researcher, who suggests that "Russian law enforcement and the FSB (Federal Security Bureau) in particular have a very good idea of what is going on and they are monitoring it, but as long as the fraud is restricted to other parts of the world they don't care."[155]

Russia's quick rise to a "full-scope cyber actor" despite its apparent latency in establishing cyber military commands, may have occurred with the assistance of cyber proxies.[156] Its non-state hackers are considered sophisticated and professional actors. Recorded Future's Inskit Group assesses that "Russian [hacker] forums leave very little room for socializing or camaraderie. These sites are places of business, not bastions for the community."[157] Indeed, recent indictments underscore a belief that Russia engages

---

[153] Nicu Popescu and Stanislav Secrieru, 'Hacks, Leaks and Disruptions Russian Cyber Strategies', *Issue* Chaillot Paper, no. 148 (October 2018), 16.
[154] Maurer, "Cyber Proxies and Their Implications for Liberal Democracies."
[155] Alissa de Carbonnel, 'Ex-Soviet Hackers Play Outsized Role in Cyber Crime World', *Reuters*, 22 August 2013.
[156] Daniel R. Coats, 'Worldwide Threat Assessment of the US Intelligence Community 2017', *Office of the Director of National Intelligence,* 11 May 2017, 1.
[157] DeSombra and Byrnes, 3.

with both formal security organizations but also informal hacker communities or individuals. For example, in 2017, the US Department of Justice (DoJ) indicted Karim Baratov, a Canadian national**,** for his role in compromising Yahoo's network and email accounts at the behest of the Russian Federal Security Service (FSB). The language of the indictment indicates that Baratov was not formally part of the FSB apparatus labeling him as a "criminal hacker."[158] A subsequent press release detailing Baratov's sentence identified him as a "Hacker-for-Hire."[159]

The Russian's decision to use Baratov is fascinating. As detailed within the indictment, the incentive for Baratov was financial.[160] Additionally, as a non-Russian national, his alignment with the FSB is more uncertain – a picture of principal-agent risks. As assessed by Brian Krebs, a cybersecurity and crime expert, Baratov "appears to have been the least careful about hiding his activities, leaving quite a long trail of email hacking services that took about 10 minutes of searching online to trace back to him specifically."[161] Whilst this thesis mostly finds evidence of domestically based cyber proxies, this event demonstrates the risks inherent with outsourcing to non-state actors, and the complex nature of the threat environment. The indictment further details two FSB

---

[158] Department of Justice, 'United States of America V. Dmitry Dokuchaev, a/k/a "Patrick Nagel". Igor Suschin, Alexsey Belan, a/k/a "Magg", and Karim Baratov, a/Ka/ "Kay," a/k/a "Karim Taloverov," a/k/a "Karim Akehmet Tokbergenov"', United States District Court For the Northern District of California (February 2017.), 4.

[159] Department of Justice, 'International Hacker-For-Hire Who Conspired with and Aided Russian FSB Officers Sentenced to 60 Months in Prison'*, Office of Public Affairs*, 29 May 2018.

[160] "When Baratov successfully obtained unauthorized access to a victim's account, he notified Dokuchaev and provided evidence of that access. He then demanded payment—generally approximately U.S. $100—via online payment services. Once Dokuchaev sent Baratov a payment, Baratov provided Dokuchaev with valid, illicitly obtained account credentials.", Department of Justice, 'United States of America V. Dmitry Dokuchaev, a/k/a "Patrick Nagel". Igor Suschin, Alexsey Belan, a/k/a "Magg", and Karim Baratov, a/Ka/ "Kay," a/k/a "Karim Taloverov," a/k/a "Karim Akehmet Tokbergenov"', United States District Court For the Northern District of California.

[161] Brian Krebs, 'Four Men Charged with Hacking 500M Yahoo Accounts', *Krebs on Security* (blog), 15 March 2017.

agents and a Russian-national as actors within this operation. The inclusion of FSB agents suggests that cyber proxies and state agents may work together in tight cooperation, rather than at an arm's length.

Reports suggest the Russian security services may also exploit established cybercriminal groups to serve national interest goals. An example is the Russian Business Network (RBN), whose activity is mostly directed at foreign entities.[162] The RBN – a commercial, offensive cybercrime syndicate – is suspected to have state affiliations as their activity demonstrates a "high-level of coordination in both timing and target selection of cyber-attacks" with Russian government security concerns.[163] Brian Krebs posits that there is likely to be some form of relationship between the state and the RBN.[164]

Another example of a seemingly sophisticated group is APT28, a suspected Russian cyber proxy who according to Crowdstrike targets "government, aerospace, NGO, defense, cryptology, and education sectors."[165] FireEye concludes that APT28's espionage campaigns source "intelligence that would only be useful to a government."[166] Its tactics, techniques, and procedures (TTPs) also "reflect a degree of sophistication and creativity generally not seen amongst advanced hacker groups", according to Stefan

[162] Brian Krebs, 'Shadowy Russian Firm Seen as Conduit for Cybercrime', *Washington Post*, 13 October 2007.
[163] Creery, 'Hacker Militias or Cyber Command? The U.S. and Russian Institutionalization of Cyber Warfare'.
[164] Krebs, "Shadowy Russian Firm Seen as Conduit for Cybercrime."
[165] Adam Meyers, 'Meet CrowdStrike's Adversary of the Month for March: VENOMOUS BEAR', *Crowdstrike,* March 12 2018.
[166] Meyers.; 'APT28: A Window into Russia's Cyber Espionage Operations?', FireEye (2014), 3.

Tanase of Kaspersky Labs.[167][168] For example, the group allegedly stole the TTPs of an Iranian non-state actor, OilRig.[169] Considering the sophistication of Russia's cyber-infrastructure, and the fact that APT28 had been linked to exploiting two distinct zero-days before this discovery, the copying of TTPs indicates an attempt to create "false flags", and avoid attribution.[170]

These two examples not only indicate that Russia does use non-state actors in the pursuit of launching offensive cyber-attacks but also suggests that they rely on both structured entities and "hackers-for-hire" for doing so. Furthermore, there appear to be efforts to obscure their activity, suggesting either a pursuit for plausible deniability and/or a desire to create confusion upon the international stage.

3.4 North Korea and the Necessity of State-Sponsored Operations

North Korea is the hardest state to understand due to its separation from the international community. All cyber proxies attributed to North Korea must be considered with a critical eye due to the pervasiveness of the state within civil society. Nevertheless, some indications that using a cyber proxy strategy would mimic historic tactics.

---

[167] Ellen Nakashima, 'Russian Hacker Group Exploits Satellites to Steal Data, Hide Tracks', *Washington Post*, 9 September 2015.
[168] One of the indicators of sophistication are the use of zero-day exploits which are vulnerabilities that are unknown to those intending to protect the system upon which the vulnerability exits. Zero-days are rare and hard to discover. Jai Vijayan, 'APT28, Turla Nation-State Groups Deployed Multiple 0Days in Recent Attacks', *Dark Reading*, 5 November 2017.
[169] 'Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments', *Symantec*, 20 June 2019; 'NSA and NCSC Release Joint Advisory on Turla Group Activity', *US Cybersecurity & Infrastructure Security Agency*, 21 October 2019.
[170] False Flags in cyber operations are efforts taken to deceive victims and cause misattribution. Helen Warrell and Henry Foy, 'Russian Cyberattack Unit "Masqueraded" as Iranian Hackers, UK Says', *Financial Times*, 21 October 2019.

According to a report published by Center for Strategy and International Studies (CSIS), North Korea has long relied upon asymmetric strategies, constantly engaging in provocations that fall "outside…the framework of traditional military activity" but are still effective in causing disruption.[171] Cyber operations, particularly those conducted through proxies, would provide another avenue through which to exercise their asymmetric strategy.

Since the 1990s, North Korea has significantly invested in its cyber capabilities.[172] Furthermore, an alleged restructuring of the North Korean security apparatus in 2009 led to the creation of the General Reconnaissance Bureau, (RGB) - the primary state-cyber command-assisted by the General Staff Department (GSD). Despite this restructuring effort, the "organizational distinction between cybercrime, espionage and offensive operations are not clear-cut in North Korea"[173]

Whilst North Korea has not benefited from reliance upon readily available underground hacker communities, that does not mean that North Korea is lacking in cyber activity. Rather, it appears to leverage relationships with external actors to achieve strategic ends. According to Recorded Future's Insikt Group, "North Korea is not using territorial resources to conduct cyber operations and most North Korean state-sponsored activity is likely perpetrated from abroad."[174] Historically, North Korea supplemented its national economy through international organized criminal networks that generate illicit

[171] Jenny Jun, Scott LaFoy, and Ethan Sohn, 'North Korea's Cyber Operations: Strategy and Responses', *Center for Strategic and International Studies (CSIS)*, December 2015, 12.
[172] Ibid, 19.
[173] Ibid, 56.
[174] Insikt Group, 'North Korea Cyber Activity', *Recorded Future*, 15 June 2017, 17.

income for the country.[175] The US Director of National Intelligence Worldwide Threat Assessment claims that North Korea conducted cyber-heists, siphoning "$1.1 billion from financial institutions around the world."[176] According to Dmitri Alperovitch, CEO of Crowdstrike, North Korea uses cybercrime "to fill in the gaps in budgets at … [government] agencies."[177] Such a trend indicates that North Korea is using tactics consistent with income-generating operations of the past.

Although most of the cyber operations from North Korea appear financially motivated, evidenced by cyber-attacks on SWIFT banking communication systems, [178] 2014 saw a shift in its strategy towards the US. There have also been attacks that appear to take on a more disruptive and destructive approach. The Lazarus Group, an APT widely known by the threat intelligence community, is a suspected state-sponsored group. It appears to be an umbrella organization that has a wide mandate in carrying out attacks that are both financial and political. In 2014, Lazarus was accused of deleting, stealing, and publishing sensitive internal company data and communications of Sony Entertainment that eventually led to the pulling of the satirical film, "The Interview." Whilst it is still unclear if this hack was the work of the North Korean government or a sponsored-proxy, the Korean Central News Agency (KCNA) called the operation a

[175] Sheena Chestnut, 'Illicit Activity and Proliferation: North Korean Smuggling Networks', *International Security* 32, no. 1 (2007): 80–111, 84.
[176] Coats, 'Worldwide Threat Assessment of the US Intelligence Community 2019', 6.
[177] Samantha F. Ravich et al., 'Cyber-Enabled Economic Warfare: CEEW Threats from Iran and North Korea' (The Foundation for Defense of Democracies Conference on Cyber-Enabled Economic Warfare, Washington, D.C., 13 November 2018), 7.
[178] Insikt Group, 'North Korea Cyber Activity', 7.

"righteous deed", indicating North Korea's willingness to turn a blind eye to non-state actors that work in favor of the regime's interests.[179]

North Korea's capabilities appear to have enhanced rapidly. Only three years after the Sony Hack, the UK's National Health Service (NHS) was crippled by the North Korean attributed WannaCry attacks.[180] By 2019, the US Department of the Treasury had announced sanctions upon three "North Korean state-sponsored malicious cyber groups" that conducted pervasive attacks upon "critical infrastructure."[181] According to the Treasury announcement, the three groups Lazarus Group, Bluerunoff, and Andariel are "controlled" by the RGB and working, in part, for financial gain.[182] The decision of the US to sanction these groups as separate entities rather than just targeting the RGB directly may indicate some semblance of delegated authority. As North Korea develops and cyber talent increases, its cyber proxy strategy may mimic those of China, Russia, and Iran and further shift towards more disruptive or destructive attacks.[183]

3.5 Iran and its Struggle for Influence and Ideological Alignment

Iran is relatively new to the cyber offensive actor space in comparison to Russia and China. Nevertheless, according to the U.S. Army's Strategic Studies Institute, since

[179] Kahyun Yang and Jim Finkle, 'North Korea Says Its Supporters May Be behind Sony Attack', Reuters, 12 June 2014.
[180] Matthew Field, 'WannaCry Cyber Attack Cost the NHS £92m as 19,000 Appointments Cancelled', *The Telegraph*, 11 October 2018.
[181] 'Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups', *U.S. Department of the Treasury*, 13 September 2019.
[182] "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups."
[183] Mark Ciluffo, director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security, argues that the Sony attack is an indication that North Korea has the intent to move beyond just financially-motivated attacks. Samantha F. Ravich et al., 'Cyber-Enabled Economic Warfare: CEEW Threats from Iran and North Korea', 9.

late 2011, Iran invested heavily in its cyber-infrastructure with approximately "$1 billion dollars…[towards building] cyber technology, infrastructure, and expertise."[184] Although Iran does not possess the same level of technological sophistication as Russia and China, it displays a high degree of confidence in its cyber capabilities.[185] Iran started heavy development of its hacking abilities in 2009 at the height of the "Green Revolution."[186] Since then it has established a tiered approach to its cyber operations, spearheaded by three main state entities; the Iranian Revolutionary Guard Corps (IRGC), the Basij (state recognized volunteers), and Iran's Passive Defense Organization (NPDO).[187] Whilst the latter is primarily focused on cyber defense, the two former are believed to engage in more aggressive operations. The IRGC – evaluated as Iran's Cyber Command[188] - reportedly onboarded approximately " 120,000 [extra] personnel" from 2009-2012.[189] Basij is subordinate to the direction of the IRGC and their use within the state recognized ecosystem of cyber actors, demonstrates Tehran's policy of outsourcing executory power, whilst also controlling threat actors within their borders.

These initiatives indicate a willingness on behalf of Iran to professionalize and institutionalize their cyber talent into a central command. However, there is also evidence that they supplement their capabilities through the use of cyber proxies both from old proxy links and newly established groups. For example the relationship between Iran and the UN-designated terrorist group, Hezbollah, is well-documented. According to

---

[184] Brunner, 'Iran Has Built an Army of Cyber-Proxies', *The Tower*, no. 29 (August 2015).
[185] Collin Anderson and Karim Sadjadpour, 'Iran's Cyber Threat: Espionage, Sabotage and Revenge' (Carnegie Endowment for International Peace, 2018), 13.
[186] James Andrew Lewis, 'Iran and Cyber Power', *Center for Strategic and International Studies (CSIS)*, 25 July 2019.
[187] Ibid.
[188] Ibid.
[189] Jordan Brunner, 'Iran Has Built an Army of Cyber-Proxies'.

Counterterrorism Ambassador to the State Department, Nathan Sales, "Iran provides Hezbollah…some $700 million a year."[190] Whilst, traditionally Hezbollah has relied on physical attacks, in 2015 Check Point, an Israeli cybersecurity firm, uncovered a global cyberespionage campaign with possible ties to a Lebanese Political group. This was assessed through a combined technical and contextual analysis of the operation that saw "some of the [command and control]…servers hosted in Lebanon" and language analysis of file formats within the malicious files detected the use of Lebanese Arabic.[191] Subsequent news reporting on the campaign suggested a possible Hezbollah-link, although this was not confirmed by Check Point itself or any government statements. [192]

However, perhaps due to Iran's concerted investment towards its cyberinfrastructure and education, there appears to be a shift towards organically-grown, non-state cyber actors.[193] The structure between non-state and state appears more formalized and monitored than in other nations. A report by Recorded Future stated that Iran relies upon a formal, "tiered approach, whereby an ideologically and politically trusted group of middle managers translate intelligence priorities into segmented cyber tasks which are then bid out to multiple contractors."[194] It follows that cyber proxies may demonstrate specificity in their activity and highly organized approaches. For example, in 2018, the DoJ charged nine Iranian individuals belonging to an Iran private company called "The Mabna Institute" for their role in an extensive hacking campaign against

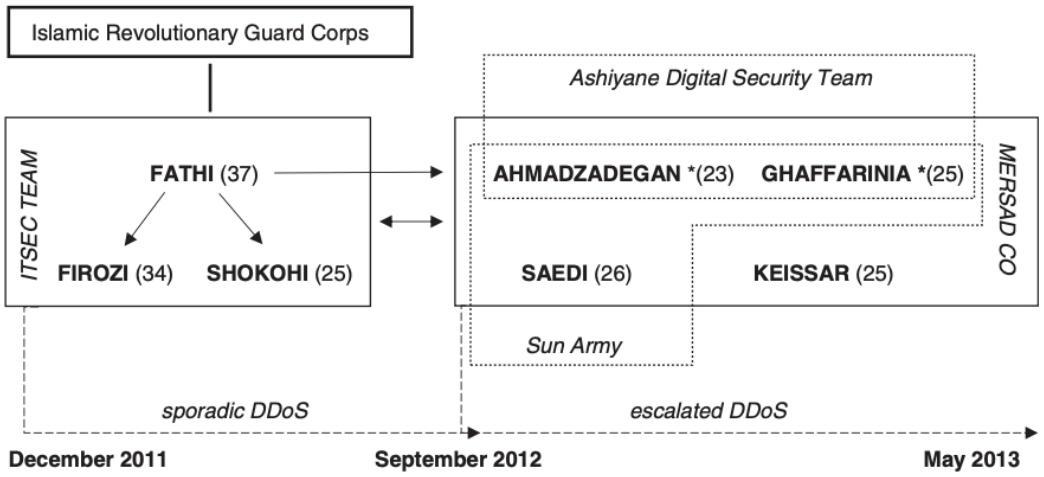
[190] Nathan Sales, 'Tehran's International Targets: Assessing Iranian Terror Sponsorship', *The Washington Institute*, 11 December 2018.
[191] 'New Data: Volatile Cedar Malware Campaign', *Check Point Blog,* 2015.
[192] Jeff Moskowitz, 'Cyberattack Tied to Hezbollah Ups the Ante for Israel's Digital Defenses', *The Christian Science Monitor*, 6 January 2015.
[193] 'Internet Penetration Rate in Iran Highest among Students: Report', *Tehran Times*, 29 June 2019.
[194] Levi Gundert, Sanil Chohan, and Greg Lesnewich, 'Iran's Hacker Hierarchy Exposed' (Recorded Future, 5 September 2018).

multiple academic institutions and private companies. The indictment directly cites the individuals as "leaders, contractors, associates, hackers-for-hire or affiliates of the Mabna Institute, an Iran-based company", working at the behest of the IRGC.[195] The clear motive from these attacks was to steal IP and research that would aid with Iran's domestic development. It was telling that the attack targeted "generally prominent research, technical, or medical universities," suggesting a targeted strategy, indicative of state involvement and planning.[196]

Iran seems to rely heavily on cyber proxies for obscuring the origin of an attack. The government "compartmentalizes" through outsourcing various tasks along the supply chain to multiple proxies, such that the non-state entity that launches the attack, might be distinct from the one that developed it.[197] Indeed, Iran also benefits from its organically developed hacker communities within Iranian security forums that serve as talent pipelines for state-proxy relationships. Tim Maurer examines in-depth the nature of the cyber proxy relationships within Iran. Using the US indictment of seven non-state Iranian hackers, Maurer explains how Iran has employed cyber proxy talent found within its domestic hacker forums. (Figure 3.3)

[195] Department of Justice, 'Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps', *Office of Public Affairs* (2018).
[196] Crane Hassold, 'Silent Librarian: More to the Story of the Iranian Mabna Institute Indictment', *Phishlabs*, 26 March 2018.
[197] Gundert, Chohan, and Lesnewich, "Iran's Hacker Hierarchy Exposed."

Figure 3.3: "Organizational structure and timeline of hackers mentioned in US indictment in 2016 of seven Iranian hackers."[198]



Source: Tim Mauer, Cyber Mercenaries, Cambridge University Press (2018), 86

The chart above describes how the two private companies, the ITSec Team, and the Mersad Group, worked concurrently to achieve the objectives of the IRGC. The groups conducted extensive DDoS (Distributed Denial-of-Service) attacks "against US financial institutions and other corporations in the financial sector", disrupting services and causing millions in remediation costs.[199] There are a number of aspects to focus on. First, Maurer's structure appears to reflect reports claiming that Iran uses "middle managers". Although the ITSec Team may not be the official middle man facilitating the relationship between the IRCG and its proxies, Mauer's mapping demonstrates a hierarchical structure. The ITSec Team exhibits more direct access to the IRGC and is further tasked with delegation to Mersad. Secondly, Mersad consists of members from established cybercriminal groups, the Sun Army, and the Ashiyane Digital Security Team, indicating that these underground cyber groups serve as a viable talent pipeline.

[198] Maurer, *Cyber Mercenaries, 86*.
[199] Department of Justice, 'United States of America v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, Omid Ghaffarinia, Sina Keissar, and Nader Saedi, Defendents.', *United States District Court Southern District of New York*, March 24, 2016, 3.

According to the indictment, the Ashiyane Digital Security Team "has publicly claimed to perform computer hacking work on behalf of the Government of Iran."[200]

3.6 Conclusion

As discussed, China, Russia, Iran, and North Korea all have some central cyber capabilities but they also appear to utilize cyber proxies. China stands out as a nation that is attempting to institutionalize its cyber proxies and, even Iran's formalized structure – mimicking contracting – shows a desire to control and direct hacker communities. Russia by comparison, demonstrates its use of cyber proxies along the relationship spectrum, using individual hackers and groups. Furthermore, the use of established hacker groups as cyber proxies further introduces risks as once personally motivated entities begin to partially serve national interest goals. Despite their developing central capabilities and the risks posed, why do states elect to use them? In the next chapter, I will analyze my four hypotheses, providing an empirical analysis of available evidence.

[200] Ibid, 10.

Chapter 4. Cost, Plausible Deniability, Skills and Specializations, and Risk Management

4.1 Exploring the Framework

Within the context of the available data, I explore the rationale for cyber proxy use within China, Russia, Iran, and North Korea. Due to data constraints, I expect that future researchers may find variation in the strength of these explanations among these four states, particularly as they are not homogenous entities. Therefore, much of my analysis will focus on what we should expect to see if such hypotheses were valid. I also expect that no one explanation is sufficient to answer the question, but rather they complement one another .

Three variables have historically been used to understand the state use of proxies in the physical space, which one can see parallels in the limited literature on cyber proxies. These are:

1. Economic costs
2. Plausible Deniability
3. Skills and Specializations

These variables result in four hypotheses:

1. States use cyber proxies to reduce economic costs.
2. States use cyber proxies in order to obtain enhanced plausible deniability benefits.
3. States use cyber proxies to incorporate and make use of skills and specializations that national cyber agencies are not privileged to
4. States will be motivated to use cyber proxies when they have adequate punitive power to threaten misbehavior

In this chapter I will look at each of these hypotheses in turn and provide empirical data to suggest whether these hypotheses motivate cyber proxy use

4.2 Cost

As discussed in the literature review, cost is a key component that drives the use of physical state-sponsored proxies. This trend is not new. Since the birth of privateering and the surge in private-public partnerships, the use of outsourcing within the government sector is an increasingly attractive prospect. There is significant rhetoric around outsourcing cyber capacities and development to the private sector even within the United States. Cost and efficiency appear connected to outsourcing. As costs are usually higher through internal development, the ability to update continuously, in the presence of budget restrictions and reviews, becomes increasingly limited. The US itself has increased its defense contracting budgets annually, with a large proportion focused on "professional engineering/technical" services.[201] Furthermore, the private sector lures highly qualified technical experts away from government agencies.[202] However, simply outsourcing development, whilst a critical component, does not actually address the question as I have defined it. My question seeks to ask why delegating the launch and execution of a cyber operation to a proxy is preferable to state agents. For economic cost to be a driver, either there must be a significantly higher marginal cost of launching and continuing the operation at the hands of a government agent, or a higher economic punishment cost if a government agent is directly linked.

[201] 'A Snapshot: Government-Wide Contracting', *GAO*, 2018.
[202] Martin C. Libicki, David Senty, and Julia Pollak, 'Upper-Tier Cybersecurity Professionals and Policy Options', in *Hackers Wanted* (RAND Corporations, 2014) , 57.

The following sub-hypotheses follow:

a) Using a government agency is more costly than using a proxy.

b) Using a government agency is less costly (or equal to) than using a proxy.

This thesis does not examine the use of proxies for the creation of exploits themselves but rather focuses on the operational costs of conducting the cyber operation, and the potential costs incurred if the victim discovers the source.

4.2.1 Operational costs

Operational costs for cyber operations can be broken down into three distinct parts:

1. Setup – The necessary reconnaissance and technical assets required before leveraging a cyber operation.
2. Action – Delivery of a cyber operation with malicious intent onto target networks.
3. Persistence – sustained presence on an adversary's network and successful continuation of the operation, without detection or removal, until the goal is reached.

These elements vary depending on the objective. For example, setup costs for hardened targets are likely greater due to the need for more thorough information about the networks in question. However, the expense of cyber operations is difficult to ascertain because, beyond technical assets, costs, such as salaries, are likely to change depending on the country of origin. As all sectors wise up to cyber threats and begin to invest in cybersecurity protections, attackers must now contend with increasingly

sophisticated cyber defenses.[203] Therefore maintaining a presence on a network (persistence) is a key area where costs can ramp up. The coordination between state and non-state entities in cyber operations have resulted in the emergence of diverse supply chains that all need to maintain their function for the mission to succeed.[204] Due to limited data, I focus this section on one particular cyber operation attributed to Russia in 2018. Using a similar methodology to examine the Russia case, I examine operational cost issues in China through understanding wage comparisons between the private and public sectors. The indictment for the first time was able to detail some of these operational costs, shouldered by proxies, as mentioned above.

Project Lakhta

Project Lakhta – detailed in a criminal complaint against an accountant, Elena Alekseevna Khusyaynova – was a Russian-origin influence campaign deployed on US social media networks.[205] The campaign consisted of multiple parts and supply chains to obtain the objective of spreading "distrust towards candidates [running] for political office and the political system in general."[206] The DoJ complaint identifies twelve distinct Russian entities that appear to be non-state, which assisted with influence campaigns from 2014 until 2018. Methods included timed posts, content creation, fake personas and the creation of Facebook events to promote protest rallies.[207]

---

[203] 'M-Trends 2020', *FireEye Mandiant Services*, 2019, 11.
[204] 'Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations', *Booz Allen Hamilton*, 2020, 39.
[205] Department of Justice, 'United States of America v. Elena Alekeevna Khusyaynova, Defendant.', United States District Court for the Eastern District of Virginia: Alexandria Division (2018), 4.
[206] Ibid.
[207] Renee DiResta, Jonathan Albright, and Ben Johnson, "The Tactics & Tropes of the Internet Research Agency," *New Knowledge*, 2019.

These operations were assisted through funding channels originating from a private sector company, Concord Management and Consulting LLC, and its subsidiary Concord Catering. Project Lakhta displays all of the three key operational costs that tie to the categories mentioned. The affidavit detailing the financial statements of Project Lakhta indicate:

- The use of multiple proxy agents that needed to be paid for the strategic goal of the operation to materialize.[208]
- Preparatory work costs in the form of setting up and building the notoriety of online personas
- A multi-year campaign with persistent engagement

The use of so many different proxy agents in propagating fake news, posing as legitimate actors, to influence the 2016 election was a necessary component to systemically impact the political environment within the US.

The affidavit indicates that very little of the budget appears to be spent on purchasing the technical assets required to leverage the influence campaign. From January-June 2018, only 0.84% of the total budget was spent on advertisements on Instagram and Facebook, and "bloggers and developing accounts on Twitter."[209] (Figure 4.1) Six other remaining potential costs are not explicitly associated with a dollar value. I determine five of these remaining charges to be fixed costs, such that they would not significantly increase or decrease whether they are purchased by a government agent or a proxy agent. (Figure 4.2) The last expense is administrative, a group term which is likely

[208] According to the indictment, activities were "obscured by operating through" twelve, named Russian entities. Department of Justice, United States of Amerca v. Elena Alekeevna Khusyaynova, Defendent.
[209] Department of Justice, United States of Amerca v. Elena Alekeevna Khusyaynova, Defendant, 9.

to include salaries and less variable costs, such as utility expenses. As a result administrative expenses constitutes the only potential variable cost. Figure 4.1 and Figure 4.2 combined suggest that administrative costs, due to personnel salaries, may comprise the majority of the January-June 2018 estimated $10,000,000 budget.

Figure 4.1: Expenses explicitly addressed in the DoJ indictment of ELENA ALEKSEEVNA KHUSYAYNOVA from January-June 2018[210]

Expenditures (Jan-June, 2018)		
	US Dollars (000s)	**% of the total budget in 2018**
Advertisements on Facebook	**60**	**0.60%**
Advertisements on Instagram	**6**	**0.06%**
"bloggers" and "developing accounts" on Twitter	**18**	**0.18%**
Total Accounted costs	**84**	**0.84%**
Unaccounted costs	**9,916**	**99.16%**
Total Budget	**10,000**	**100%**

[210] Department of Justice, United States of Amerca v. Elena Alekeevna Khusyaynova, Defendant, 10-13.

Figure 4.2: Expenses without numerical value explicitly mentioned the DoJ indictment of ELENA ALEKSEEVNA KHUSYAYNOVA from January-June 2018[211]

Unaccounted costs	Fixed or Variable?
Registration of domain names	Fixed
Purchase of proxy servers	Fixed
Purchasing posts for social networks	Fixed
Promoting news postings on social networks	Fixed
Social media optimization software (Twidium, Novapress)	Fixed
Administrative costs	Variable

If using proxies in Project Lakhta was motivated by cost, we would expect that state personnel costs would be higher than utilizing one of these non-state groups. According to the Mueller indictment,[212] workers at the IRA were "making nearly double the average Russian's salary."[213] According to two former IRA employees, they were able to earn $1,000 monthly from working with the most "prestigious wing" of the company.[214] Moscow's Federal Reporting Agency, Rosstat, that claims "the average federal civil servant salary" was around approximately $2,080/month in 2018.[215] An average civil servant salary appears to circa 50% higher than an estimated IRA salary. Whilst it is unclear whether a federal civil servant salary compares to cyber operatives within the GRU, it does indicate that government sector jobs are reasonably well-paid in Russia. Therefore, it may be possible that Russia uses proxies for their cheaper workforce supply, and insourcing them would thus increase the marginal cost of a project.

[211] Ibid, 9
[212] The Mueller Indictment was the lengthy investigation conducted as a result of Russian interference in to the 2016 US Presidential Election.
[213] Krishnadev Calamur, 'What Is the Internet Research Agency?', *The Atlantic*, 16 February 2018.
[214] "Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interferance in the 2016 U.S. Election," *116th Congress Senate* Report 116-XX (n.d.), 26.
[215] 'Russian Civil Servant Salaries To Increase for First Time Since 2013', *The Moscow Times*, 13 December 2017.

The above analysis is contingent on two confounding variables both relating to the type of mission conducted, and the employment structure of the sponsoring state. Project Lakhta was successful due to the amount of manufactured information pervading into US mainstream media. To do this however, Project Lakhta sought the services of twelve distinct Russian non-state entities all of which had designated tasks.[216]

However, it appears that in operations where fewer personnel are required, Russia does not always use proxies. In 2016, the Democratic National Committee (DNC) was subject to a collection of embarrassing email leaks as a result of intrusions by APT28.[217] APT28 was attributed to a collection of GRU agents in July 2018. In an indictment as a result of the Mueller investigation, the US accused twelve GRU agents of unauthorized hacking into protected US computers to steal information on candidates in the 2016 Presidential election, and their subsequent public release.[218] The indictment details the responsibilities and actions of the twelve agents that worked in tandem to execute the mission. There are a number of similarities between the Project Lakhta campaign and the DNC hack:

1) Both had the same strategic goal of attempting to influence political discourse within the US in connection to the 2016 elections.

[216] According to the Indictment, to "effectively manage such a large-scale operation, [each group] was headed by a management group and organized into departments, including a design and graphics department, an analysts department, a search-engine optimization ("SEO") department, an information-technology ("IT") department, and a finance department." Department of Justice, United States of Amerca v. Elena Alekeevna Khusyaynova, Defendent.
[217] Department of Justice, 'United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleskey Alesandrovich Potemkin, and Anatoliy Sergeyevich Kovalev, Defenandts.'
[218] Alex Ward, 'Read: Mueller Indictment against 12 Russian Spies for DNC Hack', *Vox*, 13 July 2018.

2) Both relied on influence campaign-type operations into order to achieve that goal.

The differences between the two operations were:

1) The DNC operation had a shorter time scale – Project Lakhta was conducted from 2014-2018, whilst the DNC hack occurred within a one year period.
2) The DNC operation was targeted whilst Project Lakhta was not.
3) The DNC hack required some technical skill whilst Project Lakhta utilized open-source tools.

As both Project Lakhta and the 2016 DNC Hack occurred within similar time frames, it suggests that the Russian state is actively delegating certain operations to proxies, whilst keeping more targeted operations within the confines of state agencies. This indicates that:

a) Some operation types do not present cost savings, as existing internet resources need to be largely utilized to avoid redundant costs or,
b) The risks of using a cyber proxy in some operations outweigh this benefit. [219]

The DNC hack by comparison was more technically sophisticated, but also involved some similar tactics that the proxies of Project Lakhta employed. One of the proxies listed within Project Lakhta was the IRA. They were one of the non-state entities accused of conducting an influence campaign on major social media sites through establishing fake pages and accounts.[220] Similarly, the GRU agents accused of the DNC hack created

[219] This could be for a number of reasons particularly pertaining to mission backlash and agency slack as discussed in the literature review.
[220] Department of Justice, "United States of America v. Elena Alekseevna Khusyaynova, Defendant.", 7.

a fake persona by the name of Guccifer 2.0 whose activity was most prolific on Twitter.[221] This suggests that the GRU itself has some expertise in influence campaign-type activity and there was an overlap in skills required between the IRA and the GRU operation. A report to the House Senate Committee on Intelligence confirmed that the GRU "exploited social media platforms" for influence campaigns[222] This suggests that the GRU can conduct operations of this type utilizing their own skills. Therefore, it appears that the reason for outsourcing this operation was largely due to a resource constraint within the GRU.

If Russia were to internalize this workforce, it would have likely required such planning several years before the start of the campaign so as to account for the multiple administrative actions that are required in the onboarding of state personnel and an increase in personnel costs. Through internalizing a large force, such that was utilized in project Lakhta, budgets will need to increase thus creating larger fixed costs for the government, and a large workforce that is not necessarily always required for normal activities. Through outsourcing to proxies the government avoids two operational costs:

1) The set-up required in training and onboarding into the government sector.
2) High fixed personnel costs, circumvented through employing proxies on an as-needed basis variablizes the operational costs, particularly for large projects.

[221] Department of Justice, "United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleskey Alesandrovich Potemkin, and Anatoliy Sergeyevich Kovalev, Defendants", 12-17

[222] "Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interferance in the 2016 U.S. Election", 8.

China

However, it is not always the case that government sector jobs pay higher than private-sector jobs - it may be different across states. Although the Project Lakhta criminal complaint is the first open-source document to suggest costs of a foreign cyber operation, an analysis of other nation's salaries and attitudes towards government work may suggest whether the state will see similar cost savings from outsourcing to proxies.

China appears to have increased agency salaries since 2015.[223] However, a blog run by Brett Becker, assistant professor in computer science professor at University College Dublin, claims that Chinese computer science graduates can earn "5,452 yuan a month, half a year after graduation,"[224] representing the highest pay after graduation. Based on an article by the South China Morning Post, the lowest level civil servant salaries are circa 1,820 yuan per month in 2018[225] Using these figures as an example, there is approximately a 60% difference between public sector and private sector salaries, demonstrating an overall trend of higher wages in the private sector. If true, it does not appear that the government sector will be able to offer financial incentives to internalize its cyber capabilities. This is evidenced through the use of cyber militias, frequently composed of students whose enrollment in technical universities is conditional upon their participation. According to Lindsay, Ming Cheung, and Reveron, authors of a book discussing China's approach to cybersecurity, national policies of civil-military integration hope to "leverage civilian capabilities without the burden of bearing the full

[223] Phoebe Zhang, 'China's Civil Servants Find There Is a Price to Pay for Corruption-Busting Salary Boost', *South China Morning Post*, 19 April 2019.
[224] Brett Becker, "Computer Science in China: High Employment, Highest Satisfaction and Salaries," *CS0* (blog), May 24, 2017.
[225] Zhang, "China's Civil Servants Find There Is a Price to Pay for Corruption-Busting Salary Boost."

cost and without isolating the individuals from the arguably more dynamic private sector."[226] This indicates that in order for China to conduct large-scale, long-term campaigns such as Project Lakhta, they may be required to outsource in order to stay within bureaucratic resource constraints. Thus, the calculus of outsourcing is similar to Russia but can be evaluated from a different standpoint. In Russia salaries are potentially higher than in proxy entities and thus marginal cost savings are achieved by outsourcing. However, in China internalizing all its capabilities is infeasible without a significant rise in existing state personnel salaries, resulting in increased costs for future state-run projects.

Comparatively to Russia, China appears to place greater emphasis on controlling its hacker communities and bringing skills within its central military. According to the Congressional Research Service, the 2013 PLA Science of Military Strategy details three cyber forces:

> *"1) specialized military network warfare forces in the PLA, (2) PLA-authorized teams of network warfare specialists in government organizations, and (3) non-governmental forces that may be mobilized for network warfare operations."*[227]

Notably, two of the above forces focus on recruiting internal specialized forces, whereas only the third explicitly mentions "non-governmental forces" for the specific use of "network warfare operations." Whilst there is a significant amount of rhetoric surrounding IP theft from Chinese state-sponsored and non-state entities[228], this doctrine suggests that China prefers to employ an internal cyber force for "network warfare"

---

[226] Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford University Press, 2015), 193.
[227] Ian E. Rinehart, 'The Chinese Military: Overview and Issues for Congress', *The Congressional Research Service*, 24 March 2016.
[228] "How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World," *White House Office of Trade and Manufacturing Policy*, June 2018.

rather than relying on non-state actors.[229] As such, even their non-governmental actors may be under tight supervision and control by the state – matching previous analyses by Maurer and others of tightly controlled relationships between state and cyber proxies in China.

Conclusion

Based upon the analysis in this section, I conclude that operational costs may have been a motivating factor for the use of proxies, particularly in the case of Russia when conducting widespread and pervasive campaigns. China's resistance to insourcing can also be seen from the same perspective but from a different viewpoint. As private sectors salaries are likely to be higher, material insourcing would cause issues in controlling state budgets. However, as detailed from findings in hypothesis 3 (Section 4.4), another explanation for outsourcing larger operations could reflect different management structures across these states and their inability to flexibly respond to more complex requirements. For example, the DNC, as a targeted operation, perhaps did not require such an extensive chain of command or proliferation of activity as the influence campaign detailed within the Khusyaynova complaint. As a result, skills and specialization of cyber proxies may also prompt their use in such cases.

4.2.2 Economic Punishment Costs

Sanctions are frequently utilized by the US and its allies to respond to the activities of adversarial states and individuals. The threat of economic punishment may motivate the use of cyber proxies. If true, we should expect to see that using a cyber

[229] Kieran Richard Green, "People's War in Cyberspace: Using China's Civilian Economy in the Information Domain," *Military Cyber Affairs* 2, no. 1 (2016), 8.

proxy incurs less economic cost to a state than if the operation were directly attributed to a state agent.

Two sub-hypotheses emerge as a result:

a) The use of proxies lowers the risk of incurring punitive economic costs compared to using government agents.
b) The use of proxies increases the risk (or is equal to) of incurring punitive economic costs compared to using government agents.

To understand if punitive action would create greater economic cost if the state itself were to launch the attack rather than a proxy, it may be useful to analyze the sanctions that have occurred in connection to cyber operations by these four states.

Sanctions and Cyber Operations

Sanctions are mainly utilized to force changes in behavior and invoke punishments to adversarial actors without military escalation.[230] In the case of Iran and North Korea where wholescale country sanctions were invoked for non cyber-related activities, cyber operations are used both as an asymmetric threat to militarily stronger nations, and to counter punitive economic impacts of sanctions.[231] According to Priscilla Moriuchi, a former National Security Agency analyst, North Korea has created a method to "move large amounts of money around the world, and do it in a way which [the US] sanctions do not touch."[232] In the case of Russia and China, US sanctions have not been

[230] David A. Baldwin, 'The Sanctions Debate and the Logic of Choice', *International Security* 24, no. 3 (2000 1999): 80–107, 86; T. Clifton Morgan and Valerie L. Schwebach, 'Fools Suffer Gladly: The Use of Economic Sanctions in International Crises', *International Studies Quarterly* 41, no. 1 (March 1997): 27–50, 29; Robert A. Pape, 'Why Economic Sanctions Do Not Work', *International Security* 22, no. 2 (1997): 90–136, 93-94.
[231] David E. Sanger, 'North Korea's Internet Use Surges, Thwarting Sanctions and Fueling Theft', *The New York Times*, 9 February 2020.
[232] Ibid.

as pervasive and focus on specific individuals or entities.[233] This section seeks to answer whether cyber proxies helps states avoid the economic costs posed by sanction. If cyber proxies do reduce the likelihood of incurring economic punishment costs, we should see that using state cyber agents results in sanction implementation more often than cyber proxy use.

To evaluate this, I consult a dataset produced by the Foundation for Defense of Democracies (FDD) that tracks "cyber-related" sanctions and indictments from 2013 to early 2020.[234]

[233] 'US Sanctions on Russia', 17 January 2020, 57; 'China: Economic Sanctions', *Conressional Research Service*, 22 August 2016, 11-31.
[234] Trevor Logan and Pavak Patel, 'Data Visualization: U.S. Sanctions Against Malicious Cyber Actors', *Foundation for Defense of Democracies*, 20 April 2020.

The Difference between Sanctions and Indictments

Economic sanctions are executed by US Department of the Treasury Office of Foreign Assets (OFAC). They are administered at the request of decisions made within the executive and legislative branches, responding to a perceived threat to US national interests by an external entity. The President usually will issue an Executive Order that then gives the Treasury the power to invoke sanctions upon foreign nationals, entities and governments. In doing so, it prevents US nationals and entities from trading and commerce with the sanctioned entity. (Masters, 2019) The Treasury also invokes "secondary sanctions" whereby sanctions are used as a threat against third party actors to prevent other nations from trading with the primary target of the sanction. For example, the US Countering America's Adversaries Through Sanctions Act (CAASTA) of 2017 allows OFAC to administer sanctions on non-US entities who engage in activities detailed within the Act. Cyber-related offenses have caused the US to invoke sanctions on entites suspected of complicity in these incidences. (Sultoon & Walker, 2019)

Indictments are different in that they are criminal accusations that are conducted by the US Department of Justice. The ability to indict an individual is based within concepts of legality and due process that require a level of admissible evidence so that a grand jury determines "probable cause." (FindLaw, 2019) "Probable cause" must come from a presentation of "specific facts and circumstances" that would "lead a reasonable person to believe that that the suspect has committed, is committing, or is about to commit a crime." (FindLaw, 2019)Indictments in relation to foreign nationals communicate that there is reasonable suspicion that they have violated US law. If the foreign nationals indicted step into US territory or into nations with bilateral extradition treaties with the US, they will risk being formally tried within US courts and potentially sentenced for their crimes.

The two methods are punishments for undesired behaviour. Both, to varying degrees, also communicate deterrent threats in attempts to prevent the reoccurrence of similar activity.[235] Although separate mechanisms, leveraged by different US bodies, intuitively you would expect that if you are able to indict an individual, you could also sanction them – thus enhancing the punishment. You cannot always indict those you sanction as

[235] The effectiveness of sanctions in this regard is disputed. See: Robert A. Pape, "Why Economic Sanctions Do Not Work*", International Security* 22, no.2: 90-136 (1997); Richard N. Haass, "Sanctioning Madness", *Council on Foreign Relations* 76, no. 6: 74-85 (Nov-Dec 1997).

sanctions can be against groups or organizations, whereas indictments are always against individuals. Furthermore, there is usually a higher burden of proof required for an indictment.

As shown by Figure 4.3 sanctions and indictments are not applied consistently across these states by the US.[236]

Figure 4.3: Percentage of total within-nationality, cases included in the FDD cyber-related offenses dataset that resulted in an indictment or sanction from 2013 to February 2020.[237]

Nationality	% Indicted	% Sanctioned
China	100	5
Russia	60	67
Iran	76	91
North Korea	17	100

Source: Foundation for Defense of Democracies Cyber Operations Dataset

Figure 4.3 demonstrates that despite multiple indictments against Chinese individuals for cyber-related offenses, this does not necessarily translate into economic punishment impacts by the way of sanctions. This could be seen as surprising considering the amount of cyber-enabled IP theft from China as mentioned in Chapter 3. Whereas, North Korean cyber activity is always sanctioned, but receive less indictments. Although it is difficult to ascertain whether cyber proxies receive sanctions more or less than government agents based upon this dataset, it does suggest that discrepancies in sanction application is not due to cyber proxy use but rather based upon different treatment of each of these countries. In fact, it may suggest a path dependency. Sanctions have been

[236] Trevor Logan and Pavak Patel, 'Washington Uses Sanctions and Indictments Inconsistently When Combating Malicious Cyber Activity', *Foundation for Defense of Democracies*, 20 April 2020.
[237] Ibid.

expansively used against North Korea and Iran for many years and have shown material impacts upon their economies and restricted access to financial channels.[238] Whereas Washington has been more measured in its approach to Russia and more so China, perhaps in an effort to reduce the risk of "escalation or economic retaliation against American companies."[239]

The two cases in which Chinese nationals were sanctioned were in relation to money laundering for the North Korean-attributed group, Lazarus. The rest of the Chinese national cases included within the dataset were a mix of state and non-state actors (some of which were cyber proxies as identified within this thesis, for example Boyusec). There was nothing to suggest from this data that Chinese cyber proxies or state entities involved in cyber-related offenses against the US would be more or less likely to receive sanctions.

However, such insights may reflect political, intelligence and legal constraints more than clear patterns of sanction application. The fact that sanctions were utilized more widely in the case of North Korea does not necessarily reflect that state agencies or cyber proxies would receive sanctions more or less than one another, but rather a legacy of US sanction on North Korea as one of its primary methods to exert control. Furthermore, it may just be too early to tell if there is any difference between state agencies and cyber proxies. Out of six included North Korean cases, five received sanctions in 2018 or later despite significant North Korean-attributed cyber activity in

[238] The US uses "secondary sanctions" to reduce financial flows to and from Iran and North Korea. 'Iran Sanctions', *Congressional Research Service*, 14 April 2020; 'North Korea: Legislative Basis for U.S. Economic Sanctions', *Congressional Research Service*, 9 March 2020,.
[239] Logan and Patel, 'Washington Uses Sanctions and Indictments Inconsistently When Combating Malicious Cyber Activity'.

2014 (Sony Hack) and 2017 (WannaCry) – these numbers could either reflect a lagging sanctions process or a decline in insight. Lastly, when indictments are publicly announced, doing so may reveal US intelligence efforts, which would not be conducive to US strategic interests.

4.2.3 Conclusion

The evidence suggests that cyber proxies may be used for their operational cost benefits although there is no clear link with economic retribution costs. The latter is something that will need to be observed closely over time as data and attribution improves. However, current evidence does not show that the use of a cyber proxy is motivated by the prospect of differing economic retribution costs as demonstrated by the inconsistencies of US application of sanctions. Large operational costs appear to correlate with large personnel requirements, which may necessitate the use of third parties such as cyber proxies. The literature claiming that cyber-attacks are wars "on the cheap" is correct when assessing the technical abilities required, but it is the execution where costs rise. As influence campaigns become increasingly attractive forms of warfare, cyber proxies will likely continue to play a significant role.

4.3 Plausible Deniability

Linked to the threat of punitive actions is the concept of plausible deniability. Plausible deniability is exploited by states to proclaim innocence in the face of domestic and/or international audiences. This section focuses on plausible deniability in the presence of international audiences, utilized to obscure evidence for prosecutors of a

target country. Cyber proxies may represent a strategy through which to ensure plausible deniability and its benefits. If plausible deniability were a motivating factor for the use of cyber proxies, we should see that plausible deniability is feasible and that they achieve the benefits of it more than a state agency can.

4.3.1 Feasibility of Plausible Deniability

True plausible deniability would theoretically absolve the sponsoring state of responsibility for the cyber proxy's operation. However, advances in technical attribution combined with contextual intelligence have made true plausible deniability increasingly difficult to attain. The US has directly named the North Korean, Iranian, Chinese, and Russian governments as complicit or directly engaged in cyber offensives against the US.[240] Private cybersecurity companies have engaged in motivations analysis to conclude how certain cyber operations benefit states and continuously track the use of malicious exploits and payloads to ascertain the toolkits of certain APTs. The practice allows cybersecurity companies to assess, with varying levels of confidence, the likelihood of links between cyber proxies and state sponsors. US indictments can provide some color as to the level of visibility victims have into the operations of hackers. As stated by Lance Cottrell, a cybersecurity professional, "the amount of detail revealed in the [Mueller

[240] Coats, 'Worldwide Threat Assessment of the US Intelligence Community 2019.'

indictment of the 2016 DNC hacks] stunned me, and suggests that the US had very deep visibility into the hackers' operations."[241]

Furthermore, attempts to disguise the origin of attacks have not prevented consensus rhetoric around the true origin. Russian-based hacker group Turla has been known to conduct intrusions upon industries with a national security focus.[242] In 2019, a technical analysis report by the UK National Cybersecurity Center (NCSC) and US National Security Agency (NSA) concluded that Turla had acquired the known TTPs used by Iranian-based, government-linked group, OilRig.[243] Turla's actions are indicative of a false-flag operation, intended to mislead attribution efforts. The effort involved a "two-year probe by the UK's National Cyber Security Centre in collaboration with the US's National Security Agency."[244] Although this does indicate that attribution may not be able to keep pace with the ever-evolving nature of cyber operations, it does demonstrate that states cannot rely on attaining true plausible deniability.

4.3.2 Benefits of (im)plausible deniability

As mentioned in Chapter 2, plausible deniability does not appear to be a binary concept. Rather, it is a spectrum that starts at completely plausible deniability and ends at

[241] Lance Cottrell, 'The DNC Hacker Indictment: A Lesson in Failed Misattribution', 4 October 2018.
[242] Meyers, "Meet CrowdStrike's Adversary of the Month for March: VENOMOUS BEAR."
[243] 'Advisory: Turla Group Exploits Iranian APT to Expand Coverage of Victims', *NCSC and NSA*, 21 October 2019.
[244] Warrell and Foy, "Russian Cyberattack Unit 'Masqueraded' as Iranian Hackers, UK Says."

unacknowledged action. As stated by Rory Cormac and Richard Aldrich, "plausible deniability is a spectrum of attribution and exposure, since covert action has multiple audiences, both internal and external."[245] States that appear to have conducted cyber-attacks against the US have already been sanctioned and recognized on the world stage for their actions, yet they continue to either use state agents or proxies that have been connected to the central government. The use of false-flag operations, intended to mislead victims, indicates that there appears to be some benefit in obscuring the origin of cyber activities.

I examine in this section two intersecting (im)plausible deniability benefits that perhaps might motivate the use of proxies:

1. Reduced Legal Liability: If this is the case, cyber proxies should be subject to more ambiguous legal guidelines than states. Therefore, this would allow states to appear aligned to international conventions and bilateral treaties.
2. Reduced Conflict Escalation: If this is the case, cyber proxies would enhance plausible deniability benefits such as reducing the likelihood of direct conflict or escalation that these states may not be able to sustain.

Legal Liability

Internationally, there very little legal recourse to rely on. The Tallinn Manual is the current prevailing legal guidebook on the interaction between international law and cyber operations. Under such interpretation, election interference, even though network intrusion, would not be considered an act of war because it does not result in direct

[245] Cormac and Aldrich, 'Grey Is the New Black: Covert Action and Implausible Deniability', 479.

physical damage.[246] There are even disputes whether leaking documents to influence an election would flout the international law against interference in extraterritorial affairs.[247]

Secondly, attempts to build consensus on international norms governing cyberspace have been met with political one-upmanship and bureaucratic infighting. An example are the UN two groups established to address the application of international law to cyber operations, attempting to discern matters of state complicity. The UN Group of Governmental Experts (UNGGE) and the UN Open-Ended Working Group (OEWG) were established by the US and Russia respectively. As assessed by Alex Grisby, Assistant Director for the Digital and Cyberspace Policy program at the Council on Foreign Relations, Russia regarded the UNGGE as too exclusive as they failed to bring all nations into the conversation. The US, in contrast, regarded the OEWG as an attempt to restrict consensus agreement on norms.[248] Nevertheless, the UNGGE did state the explicitly grounded cyber proxies in international norms in 2013 and 2015 saying that "States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts."[249] However, as posited by Tim Maurer, no efforts were made to define what constitutes a proxy or where the lines of state complicity begin.[250]

---

[246] Ellen Nakashima, 'Russia's Apparent Meddling in U.S. Election Is Not an Act of War, Cyber Expert Says', *The Washington Post*, 7 February 2017.
[247] Anat Eisenstein Bar-On, 'The (Il)Legality of Interference in Elections under International Law', *The Federmann Cyber Security Research Center - Cyber Law Program*, 27 February 2019.
[248] Alex Grigsby, 'The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased', *Council on Foreign Relations*, 15 November 2018.
[249] "Report of the Group of Governmental Experts on the Developments in the Field of Information and Telecommunications in the Context of International Security" (UNGA, July 22, 2015).
[250] Tim Maurer, '"Proxies" and Cyberspace', *Journal of Conflict & Security Law* 21, no. 3 (2016): 383–403, 386.

Overall there does not appear to be any clear international consensus legal stipulation or consistent application of recourse that will account for influence campaigns or the chain of conspirators involved in unauthorized access to a protected computer. Although there is no clarity as to how cyber proxies are treated in international law, there is little legal clarity generally in issues of cyberwarfare. Therefore, avoiding legal liability does not adequately explain cyber proxy use as the norms are lacking whether the cyber operations are conducted by a state agent or a proxy agent. As a result, it does not appear that legal liability would increase or reduce in the presence of state or proxy agents.

Conflict Escalation

Cyber operations provide states which a method to threaten adversaries whilst avoiding conventional warfare. If a state can plausibly (or implausibly) deny their involvement in a cyber operation through the use of a proxy, conflict escalation is increasingly unlikely. Therefore, if a desire for plausible deniability benefits was a motivating factor, we would expect that using cyber proxies reduces the likelihood of conflict escalation.

Austin Carson's work on the use of covert action for minimizing conflict escalation discusses how states may use a "backstage" space to maintain the "illusion of a … limited war".[251] However, to achieve this the opponent state must also have an interest in upholding this illusion. The available data suggests that this is not always the case. Using The New York Times Archives and the US Department of Justice search function, I identified twenty-eight cases of alleged cyber proxy activity conducted on behalf of one

[251] Austin Carson, 'Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War', *International Organization* 70, no. 1 (Winter 2016): 103–31, 105.

of these four states between January 2010 until January 2020.[252] Whilst the data collected may be biased due to the focus on US-centric reporting, it shows an increased effort to name and shame activity connected to cyber proxies. Of the twenty-eight cases, I identify eleven as explicitly referencing a cyber proxy and its association with its sponsoring state. Of these eleven, six are referenced in official DoJ complaints or indictments. If the motivation behind using cyber proxies was to avoid conflict escalation, such explicit recognition on behalf of the United States would not foster the illusion of limited conflict.

In general, victim responses to cyber operations are largely defensive.[253] It appears that it is the lack of clarity around the cyber domain itself that limits escalation rather than the use of cyber proxies. This concept is emphasized in the 2018 Command Vision for US Cyber Command that state adversaries are aware of the US' "traditionally high threshold for response to adversary activity."[254] The use of the word "activity" indicates that there is a specific action that would provoke escalation rather than a specific actor. That is not to say that if the rules of cyber warfare were more clearly defined in the future that cyber proxies wouldn't become more attractive in this regard. However, with the current state of undefined thresholds, and lacking international norms and standards around cyber conflict, conflict escalation appears to be avoided regardless of whether attribution is direct to the state or a proxy. Therefore, using cyber proxies does not appear to provide any significant benefits in terms of conflict escalation.

---

[252] Note: Within each "case" it may either cite an incident or a responsible entity/individual. See Appendix 1 for cases considered, sources, and collection methodology.
[253] Note: Much of the activity in cyberspace is covert. It is possible that opaque, proportional responses within cyberspace do occur but public reporting is lacking. Martin C. Libicki, "Crisis and Escalation in Cyberspace", *RAND Corporation* (2012), 60. Libicki notes that "80 to 90 percent" of CYBERCOM's activity is defensive.
[254] "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command", *United States Cyber Command*, 20 April 2018, 3.

The escalation and legal benefits argument mostly focus on plausible deniability in the presence of external audiences. However, it could be possible that states use proxies to provide flexibility in the presence of potential domestic audience costs. These costs result from domestic opposition, either from electorates or institutional elites, deploring a public action or inaction taken by political leaders. This can produce weakening domestic support, resulting in leadership challenges or removal.[255] For example, if a GRU agent is directly indicted it may be harder to sell the message of innocence domestically. The separation is far less "plausible" when the accused is a member of the state apparatus. However, assessing whether using a cyber proxy reduces audience costs is outside the scope of this thesis. For future researchers, examining the extent of control over information and censorship within these four countries, along with a further understanding of the domestic perception of political leadership would indicate whether cyber proxies are beneficial in this manner.

4.3.3 Conclusion

There is not sufficient evidence to support that the use of cyber proxies enhances the benefits of plausible deniability. Although attribution is not perfect, true plausible deniability is not as feasible as it once was due to technical and contextual intelligence improvements as well as a lack of reciprocal acknowledgment, evidenced by an increase in the number of US indictments directly attaching non-state actors to their alleged state sponsors. Although proxies are still afforded some flexibility due to a lack of legal

[255] James D. Fearon, 'Domestic Political Audiences and the Escalation of International Disputes', 581-582; Kenneth A. Schultz, 'Looking for Audience Costs', *The Journal of Conflict Resolution* 45, no. 1 (February 2001): 32–60, 33.

definition, they do not appear to drive the lack of escalatory response that plausible deniability is often associated with. It is the domain itself that appear to provide this benefit. Of course, the data is limited by uncertainty over covert responses to cyber-attacks and lacking examination of domestic audience costs. Nevertheless, it appears that plausible deniability is not enhanced or reduced through the use of a cyber proxy.

4.4 Skills and Specializations

The third set of explanations for using cyber proxies focuses on the distinct value-add and skills that they provide sponsoring states. If skills and/or specializations were a distinct reason for using proxies, then we may expect to see several trends, including proxies carrying out longer and more sophisticated attacks - such as zero-days - and/or a low commitment to building an internal cyber workforce. Whilst numbers of offensive cyber government operatives are unclear, what is clear is that due to the dynamic nature of cyberwarfare, specialization and speed in offensive cyber operations may be particularly difficult to attain within the structure of government agencies.

Bureaucracy and overlapping functions can limit the ability of agencies to act flexibly and with speed. According to Amy Zegart's Spying Blind, a number of internal and external factors limit the ability of government agencies to respond adequately to emerging threats.[256] The public sector itself may not immediately have the relevant talent in-house to be able to achieve all desired outcomes, and whilst they could acquire it,

[256] Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton University Press, 2007), 52.

recruitment of such people into the state infrastructure would still involve a considerably longer processing time than selecting from a readily available private-sector force.

The ability of the private sector to specialize may prove the motivating variable. As mentioned earlier some types of operations require a larger operating and management structure. This takes up resources and time that are better managed within the large workforces of the private sector, who are specialized in conducting these operations. The IRA is labeled as a troll factory, thus their métier is trolling online and other activities pertaining to social media influence campaigns. Obtaining that degree of specificity within the government sector, keeping up with the dynamism of an influence campaign, all whilst being flexible enough to execute other governmental functions, is unlikely to provide the fastest route to efficiency.

In 2014, the DoJ announced an international effort and indictment against Russian hacker, Evgeniy Mikhailovich Bogachev. At the height of his activities, Bogachev was thought to have stolen "millions of dollars from numerous bank accounts" around the world and "millions of computers under his control."[257] A New York Times article claims that "Russian authorities were looking over his shoulder, searching the same computers for files and emails."[258] If this is true, then it suggests that Russia's native hacker community provides the states with efficiency, allowing them to use the intrusions already established by hackers rather than repeat the work. Tim Maurer argues that such a practice may continue, fueled by the fact that "the legitimate (technology) industry is not

[257] Department of Justice, 'United States of America v. Evgeniy Bogachev', *United States District Court for the Western District of Pennsylvania*, 19 May 2014, 5; Michael Schwirtz and Joseph Goldstein, 'Russian Espionage Piggybacks on a Cybercriminal's Hacking', *The New York Times*, 12 March 2017.
[258] Schwirtz and Goldstein, 'Russian Espionage Piggybacks on a Cybercriminal's Hacking'.

big enough to absorb all the labor."[259] However, what this does suggest is that perhaps it is operational ease, which would also result in cost savings, that motivates the use of cyber proxies. Such a practice is reliant upon a solid existing hacker force.

4.4.1 Case study: Iran

Iran has a long history of curating and building its relationships with physical proxies. According to Colin Clarke and Ariane Tabatabai, " Tehran has never been interested in cultivating a network of completely dependent proxies", preferring to help these groups "integrate into their countries' political processes and economic activities."[260] Such an approach does not seem to translate as neatly into cyberspace.

The buildup of significant cyber capabilities was, as argued by private cybersecurity firms, a response to the Stuxnet virus worm attack in 2001 that targeted the Natanz Nuclear facility.[261] As a result, Iran built out a large cyber-bureaucracy that according to the Congressional Research Service has nine official central agencies, one of which includes the Islamic Revolutionary Guard Corps (IRGC).

Wilfried Buchta's book, "Who Rules Iran", examines the governmental power hierarchies that exist within Iran. Within these hierarchies, he concludes that the Islamic IRGC - the agency that is believed to control many of Iran's offensive cyber operations today-"is among the most autonomous power centers in Iran, and… has resisted subordination to any civilian authority, from the presidential executive to the clerical

---

[259] Maurer, *Cyber Mercenaries*, 94.
[260] Colin P. Clarke and Ariane M. Tabatabai, "Iran's Proxies Are More Powerful Than Ever," RAND Corporation, *TheRANDblog* (blog), October 16, 2019, https://www.rand.org/blog/2019/10/irans-proxies-are-more-powerful-than-ever.html.
[261] "Iranian Offensive Cyber Attack Capabilities", *Congressional Research Service*, 13 January 2020.

control apparatus embodied in the supreme leader's representatives. Since the IRGC is not subject to any real political control, it can easily deploy against any perceived threat."[262] With such power, it suggests that the IRGC would have the ultimate flexibility to be able to act quickly. Although Batcha only examines the bureaucracy up until 2000, before the push to develop cyber-centric agencies occurred, the persistence of the IRGC as one of the most powerful unit has continued.[263]

Based upon the Congressional Research Service report, I further investigate the nine identified state cyber entities through a language analysis of cybersecurity firm reports, think tank analysis, and government agency statements. I demonstrate that there is overlap within these bodies in Iran today. (Figure 4.5)[264]

[262] Wilfried Buchta, *Who Rules Iran* (Washington DC: The Washington Institute for Near East Policy & Konrad Adenauer Stiftung, 2000), 70.
[263] Robin B. Wright, *The Iran Primer: Power, Politics, and U.S. Policy* (Washington DC: United States Institute of Peace Press, 2010), 59; According to Abbas Milani, the co-director of the Iran Democracy Project at Stanford University's Hoover Institution, "the I.R.G.C. now has the upper hand. Khamenei knows that without the I.R.G.C. he'd be out of a job in twenty-four hours." Dexter Filkins, 'The Twilight of the Iranian Revolution', *The New Yorker*, May 18, 2020.
[264] See: Appendix 2 for Language Analysis Methodology

Figure 4.5: Iranian State Cyber Agencies[265]

	Iran Cyber Police	Ministry of Intelligence and Security (MOIS)	Supreme Council of Cyberspace	National Cyberspace Center (NCC)	Islamic Revolutionary Guard Corps (IRCG)	IRGC Electronic Warfare and Cyber	Basij Cyber Council	National Passive Defense Organization (NPDO)	Cyber Defense Command
Internal focus	*	*	*	*	*	*	*	*	*
External focus		*			*		*		*
Offensive focus		*	*	*	*	*	*	*	*
Defensive focus	*		*	*		*		*	
Intelligence focus	*	*	*	*		*			
Executory focus					*		*	*	*
Policy focus			*					*	

[265] Farzin Nadimi, 'Iran's Passive Defense Organization: Another Target for Sanctions', *The Washington Institute*, 16 August 2018; 'Iran's Ministry of Intelligence and Security: A Profile', 16; 'Treasury Sanctions Iranian Organizations and Individuals Supporting Intelligence and Cyber Targeting of U.S. Persons'; 'Iran's Revolutionary Guards', *Council on Foreign Relations*, 6 May 2019; Insikt Group, 'Despite Infighting and Volatility, Iran Maintains Aggressive Cyber Operations Structure', 7; 'Iranian Offensive Cyber Attack Capabilities'.

As with most bureaucracies, multiple agencies with overlapping duties can result in competition and bottlenecks. The IRCG and the MOIS have a history of alleged competition, with some reports citing the execution of operations conducted to discredit the other.[266] [267] The threat from competing agencies (as depicted by Figure 4.5), may motivate state agencies to utilize cyber proxies to demonstrate efficiency to superiors and overcome bureaucratic constraints.

Furthermore, according to a report released by the Inskit Group, "there are over 50 estimated contractors vying for Iranian government-sponsored offensive cyber projects."[268] The report argues that the process for state-sponsored operations and the use of proxies is tightly controlled and methodological. Such an approach indicates that Iran isn't too concerned about covering its connections with its cyber proxies but rather prefers to benefit from the market forces that result in competition, which include specialization and high quality.[269] If true, it indicates that the skills and specializations of cyber proxies may explain why Iran uses them.

4.4.2 Conclusion

Through examining Iran as a case study, some evidence suggests that bureaucratic structures may encourage states to use cyber proxies for their unique skills and specializations. Although I rely heavily on Iran as a case study, there are similarities in particular with China and Russia. All have suffered allegations of corruption and Russia

[266] Insikt Group, "Despite Infighting and Volatility, Iran Maintains Aggressive Cyber Operations Structure", *Recorded Future*, 9 April 2020.
[267] 'Iran's Ministry of Intelligence and Security: A Profile' (Federal Research Division, Library of Congress, December 2012, 16.
[268] Gundert, Chohan, and Lesnewich, 'Iran's Hacker Hierarchy Exposed', 3.
[269] Ibid, 2.

has similar competition issues and overlap between its intelligence agencies.[270] In the presence of such challenges, cyber proxies provide an avenue through which to remedy the drawbacks of multifaceted bureaucracies.

4.5 Conclusion for Cost, Plausible Deniability, and Skills and Specialization hypotheses

So far in this chapter, I conclude that costs, and skills and specialization may provide some explanation for cyber proxy use, but there is not enough evidence to suggest that they enhance plausible deniability. As such, the historical literature for using proxies, does not seem to be sufficient to explain their use in the cyber context. However, confounding variables, such as type of mission, different employment structures, and distinct bureaucratic organizations, may cause variations among these states. In short, the evidence to date for whether plausible deniability benefits lead to cyber proxy use is inconclusive at best.

Having shown however that proxies might provide cheaper options and specialized skills for conducting offensive cyber operations, the following section will focus on trying to understand why some states are more willing to use proxies for these benefits when the price of mission backlash could undermine strategic goals. As I have shown in previous chapters, certain states – such as Russia – give their proxies a seemingly large degree of operational leeway. The following sections provides an analysis of the necessary conditions that must be in place to benefit from such a strategy.

[270] Mark Galeotti, 'The Spies Who Love Putin', *The Atlantic*, 17 January 2017.

4.6 Punitive Power: Assessing states' ability to threaten their proxy actors

The literature on principal-agent dilemmas explains how multiple risks can arise in such relationships, often facilitated through information asymmetries, leading to Adverse Selection and Agency Slack. This chapter attempts to explain why Russia, China, Iran, and North Korea are well positioned to control these unintended consequences with their use of cyber proxies.

Agency Slack or mission backlash is thought to occur due to numerous potential externalities including the presence of multiple competing principles, economic incentives as well as ideological misalignment. In the presence of incomplete information, states that use cyber proxies must rely on other coercive elements to ensure alignment. If a cyber proxy believes that there is a high probability of punishment, then it may create an optimal environment for a state to use cyber proxies with confidence. Thus, I hypothesize that states with a high level of punitive power are more likely to use cyber proxies.

There are nations who do have high levels of punitive power but likely do not use cyber proxies as defined in this thesis, such as the United States. However, to further examine the punitive power variable, I look within the four countries of focus. If this variable is a compelling driver, then we would expect states with a greater variety of cyber proxies, like Russia, to have the most punitive power.[271]

[271] The reasoning behind this is that as states utilize more types of cyber proxy – particularly loosely controlled ones- , the greater the risk of principle-agent problems occurring.

This chapter examines four types of punitive power and assesses to what extent these four countries wield each one. (Figure 4.6)

Figure 4.6: Matrix of sources of state punitive power with examples

	Formal	Informal
Internal	Travel Bans	Black Jails
External	Extradition Treaties	Extra-territorial Assassinations

This matrix builds loosely off a rich literature in political science about sources of strength and weakness of states power. In "Weak States in the International System", Handel lays out the "elements determining the strength of the state", which include domestic, external, informal, formal sources.[272] In doing so, Handel assessed which elements of strength were lacking within weak states and therefore their relative strength against others. Whilst this model is used to evaluate the position of weak states in the international system, it provides a framework to evaluate how states obtain power. The principal-agent framework (Chapter 2) also indicates how to prevent mission backlash.

There are a number of theories that assess how states may be able to control their agents. According to D. Roderick Kiewiet and Matthew McCubbins, agents will behave opportunistically "subject only to the constraints imposed by the relation with the principal."[273] Constraints can take many forms including limiting how much authority

[272] Michael Handel, *Weak States in the International System* (Psychology Press, 1990), 69.
[273] Kiewiet and McCubbins, *The Logic of Delegation*, 5.

they delegate to agents and utilizing multiple agents (Grant and Keohane, 2005), but can also take the form of enhanced monitoring mechanisms and deterrent threats, to encourage agents to behave. Assuming that states may experience proxy divergences even when delegation is limited, they must formulate either strong monitoring mechanisms over the agent, or pose credible threats for misbehavior. However, as discussed by McCubbins, monitoring mechanisms are often costly. (Kiewiet and McCubbins, 1991 and McCubbins and Schwartz, 1984) Furthermore, as posited by Bynman and Krebs, mechanisms of control may shift "the relationship from discretionary to instrumental", potentially "emblazon[ing] the state's fingerprints" upon the agent.[274] However, as some measures of control may be required, the ability of a state to present credible threats against their proxies could be measured by the ability to leverage punishments against them.

The credibility of the threat is measured through the sources of state strength as laid out by Handel. Whilst the coercive power is measured by deterrence, compellence, and incentives, I determine that deterrent threat is most readably available and least costly as there is no need to use it unless an agent misbehaves. To measure how credibly these states are in issuing deterrent threats, I look at sources of punitive power to understand whether there are trends that may suggest motivation to using cyber proxies.

Internal punitive power is the ability of a state to credibly threaten its proxies within their territorial boundaries, whilst external is that exercised extraterritorially. An example of internal power includes the use of travel bans and black jails, whilst external includes assassinations on foreign soils and extradition cases. External versus internal

[274] Byman and Kreps, 'Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism', 9.

punitive power can be easily conceptualized, however, formal versus informal punitive power proves more challenging. In Russia, China, Iran and North Korea, the lines between informal and formal power are particularly difficult to define. For this thesis, I define formal power as that which adheres to the rule of law, including measures taken by the state that are centrally acknowledged, including travel bans, the judicial system, etc. To assess informal power therefore, I looked at methods conducted extrajudicially with a large degree of clandestine activity. Although the public may be aware of such informal institutions, central messaging denies their existence or obfuscates the threat to the international community. An example is the "re-education camps" that the CCP (Chinese Communist Party) implemented to threaten its Uighur Muslim population.[275] Despite, multiple advocacy and rights groups detailing these camps as "extra-legal detention facilities [for those] who have not been lawfully charged, tried and convicted"[276], Chinese officials claim that these centers help individuals "improve their quality of life" after graduation.[277] Other examples include the use of non-state or quasi-state entities that engage in vigilante-type activity and secret police. Formal capability is more publicly recognized procedures and institutions that might be applied arbitrarily but are nonetheless not highly obfuscated. Examples include the legitimacy of the court system, its independence from the state, the existence of free and fair trials, proportional criminal sentencing, and formal treaties or international agreements. As noted by Patrick Köllner

[275] Nectar Gan and Mimi Lau, 'China Changes Law to Recognize "re-Education Camps" in Xinjiang', *South China Morning Post*, 10 October 2018.
[276] Nigel Walker, "China's Policy on Its Uighur Population," *House of Commons Library*, March 6, 2020.
[277] 'China Uighurs: Detainees "free" after "Graduating", Official Says', *BBC*, 9 December 2019.

in reference to the progression of informal power structures in China, these distinctions may change dependent on political leadership.[278]

4.6.1 Formal, Internal

I assess formal, internal punitive power through looking at the strength of the rule of law and separation between state and the judiciary. These concepts are not only measures of a robust and legitimate judicial system but also checks upon state power and political influence into criminal proceedings. When formal punitive power is high, states use the law arbitrarily without deference to due process. If punitive power explains the use of cyber proxies, we should expect to see that the indicators of formal, internal power are leveraged to benefit the state above the rule of law.

As all of these nations are authoritarian, "formal, internal" punitive power is high. A general absence of the rule of law ensures arbitrary interpretations, and a lack of separation between the judiciary and political leaders appears to result in politically motivated convictions and trials. According to the World Justice Project (WJP), out of 128 countries and a perfect score of 1, Iran, Russia, and China all scored low; 0.43, 0.47, and 0.48 respectively.[279] It should be noted that North Korea is not included in the index. Although Iran scored lowest in terms of rule of law, this seemed to be heavily influenced by very low scores in subfactors including "Open Government" and "Fundamental Rights". Russia scored lowest out of the three in "Constraints on Government Powers", "Absence of Corruption", and "Criminal Justice" This indicates that the judiciary is more subservient to the government within Russia than the other two countries and that the

[278] Patrick Köllner, 'Informal Institutions in Autocracies', *GIGA Working Paper* 232 (August 2013).
[279] 'Rule of Law Index 2020', *World Justice Project (WJP)*.

delivery of justice is not impartial or free from corruption. However, all these states fall within only a few points of each other therefore indicating that formal, internal punitive power is relatively consistent among China, Russia, and Iran. The result of these weak formal institutions is evidenced through high conviction rates and an increasing number of political prisoners.[280] [281] Although North Korea is not included in the WJP index, other sources such as Human Rights Watch consistently cite North Korea as lacking an independent judiciary and a prevalence of arbitrary arrests and punishment.[282] Furthermore, an analysis of North Korea's judicial structure assesses that "Korean courts and judges appear to lack any independence whatsoever and are wholly subservient to the dictates of the Korean Workers' Party."[283]

The similar Rule of Law scores between Iran, China, and Russia, combined with separate assessments on North Korea indicate that informal, internal punitive power between these four states is relatively consistent. The state appears to have an inflated ability to threaten its citizens due to a lacking rule of law and judicial independence, ensuring that state control is maintained. This practice not only permits greater punitive capacity but also encourages citizens to moderate their activity as the probability for punishment increases.

Another mechanism of formal, internal power is the use of travel bans upon its citizens to further execute jurisdictional controls. This mechanism may act as a substitute

[280] Neil Connor, 'Chinese Courts Convict More than 99.9 per Cent of Defendants', *The Telegraph*, 14 March 2016.
[281] 'Russian Political Prisoners in the Year of 2018: The Situation and Its Trends', *Memorial*, 28 September 2018.
[282] 'North Korea: Events of 2018', *Human Rights Watch*, 2018.
[283] Sung Yoon Cho, 'The Judicial System in North Korea', *Asian Survey* 11, no. 12 (December 1971): 1167–81, 1181.

for lacking external control, which I explain in subsequent sections. By preventing citizens from exit, the punitive threat increases as it is easier for a state to punish citizens within its territory. Whilst it is difficult to find written codes for all of these countries, some cover this right with more formality than others. Both Russia and China have the most formalized and publicly accessible laws concerning freedom of exit by their citizens.[284] [285] At the outset, these laws appear relatively open, and neither requires citizens to obtain an exit visa to leave the country.[286] However, both these nations make liberal use of exemption conditions and apply them in varying ways. China continuously restricts movement on those who criticize the regime and also recently denied exit to citizens of other nations.[287] Russia differs slightly in its application of exit bans, with a wide stretch of bans focused on personnel from various government agencies. This suggests that Russia is more focused on the integrity of its security apparatus. The reported widespread restriction on more than 4 million agency personnel - including those who may not be privy to state secrets - indicates the capriciousness of formal, internal punitive power.[288] It is believed that these restrictions were in response to the defection of FSB Colonel Alexander Poteyev to the US.[289] Such an aggressive potentially indicates that Russia uses a system of collective punishment, further extending the threat to its citizens and therefore, its punitive power. If state workers are put under strict

[284] 'Law on the Control of the Exit and Entry of Citizens (China)' (1986).
[285] 'Federal Law of the Russian Federation on the Procedure for Exit from the Russian Federation and Entry Into the Russian Federation', (Unofficial Translation) (1996).
[286] Excluding Macau, Hong Kong and Taiwan. 'China: Requirements and Procedures to Obtain Exit Certificates; Including Issuing Authority, Processing Time, and Grounds for Refusal as per the 2012 Exit and Entry Administration Law (2014-January 2015) [CHN105054.E]' (Research Directorate, Immigration and Refugee Board of Canada, Ottawa, 2015 2014).
[287] Thomas Kellogg and Zhao Sile, 'China's Dissidents Can't Leave', *Foreign Policy*, 23 July 2019.
[288] Vladimir Ryzhkov, 'Controlling Russians Through Travel Bans', *The Moscow Times*, 26 May 2014.
[289] Ibid.

controls such as these, even in the presence of overarching state oversight, it may indicate that such provisions would extend to contractors and proxies. In the case of Iran, a comprehensive report published by the Australian Department of Foreign Affairs indicated that most Iranian citizens can travel freely in and out of Iran without the need for exit visas.[290] However, the reports also assess that certain groups may experience restricted travel including civil society activists and journalists that report on "red line topics."[291] It is also possible that MOIS and the IRCG can impose travel bans extrajudicially.[292] North Korea remains distinct compared to other nations due to its lack of transparency on formal codes and laws. However, reports widely suggest that North Korea tightly controls exit from the state - such privilege is only afforded to a distinct few.[293] Human Rights Watch World Report 2018 detailed a number of "border-tightening" measures that North Korea has adopted to prevent exiting without explicit permission.[294]

Overall, all these states possess high degrees of internal, formal punitive power that is facilitated through a weak formal judicial and legal system. This allows the state to credibly threaten citizens within its borders through the arbitrary application of these mechanisms to serve political, rather than judicial, ends.

---

[290] 'DFAT Country Information Report Iran' (Australian Government - Department of Foreign Affairs and Trade, 7 June 2018), 48.
[291] Red line topics include reporting on 'anti-Islamic' practices. 'DFAT Country Information Report Iran', 32.
[292] Ibid, 48.
[293] 'World Report 2020 - North Korea: Events of 2019', *Human Rights Watch*, 2020.
[294] 'World Report 2018: North Korea - Events of 2017', *Human Rights Watch*, 2018.

4.6.2 Informal, Internal

As mentioned, informal capability is exercised extra-judicially, the true nature of which is unacknowledged by the state. Examples include black jails, assassinations, secret police, and vigilante-type activity occurring within their borders. Informal punishment capability is harder to track due to the lack of official documentation and the use of covert security apparatus. However, anecdotal accounts of extrajudicial proceedings may provide some indication as to the strength of a country's informal capability to pose a threat to its civilians.

In China there have been reports of a number of extrajudicial killings within the country particularly focused on quelling dissenting populations that may threaten the stability of the regime. According to Freedom House researcher, Sarah Cook, in 1999 when the traditional practice of Falun Gong was outlawed, its practitioners were subject to "extrajudicial killing—abuses which continue today."[295] However, extrajudicial practices are also used in the name of reform in China. It is reported that Xi Xing Ping's "war on corruption" launched a system referred to as the "shuanggui (双规) disciplinary system."[296] It is utilized to hold senior party officials, suspected of corruption, to account. Yet, this system operates outside official criminal courts and its practices allegedly limit people's rights and freedoms to obtain confessions. China has also been accused of using "black jails", extrajudicial detainment centers for people attempting to seek legal redress and file complaints about suspected illegal activity - although China has continuously

[295] Falun Gong is a religious movement. Sarah Cook, "Falun Gong's Secrets for Surviving in China," *Freedom House*, July 22, 2019, https://freedomhouse.org/article/falun-gongs-secrets-surviving-china.
[296] "'Special Measures': Detention and Torture in the Chinese Communist Party's Shuanggui System," *Human Rights Watch*, December 6, 2016.

denied their use.[297] Furthermore, China is using what a report by the UK Foreign and Commonwealth Office deemed "extrajudicial 'political re-education' camps", targeting Uighur Muslim populations and other minority groups.[298]

Similarly, Russia uses extrajudicial proceedings to limit protests against the state and its practices as well as limit the mobility of groups that may pose threats. Russia has been accused of allowing too much autonomy to its police and security services, such that they act with impunity and without reference to higher political leadership. The 2018 Department of State Report on Human Rights alleges that there have been targeted attacks against LGBTQ+ peoples in Chechnya which involved extrajudicial killings and torture.[299] According to Human Rights Watch 2020 Report, two Russian human rights organizations found that there were 27 extrajudicial executions of "Chechnya residents by local authorities in January 2017".[300] Furthermore, there have been allegations that those who try to protect targeted groups or are critical of the Kremlin have fallen victim to assassination attempts. A notable example was the murder of Stanislav Markelov, a human rights lawyer often depicted representing Chechens, who was shot "near the Kremlin".[301]

A Library of Congress report on the Iranian Ministry of Intelligence and Security (MOIS) details several alleged assassinations of political opponents acting inside Iran from 1988-1998.[302] Furthermore, Iran has already flexed its internal, informal punitive

[297] '"An Alleyway in Hell": China's Abusive "Black Jails"', *Human Rights Watch*, 12 November 2009.
[298] 'Human Rights and Democracy Report 2018', *Foreign & Commonwealth Office*, 5 June 2019.
[299] '2018 Country Reports on Human Rights Practices: Russia', *U.S. Department of State*, 2018, 2.
[300] 'World Report 2020: Events of 2019', *Human Rights Watch*, 2020.
[301] David Filipov, 'Here Are 10 Critics of Vladimir Putin Who Died Violently or in Suspicious Ways', *The Washington Post*, 23 March 2017.
[302] 'Iran's Ministry of Intelligence and Security: A Profile', 50.

power in attempting to control its cyber force. According to a report by Recorded Future, a former cyber commander within the IRCG was assassinated on suspicion of ideological misalignment and attempts to flee the country.[303] Similar to the other states, Iran is also concerned with internal dissidents and opponents. Notably the Ahwazis, an Arab community living in Iran, have been subject to extrajudicial assassinations, possibly by the Basij.[304] The Basij is a paramilitary, volunteer force, that has frequently been accused of using disproportionate force to quell public demonstrations as well as engaging in offensive cyber actions. However, they are considered largely unaccountable due to an inability to identify members.[305]

North Korea does not regularly publish formal doctrine or provide much public communication to the outside world as the other three states.[306] As a result, it is even more difficult to know where the lines between informal and formal lie. However, the North Korean government denies the use of forced labor camps, despite widespread reporting and accounts from escaped prisoners.[307] [308] Reports from South Korea cite the use of death squads and public sites for extrajudicial killings to "instill fear in the

[303] Gundert, Chohan, and Lesnewich, 'Iran's Hacker Hierarchy Exposed', 5.
[304] Rahim Hamid and Aaron Meyer, "Extrajudicial Killing of Ahwazis in Iran Continues Despite UN Condemnation," *The Washington Institute*, September 13, 2019.
[305] 'Iran: Stop Using Basij Militia to Police Demonstrations', *Amnesty International*, 22 June 2009.
[306] John Sifton, 'Mystery Surrounding Kim Jong Un Highlights North Korea's Totalitarianism', *Human Rights Watch*, 29 April 2020.
[307] Hyung Eun Kim, 'The Prisoner Who Escaped with Her Guard', *BBC*, 21 February 2020.
[308] In 2012, the International Coalition to Stop Crimes against Humanity in North Korea submitted to multiple UN working groups and agencies a petition for relief in reference of the gulag prison system in North Korea based on research determining the extrajudicial nature of detainment and punishment. The International Coalition to Stop Crimes against Humanity in North Korea, 'The Situation of Detainees in Gulag System (Kwan-Li-so) of the Democratic People's Republic of Korea', 3 April 2012.

populace."[309] One of the most well-documented cases was actually in reference to a US student that was allegedly tortured by North Korean officials during his detainment.[310]

Although establishing how threatening these informal punitive power mechanisms are, it is clear that all these states rely on them to further incentivize aligned behavior. Combined with the use of strong formal punitive power, internal mechanisms are well established within these four states to deter proxies from agency slack.

4.6.3 Formal, External

In analyzing the formal, external punitive capacity of these states I will focus on the use of extradition requests and treaties as it indicates the formal ability of a state to punish citizens that reside outside their territorial boundary. Extradition is a formal, legal process where one state surrenders an individual to another to face prosecution. The process is usually facilitated through the use of an existing treaty between two or more countries.[311] The process indicates a state's power in executing the long arm of their laws beyond their territorial reach, thus preventing criminals from finding safe havens through fleeing to other nations.[312]

China and Russia have laws against the extradition of their citizens, meaning that if a citizen acts criminally abroad, Russia and China assume jurisdictional responsibility for these citizens.[313] [314] However, the ability for states to exercise extradition is reliant on

---

[309] Adam Withnall, 'North Korea Death Squads Publicly Executing People in Schools, Markets and by Rivers, Report Says', *Independent*, 11 June 2019.
[310] Lesley Wroughton, 'U.S. Court Orders North Korea to Pay $501 Million in U.S. Student's Death', *Reuters*, 24 December 2018.
[311] Jonathan Masters, 'What Is Extradition?', *Council on Foreign Relations*, 8 January 2020.
[312] 'Strengthening the Long Arm of the Law: How Are Fugitives Avoiding Extradition, And How Can We Bring Them To Justice?', Pub. L. No. 108–128, § Committee on Government Reform (2003).
[313] 'Extradition Law of the People's Republic of China', *Order of the President* [2000], No. 42 (2000).
[314] "DRAFT CONSTITUTION OF THE CONSTITUTIONAL COMMISSION". *BBC Summary of World Broadcasts*, May 17, 1993.

their relationship with other states. The US benefits from over 100 bi-lateral extradition treaties with countries from around the world. Additionally, Article 3 of the ECHR - freedom from torture and inhumane treatment - bars multiple European countries from granting extradition requests to these four states.[315] As a result, attempts to exercise external, formal punitive power are often met with limited success, albeit there is some variation across these states.

China has more bi-lateral extradition treaties in place and engages in multiple joint criminal investigations than the other three countries. According to a Chinese online publication, China has successfully signed 39 extradition treaties as well as securing 52 judicial assistance treaties.[316] Six of their extradition treaties are with members of the European Union, most notably France and Spain. In 2019, Beijing pushed Hong Kong to pass a now-failed bill that would have created an extradition agreement between mainland China and Hong Kong.[317] Such measures indicate that China, to some extent, can leverage formal methods of punitive power to threaten its proxy agents abroad.

Russia by comparison does not appear to have any formal extradition treaties with other states due to its reluctance to extradite a Russian citizen to another country.[318] This limits the external, formal punitive power of Russia as it often fails to extradite its own citizens to Russia. Recent cases of competing extradition requests from the US and Russia over cyber-criminal charges, highlight the lack of formal power that Russia wields in such cases. As the US becomes more vocal in its attribution of cyber offenses against Russian citizens and agents, the number of extradition requests for various Russian

[315] 'European Convention on Human Rights', Article 3.
[316] 'China Signs Extradition Treaties with 39 Nations', *ChinaDaily*, 3 March 2015.
[317] Mike Ives, 'What Is Hong Kong's Extradition Bill?', *The New York Times*, 10 June 2019.
[318] Luke Harding, 'Russian Law Prevents Extradition', *The Guardian*, 22 May 2007.

individuals has increased.[319] In total, there have been a total of five competing extradition requests between Russia and other nations in reference to cyber-related offenses. In all but one of these requests, Russia failed to prevent the extradition of its own citizens to face trial in foreign territories. (Figure 4.7)These events perhaps suggest that Russia has a relative lack of formal, external punitive power in comparison to other states. Fleeing to democratic nations with extradition treaties with the US, or members of ECHR, Russian citizens may be able to evade Russian state retribution.

Figure 4.7: Reports of recent competing extradition requests between the US and Russia in relation to cyber offensives[320]

Year	Country of detainment	Name of Russia citizen	Origin of Competing Request	Successful request
2020	Greece	Alexander Vinnik	US, France (prisoner swap)	France
2019	Spain	Alexei Burkov	US	US
2018	Czech Republic	Yevgeniy Nikulin	US	US
2017	Cyprus	Peter Levashov	US	US
2012	Israel	Dmitry O. Zubakha	US	Russia

Although Iran does not appear to have as many formal extradition agreements as China, it has extradited foreign peoples to certain requesting states. Although I did not

[319] Andrew E. Kramer, 'A New Russian Ploy: Competing Extradition Requests', *The New York Times*, 20 December 2017.

[320] George Georgiopoulos, 'Greece to Extradite Russian Cybercrime Suspect to France', *Reuters*, 20 December 2019; Garret M. Graff, 'Russia Fails to Stop Alleged Hacker From Facing US Charges', *Wired*, 13 November 2019; Andrew E. Kramer, 'A New Russian Ploy: Competing Extradition Requests'; Andrew E. Kramer and Liz Alderman, 'Greek Court Rules for Russia in Fight Over Cybercrime Suspect', *The New York Times*, 4 September 2018; Marc Santora and Hana de Goeij, 'Russian Accused of Hacking U.S. Technology Firms Is Extradited', *The New York Times*, 30 March 2018; Department of Justice, 'Russian Hacker Arrested In Cyprus For 2008 Cyber Attacks On Amazon.Com', *United States Attorney Jenny A. Durkan, Western District of Washington*, 19 July 2012; *Department of Justice,* 'Alleged Operator of Kelihos Botnet Extradited From Spain', *Office of Public Affairs*, 2 February 2018; Department of Justice, 'Yevgeniy Nikulin Appears In U.S. Court Following Extradition', *U.S. Attorney's Office, Northern District of California*, 30 March 2018; Department of Justice, 'Russian National Extradited for Running Online Criminal Marketplace', *Office of Public Affairs*, 12 November 2019.

find any direct competing cyber-relevant extradition cases for an Iranian national, the case of Iranian engineer, Jalal Rohollahnejad, emphasizes how Iran can circumvent their lack of formal extradition treaties with other states. Jalal Rohollahnejad was detained by France and subsequently extradited to Iran through a prisoner swap - a move that was criticized by the US as a breach of US-French extradition treaties.[321] Such an example indicates that formal, external methods of punitive power can be superseded through more informal methods, where countries like Iran may have greater leverage.

North Korea has far fewer extradition treaties than the other states, although notably an extradition agreement was signed with Russia in 2016.[322] There is no evidence of a formal extradition treaty between North Korea and China, but, according to Human Rights Watch, many North Korean defectors found in China were sent back after being designated as "illegal economic migrants."[323] Most North Korean defectors travel to China to eventually settle elsewhere, for example South Korea. However, as passage through China is the main covert method utilized to exit, North Korea maintains a large degree of formal, external control over its citizens so long as China continues its practices.

It is clear that formal, external power, in terms of extradition is lacking in all of these four states. However, considering China has more formal extradition agreements than the other three states, it may have more external, formal punitive capacity. Nevertheless, what this section does signify is that in extradition processes, the US has

[321] 'US Fury after France Releases Iranian Prisoner Wanted on US Sanctions-Busting Charges', *The Telegraph*, 22 March 2020.
[322] Marzuki Darusman, 'UN Rights Expert Urges Russia Not to Implement the New Extradition Treaty with North Korea', *United Nations Human Rights Office of the High Commissioner*, 26 February 2016.
[323] 'China: Redoubling Crackdowns on Fleeing North Koreans', *Human Rights Watch*, 3 September 2017.

far more power than these four states. As a result, as the US continues to formally request the extradition of national hackers, the ability of these states to control their cyber proxies residing extraterritorially wanes.

4.6.4 Informal, External

Informal, External punitive power is similar to informal, internal in that it pertains to extrajudicial activities – the difference being that the activity occurs extraterritorially. Such measures include extraterritorial kidnapping and assassinations done through covert means. As a result, it is difficult to conclusively provide evidence to support this variable. Although democracies such as the US might possess more formal, external punitive power such as extradition treaties and sanctions implemented through Section 311 of the USA Patriot Act, non-democracies could exercise more flexibility with their informal, external punitive power due to a lack of domestic constraints on rule of law, due process, and control over information within their borders. As such, non-democracies may give their security apparatus more leeway in exacting external punitive measures.

Russia, is known to accept higher risk in its active measures and allows the FSB a large degree of flexibility.[324] [325] [326] In doing so, Russia can pose a more credible threat to its citizens abroad. An example of this surrounds a number of extraterritorial assassinations attributed to the Russian state that no longer appear to be conducted with plausible deniability in mind. One of the most notable was the UK Skripal poisoning in

[324] Andrei Soldatov and Irina Borogan, 'Russia's New Nobility: The Rise of the Security Services in Putin's Kremlin', *Foreign Affairs* 89, no. 5 (October 2010): 80–96,85,96.
[325] Galeotti, "The Spies Who Love Putin."
[326] Mark Galeotti, 'PUTIN'S HYDRA: INSIDE RUSSIA'S INTELLIGENCE SERVICES', *European Council on Foreign Relations*, 2016.

2018.[327] Whilst Russia has not accepted blame for this incident, in response the Russian President said that "Treason is the gravest crime possible and traitors must be punished. I am not saying the Salisbury incident is the way to do it, but traitors must be punished."[328] An analysis by the Atlantic Council, argues that both the Skripal and another poisoning attempt upon Emilian Gebrev, demonstrates that Russia's extraterritorial activies are increasingly aggressive and public. Atlantic Council Senior Fellow Alexander Vershbow commented that these attempts enhance "the fear [the Russians] want to instill in their enemies. The brazenness, I think, is what's most striking these days. And that they actually want us to know that they did it."[329] Russia, in comparison to the other states, appears to demonstrate a far more aggressive and public approach to their external, informal punitive capacity.

In their inability to negotiate extradition of their citizens, these four states may engage in informal methods to force extradition through threats to the detainee state. There have been some "hostage diplomacy" detainments of foreign citizens in China, Iran, Russia, and North Korea in response to the detainment of their citizens abroad. However, the ability to do so is not uniform across all these states. On December 1 2019, Canada detained the Chief Financial Officer of Huawei, Meng Wanzhou, at the request of the US after she was indicted on charges of financial fraud.[330] Ten days later, China

[327] 'Russian Spy Poisening: What We Know so Far', *BBC*, 8 October 2018.
[328] Andrew Woodcock, '"Traitors Must Be Punished": Putin Dismisses May's Demand for Skripal Suspects as Pair Meet at G20', *Independent*, 28 June 2019,.
[329] Doug Klain, 'Russian Assassinations Send Chillling Message of Impunity', *Atlantic Council*, 12 March 2020.
[330] Department of Justice, 'Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud', *Office of Public Affairs*, 28 January 2019.

detained two Canadians on alleged espionage charges.[331] A similar case occurred during the pending extradition of an alleged Russian hacker, Aleksey Burkov, to the US after his arrest in Israel. According to the Israeli newspaper, Haaretz, his extradition was delayed due to talks to exchange a swap for an Israeli woman held on drug charges.[332] In 2017, North Korea and Malaysia were involved in a diplomatic incident involving an alleged assassination of Kim Jong-Un's half-brother, Kim Jong-nam, at the behest of North Korean leadership on Malaysian soil.[333] Malaysia launched a criminal investigation into the assassination and found that Jong-nam was poisoned by the VX nerve agent, "known to be in North Korea's arsenal."[334] After the Malaysian authorities announced this as the cause of death and named several North Koreans as suspects, North Korea banned all exit of Malaysian citizens from their territory until the "safety of North Korean diplomats and citizens in Malaysia" was assured.[335] Malaysian leadership viewed this action as North Korea "holding [their] citizens hostage."[336] The use of this strategy indicates that these states do have a history of using informal methods to project their power abroad. Such a strategy could be used just as equally to force extradition of their citizens fleeing persecution.

---

[331] Anna Fifield and Jeanne Whalen, 'Canadians Detained in China after Huawei Arrest Have Now Spent a Year in Custody', *The Washington Post*, 10 December 2019.
[332] Bar Peleg and Josh Breiner, 'Israel Extends Extradition Date of Imprisoned Russian Hacker to U.S.', *Haaretz*, 23 October 2019.
[333] 'World Report 2018: North Korea - Events of 2017'; Richard C. Paddock and Choe Sang-Hun, 'Kim Jong-Nam's Death: A Geopolitical Whodunit', *The New York Times*, 22 February 2017.
[334] Richard C. Paddock, 'North Korea, Citing Kim Jong-Nam Dispute, Blocks Malaysians From Exiting', *The New York Times*, 7 March 2017.
[335] Ibid.
[336] Ibid.

4.6.5 Conclusion

From the above analysis, it is clear that China, Russia, Iran, and North Korea possess an ability to pose credible internal punitive power. Divergences occur with external punitive power. It seems likely that China possesses the greatest "External, Formal" power out of the four nations due to a larger number of extradition and legal assistance treaties. Russia potentially employs greater use of "External, Informal" power, particularly in Western states, evidenced by the increasing overtness of their targeted actions abroad. However, all of these states have methods in which to employ "External, Informal" power, whereas "External, Formal" power is reliant on relationships within the international community. With the data available, there does not appear to be a large degree of punitive power variation among these states generally, and internal punitive power is both the most credible and easily executed among these four states. It suggests that cyber proxies, in particular, may be employed within the territorial bounds of these countries so that they can better exercise their internal punitive capabilities.

Chapter 5. Conclusions and Policy Implications

5.1 Principal Findings

This thesis examines why China, Russia, Iran, and North Korea might use cyber proxies for leveraging cyber operations against external targets. I proposed four hypotheses: cost savings, plausible deniability benefits, unique skills and specializations, and that these states possess punitive power mechanisms to credibly threaten proxies and thus limit risks. In Chapter 2, I illustrate that although cyber proxy use across the four countries might demonstrate some variability, several convergences are emerging that suggest they have similar motivations.

To evaluate cost savings as an explanation, I examine both the operational costs and economic punitive costs that could result from cyber operations. I consulted US indictments and criminal complaints in connection to Russian-attributed cyber-enabled influence campaigns to demonstrate that operational costs may vary depending on the type of operation. I conclude that although cyber operations are comparatively cheap to physical operations, some cyber operations require significant resources that would represent greater costs if they were employed within state agencies. In terms of economic punishment costs, I assess how sanctions in relation to cyber events impact a proxy actor versus a government agent. I determine that sanctions programs are applied inconsistently and do not demonstrate any clear differential between cyber proxies or state agents. There is not enough evidence to conclude that using a cyber proxy would minimize the impact or likelihood of economic retribution.

In considering plausible deniability as an explanation, I first assessed whether it is fully attainable today through an assessment of technical and contextual intelligence

capabilities. In doing so, I argue that true plausible deniability is largely infeasible. However, in recognizing plausible deniability as a spectrum, I go onto evaluate whether cyber proxies provide states with any enhanced plausible deniability benefits. I view these through two lenses; legal liability and conflict escalation. Although escalation does not appear to be a characteristic of cyberwarfare as of yet, I argue that this is less to do with the ability of proxies to provide plausible deniability, and more to do with the undefined nature and legality of cyber warfare itself. Large scale cyber-attacks are not frequently followed by concrete international responses, whether they are allegedly conducted by government agency or cyber proxy. Ultimately, the evidence does not indicate that cyber proxies provide any distinct plausible deniability benefits over that of government agents.

As demonstrated in Chapter 3, technical components of cyber-attacks do not appear to be the drivers of differentiated cost. However, there is evidence of smaller cyber operations that are attributed to proxies. I explore whether this activity may be driven by the unique skills and specializations that cyber proxies employ. To assess this, I evaluate the bureaucratic structure of Iran as a case study, determining that its competitive and overlapping cyber agencies create inefficiencies and missteps that are potentially resolved through outsourcing to cyber proxies.

My last hypothesis explores the ability of states to credibly threaten cyber proxy misbehavior, through a qualitative analysis of sources of state punitive power. Through consulting various human rights institutions and journals, I concluded that all these states possess high levels of internal punitive power due to inconsistent application of the rule of law, and extrajudicial activities that further threaten their citizens. However, I assess

that these states have relatively weak external punitive power, evidenced through the use of travel bans as a substitution for credible external power and fewer extradition treaties. In determining the strength of external, formal power, I assessed the success of extradition treaties among these states. In particular, I compiled a small-N dataset of competing for extradition cases between Russia and the US in regards to cyber-related offenses. For external, informal power I consulted qualitative data surrounding extraterritorial assassinations.

5.2 Contributions

In the wake of the COVID-19 crisis, state-sponsored cyber-attacks are receiving unprecedented attention. In such crisis environments, it is important not to overstate the threat of cyber-attacks, by assuming that every attack is state-directed. However, the use of cyber proxies has national security ramifications. Further understanding the strategies employed by these states and the motivations that drive them, may provide a clearer indication of when adversarial states might use cyber proxies, thus aiding attribution.

This thesis adds to the limited literature within this space through a synthesis of qualitative data traversing multiple sources, both from private and public institutions. The conclusions of this thesis challenge and add to some of the prevailing explanations for the use of cyber proxies by China, Russia, Iran, and North Korea. For scholarship, this thesis provides a framework for future researchers, with better access to data to further investigate the puzzle of cyber proxies. From a policy perspective, the conclusions aid in structuring conditions to counter the use of cyber proxies or predict their use within cyber operations.

5.3 Implications

5.3.1 Academia

Although my focus is upon Russia, China, Iran, and North Korea, this thesis provides a framework for future researchers to consider the question of why states use cyber proxies. In future research, the interaction between regime type and this framework may provide further indications as to how different countries approach the cyber domain.

Data Collection

Researchers seeking to explore this question further should note that my project suffered data constraints, potentially limiting the validity of my conclusions. Future research into this topic should be accompanied by significant data collection and clean-up effort that creates standardized reporting and research methods across private cybersecurity companies and naming conventions for cyber threat actors.

An alternative perspective on cost

Much of the current literature around cost and cyber proxies pertains to political costs and the interaction with plausible deniability. The current literature on cyber operations emphasizes their comparative cheapness to physical operations, yet in doing so, it appears that economic costs have been generally under-evaluated. Future research should concentrate more on the operational side of cyber operations and question how these costs change depending on the nature of the operation. In doing so, we may begin to see a convergence in the types of operations outsourced to cyber proxies and those kept in-house based upon these findings.

As mentioned in Chapter 4, sanctions are not universally applied. Future researchers may want to consider the intersection between economic and cybersecurity

policy to gauge the effectiveness of US sanctions in response to cyberattacks and whether states use proxies because of, rather than in spite of, the US' application of its sanctions programs.

An Alternative Perspective on Plausible Deniability

The concept of plausible deniability is generally overlooked in literature. This thesis provides a method for evaluating (im)plausible deniability, and whether cyber proxies can allow states to benefit from claiming a higher level of deniability.

5.3.2 Policy Implications

This thesis suggests two policy implications. First, cyber proxies will likely continue to feature on the threat landscape. Second, a view into the strategies of authoritarian regimes in the presence of limited public doctrine.

Increasing Cyber Proxy Use

Cyber-enabled information warfare is an increasingly attractive option for adversarial states to challenge and influence the US domestic environment and international reputation. Google's Threat Analysis group already report a rise in North Korea's disinformation attempts in the wake of COVID-19.[337] 2019 saw a rise in reports that both China and Iran were responsible for state-sponsored election interference attempts.[338] As demonstrated in Chapter 4, workforce costs within these operations may encourage the use of cyber proxies. In addition, the threat landscape is further complicated in the presence of multiple proxies and/or a combined force of state and non-

[337] Mathew Ha, "North Korea Turns to Cyber Disinformation Attacks Amid Global Coronavirus Outbreak," *Foundation for Defense of Democracies*, April 1, 2020.
[338] Associated Press, "Not Just Russia: China and Iran May Target US Elections, Experts Say," *The Guardian*, October 30, 2019.

state actors. As worldwide economic activity slows these nations, as well as others, may adopt more aggressive and expansive techniques in pursuit of economic advantage.[339] Therefore, cyber policy should be centered around controlling the environment by discouraging the use of these cyber proxies.

Assessing Cyber Strategy in Authoritarian Regimes

As assessed in Chapter 4, Russia, China, Iran, and North Korea appear reliant upon domestic controls to counter the risk of using cyber proxies. All these states are also authoritarian and therefore the conclusions drawn could represent trends among nations of similar regime types. If policymakers Thus, policy should center around deterrence of cyber proxy through 1) disrupting the mechanisms of control that these states utilize and 2) increasing the probability of principal-agent dilemmas, made possible through exploiting the information asymmetries. If this thesis is correct in concluding that plausible deniability is not a reason why these states use cyber proxies, then the current US approach of "naming-and-shaming" these actors, may not demotivate their use. Further analysis of audience costs may indicate that support for political leadership increases domestically when the US indicts a state-affiliated group, generating a "rally 'round the flag" effect.[340]

To deter cyber proxy use, efforts should focus on increasing the likelihood of proxy failure. This can be done, as previously mentioned, through exploiting information asymmetries. Some potential policy options could include the following:

[339] David E. Sanger and Nicole Perlroth, "U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks," *The New York Times*, May 10, 2020.
[340] John E. Mueller, 'Presidential Popularity from Truman to Johnson', *The American Political Science Review* 64, no. 1 (March 1970): 18–34.

1) Utilizing US diplomatic power to further limit the movement of cyber proxy agents. In 2014, the US seized a Russian hacker, by the name of Roman Valeryevich Seleznev, in the Maldives.[341] Yet, the US does not have a bilateral extradition treaty with the Maldives. The case is demonstrative of the US' ability to leverage diplomatic action to threaten non-state actors around the world.
2) Sting operations may aid US law enforcement in obtaining admissible evidence for the high evidentiary standard expected within US courts.
3) An expanded use of honeypot traps could also aid attribution efforts.[342] This could involve an expansion of the FBI's Illicit Data Loss Exploitation (IDLE) program. As reported by arsTechnica, a website that covers technology news extensively, the IDLE program is a deception-based tactic that employs "decoy data…used to confuse illicit… collection and end-use of stolen data," with the "hope of derailing attackers."[343]
4) Focus efforts upon underground hacker forums in order to divert resources away from sponsoring states.

[341] Department of Justice, 'Russian Cyber-Criminal Sentenced to 27 Years in Prison for Hacking and Credit Card Fraud Scheme', *Office of Public Affairs*, 21 April 2017.
[342] Honeypots are "trap(s) that an IT pro lays for a malicious hacker, hoping that they'll interact with it in a way that provides useful intelligence." Josh Fruhlinger, 'What is a honeypot? A trap for catching hackers in the act', *CSO Online,* April 1, 2019.
[343] Sean Gallagher, 'Not so IDLE Hands: FBI Program Offers Companies Data Protection via Deception', *ArsTechnica*, 20 December 2019.

5) Enhance efforts to define the limits of cyberwarfare and cyber proxies within international norms and law. Whilst formulating international law has had limited success in the cyber domain, establishing further legal clarity around cyber proxies may reduce their benefit to sponsoring states.

5.4 Conclusion

Cyber proxies are enhancing complexity to the threat environment and could act as another destabilizing force within the international system. This thesis proposes a framework and explores four possible explanations to answer why Russia, China, Iran, and North Korea elect to use cyber proxies. Preliminary findings suggest that cost savings, and skills and specializations may provide some explanation although this is dependent on the type of cyber operation in question. However, the evidence is not enough to support that plausible deniability is a motivator. Furthermore, the data suggests that these states are likely to focus on using cyber proxies located with their territories due to their strong internal, punitive power. This thesis contributes to the limited literature within this space by-scrutinizing the explanations of why states use cyber proxies, and the development of cyber capabilities in the last ten years. Finally, these findings aid policymakers to further understand the cyber threat space. It is clear that the world is entering an era where conflicts in the virtual space are likely to propagate faster than in the physical space. It is therefore imperative for the US and others to not just recognize the issues and challenges, but also proactively direct efforts to blunt adversarial actions.

Bibliography

"2018 Country Reports on Human Rights Practices: Russia." *U.S. Department of State*, 2018.

"2020 Global Threat Report." *Crowdstrike*, 2020. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf.

"2020 Military Strength Ranking." *Global Firepower*, 2020. https://www.globalfirepower.com/countries-listing.asp.

"A Snapshot: Government-Wide Contracting." *GAO*, 2018. https://www.gao.gov/assets/700/699330.pdf.

"Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command." *United States Cyber Command*, April 20, 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?%20ver=2018-06-14-152556-010:%203.

"Advisory: Turla Group Exploits Iranian APT to Expand Coverage of Victims." *NCSC and NSA*, October 21, 2019. https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims.

Alexander, David. "Pentagon to Treat Cyberspace as 'Operational Domain.'" *Reuters*, July 14, 2011. https://www.reuters.com/article/us-usa-defense-cybersecurity/pentagon-to-treat-cyberspace-as-operational-domain-idUSTRE76D5FA20110714.

"'An Alleyway in Hell': China's Abusive 'Black Jails.'" *Human Rights Watch*, November 12, 2009. https://www.hrw.org/report/2009/11/12/alleyway-hell/chinas-abusive-black-jails.

Anderson, Collin, and Karim Sadjadpour. "Iran's Cyber Threat: Espionage, Sabotage and Revenge." Carnegie Endowment for International Peace, 2018.

"APT1: Exposing One of China's Cyber Espionage Units." *Mandiant (FireEye)*, 2004. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

APT28: A Window Intro Russia's Cyber Espionage Operations?, FireEye, 2014. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

"APT3 Is Boyusec, a Chinese Intelligence Contractor." *Intrusiontruth*, September 5, 2017. https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/.

"APT Definition." *Crowdstrike*, November 18, 2019. https://www.crowdstrike.com/epp-101/advanced-persistent-threat-apt/.

Arreguín-Toft, Ivan. "How the Weak Win Wars: A Theory of Asymmetric Conflict." *International Security* 26, no. 1 (2001): 93–128.

Associated Press, "Not Just Russia: China and Iran May Target US Elections, Experts Say." *The Guardian*, October 30, 2019. https://www.theguardian.com/us-news/2019/oct/30/us-elections-2020-hacking-misinformation-russia-china-iran.

Baldwin, David A. "The Sanctions Debate and the Logic of Choice." *International Security* 24, no. 3 (2000 1999): 80–107. https://www.jstor.org/stable/2539306.

Bar-Siman-Tov, Yaacov. "The Strategy of War by Proxy." *Cooperation and Conflict* 19, no. 4 (1984): 263–73. https://www.jstor.org/stable/45083584.

"Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations." *Booz Allen Hamilton*, 2020. https://www.boozallen.com/c/insight/publication/the-logic-behind-russian-military-cyber-operations.html.

Becker, Brett. "Computer Science in China: High Employment, Highest Satisfaction and Salaries." *CS0* (blog), May 24, 2017. https://cszero.wordpress.com/2017/05/24/computer-science-in-china-high-employment-satisfaction-and-highest-salaries/.

Biddle, Stephen. “Building Security Forces and Stabilizing Nations: The Probelm of Agency.” *Daedalus 146*, no.4: 126-138. https://doi.org/10.1162/DAED_a_00464.

Borghard, Erica. “Friends with Benefits? Power and Influence in Proxy Warfare.” Colombia University, 2014. https://doi.org/10.7916/D8Q81B7Z.

Borghard, Erica, and Shawn Lonergan. “Can States Calculate the Risks of Using Cyber Proxies?” *Foreign Policy Research Institute* 60, no. 3 (May 7, 2016): 395–416. https://doi.org/10.1016/j.orbis.2016.05.009.

Brunner, Jordan. “Iran Has Built an Army of Cyber-Proxies.” *The Tower*, no. 29 (August 2015). http://www.thetower.org/article/iran-has-built-an-army-of-cyber-proxies/.

Buchta, Wilfried. *Who Rules Iran*. Washington DC: The Washington Institute for Near East Policy & Konrad Adenauer Stiftung, 2000.

Byman, Daniel. “Why Engage in Proxy War? A State’s Perspective.” *Brookings*, May 21, 2018. https://www.brookings.edu/blog/order-from-chaos/2018/05/21/why-engage-in-proxy-war-a-states-perspective/.

Byman, Daniel, and Sarah E. Kreps. “Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism.” *International Studies Perspectives* 11 (February 2010): 1–18. https://doi.org/10.1111/j.1528-3585.2009.00389.x.

Calamur, Krishnadev. “What Is the Internet Research Agency?” *The Atlantic*, February 16, 2018. https://www.theatlantic.com/international/archive/2018/02/russia-troll-farm/553616/.

Carbonnel, Alissa de. “Ex-Soviet Hackers Play Outsized Role in Cyber Crime World.” *Reuters*, August 22, 2013. https://uk.mobile.reuters.com/article/amp/idUSBRE97L0TP20130822.

Carson, Austin. “Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War.” *International Organization* 70, no. 1 (Winter 2016): 103–31. https://www.jstor.org/stable/24758287.

———. *Secret Wars: Covert Conflict in International Politics*. Princeton University Press, 2018.

Chestnut, Sheena. “Illicit Activity and Proliferation: North Korean Smuggling Networks.” *International Security* 32, no. 1 (2007): 80–111. https://www.jstor.org/stable/30129802.

“China: Economic Sanctions.” *Conressional Research Service*, August 22, 2016. https://www.everycrsreport.com/files/20160822_R44605_160c92226c43bf33f590663dd758fe9b4e0b8caa.pdf.

"China: Redoubling Crackdowns on Fleeing North Koreans." *Human Rights Watch*, September 3, 2017. https://www.hrw.org/news/2017/09/03/china-redoubling-crackdowns-fleeing-north-koreans.

"China: Requirements and Procedures to Obtain Exit Certificates; Including Issuing Authority, Processing Time, and Grounds for Refusal as per the 2012 Exit and Entry Administration Law (2014-January 2015) [CHN105054.E]." Research Directorate, Immigration and Refugee Board of Canada, Ottawa, 2015 2014. https://www.ecoi.net/en/document/1205126.html.

"China Signs Extradition Treaties with 39 Nations." *ChinaDaily*, March 3, 2015. http://www.chinadaily.com.cn/china/2015-03/20/content_19865295.htm.

"China Uighurs: Detainees 'free' after 'Graduating', Official Says." *BBC*, December 9, 2019. https://www.bbc.co.uk/news/world-asia-china-50712126.

Cho, Sung Yoon. "The Judicial System in North Korea." *Asian Survey* 11, no. 12 (December 1971): 1167–81. https://www.jstor.org/stable/2642898.

Cimpanu, Catalin. "APT-Doxing Group Exposes APT17 as Jinan Bureau of China's Security Ministry." *ZDNet*, July 24, 2019. https://www.zdnet.com/article/apt-doxing-group-expose-apt17-as-jinan-bureau-of-chinas-security-ministry/.

Clarke, Colin P., and Ariane M. Tabatabai. "Iran's Proxies Are More Powerful Than Ever." RAND Corporation. *TheRANDblog* (blog), October 16, 2019. https://www.rand.org/blog/2019/10/irans-proxies-are-more-powerful-than-ever.html.

Coats, Daniel R. "Worldwide Threat Assessment of the US Intelligence Community 2017." Office of the Director of National Intelligence, May 11, 2017. https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf.

———. "Worldwide Threat Assessment of the US Intelligence Community 2019." Senate Select Committee on Intelligence: Office of the Director of National Intelligence, January 29, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Collier, Jamie. "Proxy Actors in the Cyber Domain." *St. Anthony's International Review* 13, no. 1 (May 2017): 25–77. https://www.jstor.org/stable/10.2307/26229121.

Connell, Michael, and Sarah Vogler. "Russia's Approach to Cyber Wafare." CNA Analysis and Solutions, March 2017. https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

Connor, Neil. "Chinese Courts Convict More than 99.9 per Cent of Defendants." *The Telegraph*, March 14, 2016.

https://www.telegraph.co.uk/news/worldnews/asia/china/12193202/Chinese-courts-convict-more-than-99.9-per-cent-of-defendants.html.

Cook, Sarah. "Falun Gong's Secrets for Surviving in China." *Freedom House*, July 22, 2019. https://freedomhouse.org/article/falun-gongs-secrets-surviving-china.

Cormac, Rory, and Richard Aldrich. "Grey Is the New Black: Covert Action and Implausible Deniability." *International Affairs* 94, no. 3 (2018): 477–94. https://doi.org/10.1093/ia/iiy067.

Cottrell, Lance. "The DNC Hacker Indictment: A Lesson in Failed Misattribution," October 4, 2018. https://www.securityweek.com/dnc-hacker-indictment-lesson-failed-misattribution.

Creekman, Daniel M. "A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China." *American University International Law Review* 17, no. 3 (2002): 641–81.

Creery, Madison. "Hacker Militias or Cyber Command? The U.S. and Russian Insitutionalization of Cyber Warfare." *Georgetown Security Studies Review*, March 7, 2019. https://georgetownsecuritystudiesreview.org/2019/03/07/hacker-militias-or-cyber-command-the-u-s-and-russian-institutionalization-of-cyber-warfare/.

"Cyber Threat Source Descriptions." *Cybersecurity & Infrastructure Security Agency*, n.d. https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions.

Darusman, Marzuki. "UN Rights Expert Urges Russia Not to Implement the New Extradition Treaty with North Korea." *United Nations Human Rights Office of the High Commissioner*, February 26, 2016. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17094&LangID=E.

Department of Justice. "Alleged Operator of Kelihos Botnet Extradited From Spain." *Office of Public Affairs*, February 2, 2018. https://www.justice.gov/opa/pr/alleged-operator-kelihos-botnet-extradited-spain\.

———"Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud." *Office of Public Affairs*, January 28, 2019. https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial.

———"International Hacker-For-Hire Who Conspired with and Aided Russian FSB Officers Sentenced to 60 Months in Prison." *Office of Public Affairs*, May 29, 2018. https://www.justice.gov/opa/pr/international-hacker-hire-who-conspired-and-aided-russian-fsb-officers-sentenced-60-months.

———"Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps" *Office of Public Affairs* (2018). https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

———"Russian Cyber-Criminal Sentenced to 27 Years in Prison for Hacking and Credit Card Fraud Scheme." *Office of Public Affairs*, April 21, 2017. https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-27-years-prison-hacking-and-credit-card-fraud-scheme.

———"Russian Hacker Arrested In Cyprus For 2008 Cyber Attacks On Amazon.Com." *United States Attorney Jenny A. Durkan, Western District of Washington*, July 19, 2012. https://www.justice.gov/archive/usao/waw/press/2012/July/zubakha.html.

———"Russian National Extradited for Running Online Criminal Marketplace." *Department of Justice, Office of Public Affairs*, November 12, 2019. https://www.justice.gov/opa/pr/russian-national-extradited-running-online-criminal-marketplace.

———"United States of America V. Dmitry Dokuchaev, a/k/a "Patrick Nagel". Igor Suschin, Alexsey Belan, a/k/a "Magg", and Karim Baratov, a/ka/ "Kay," a/k/a "karim Taloverov," a/k/a "Karim Akehmet Tokbergenov,"" United States District Court For the Northern District of California (February 2017). https://www.justice.gov/opa/press-release/file/948201/download.

———"U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage." *Office of Public Affairs*, November 27, 2017. https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.

———"United States of America v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, Omid Ghaffarinia, Sina Keissar, and Nader Saedi, Defendents." *United States District Court Southern District of New York*, March 24, 2016. https://www.justice.gov/opa/file/834996/download.

———"United States of Amerca v. Elena Alekeevna Khusyaynova, Defendent." *United States District Court for the Eastern District of Virginia: Alexandria Division* (2018). https://www.justice.gov/usao-edva/press-release/file/1102591/download.

———"United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleskey Alesandrovich Potemkin, and Anatoliy Sergeyevich Kovalev, Defenandts." *United States District Court for the District of Colombia* (2018). https://www.justice.gov/file/1080281/download.

———"United States of America v. Evgeniy Bogachev." *United States District Court for the Western District of Pennsylvania*, May 19, 2014. https://www.justice.gov/sites/default/files/opa/legacy/2014/06/02/pittsburgh-indictment.pdf.

———"Yevgeniy Nikulin Appears In U.S. Court Following Extradition." *Department of Justice, U.S. Attorney's Office, Northern District of California*, March 30, 2018. https://www.justice.gov/usao-ndca/pr/yevgeniy-nikulin-appears-us-court-following-extradition.

DeSombra, Winnona, and Dan Byrnes. "Thieves and Geeks: Russian and Chinese Hacking Communities." *Recorded Future*, 2018. https://go.recordedfuture.com/hubfs/reports/cta-2018-1010.pdf.

"DFAT Country Information Report Iran." Australian Government - Department of Foreign Affairs and Trade, June 7, 2018. https://www.ecoi.net/en/file/local/1437309/1930_1530704319_country-information-report-iran.pdf.

DiResta, Renee, Jonathan Albright, and Ben Johnson. "The Tactics & Tropes of the Internet Research Agency." *New Knowledge*, 2019. https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf.

"DRAFT CONSTITUTION OF THE CONSTITUTIONAL COMMISSION". *BBC Summary of World Broadcasts*. May 17, 1993. Retrived through: https://advance-lexis-com.stanford.idm.oclc.org/api/document?collection=news&id=urn:contentItem:3S51-VBH0-0017-G3SG-00000-00&context=1516831.

"Economic Impacts of Nuclear Weapon Detonation." *Article 36*, March 2015. http://www.article36.org/wp-content/uploads/2015/08/Economic-impact.pdf.

Eisenhardt, Kathleen M. "Agency Theory: An Assessment and Review." *The Academy of Management Review* 14, no. 1 (January 1989): 57–75. https://www.jstor.org/stable/258191.

Eisenstein Bar-On, Anat. "The (Il)Legality of Interference in Elections under International Law." *The Federmann Cyber Security Research Center - Cyber Law Program*, February 27, 2019. https://csrcl.huji.ac.il/people/illegality-interference-elections-under-international-law.

European Convention on Human Rights, Article 3. https://www.echr.coe.int/Documents/Convention_ENG.pdf.

"Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements." *U.S. House of Representatives Permanent Select Committee on Intelligence*, n.d. https://intelligence.house.gov/social-media-content/.

"Extradition Law of the People's Republic of China." *Order of the President* [2000] No. 42 (2000) . Accessed through: https://advance-lexis com.stanford.idm.oclc.org/document/?pdmfid=1516831&crid=e0c50c8d-04ab-46a6-a377-91ffe2e9ba63&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A50VC-38K0-01PR-3491-00000-00&pdcontentcomponentid=323050&pdteaserkey=sr0&pditab=allpods&ecomp=kb63k&earg=sr0&prid=0a962efb-ee15-4985-b21d-998b86e11382#

Fearon, James D. "Domestic Political Audiences and the Escalation of International Disputes." *The American Political Science Association* 88, no. 3 (September 1994): 577–92. https://www.jstor.org/stable/2944796.

Federal Law of the Russian Federation on the Procedure for Exit from the Russian Federation and Entry Into the Russian Federation, (Unofficial Translation) § (1996). https://www.refworld.org/pdfid/3ae6b50324.pdf.

Field, Matthew. "WannaCry Cyber Attack Cost the NHS £92m as 19,000 Appointments Cancelled." *The Telegraph*, October 11, 2018. https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

Fifield, Anna, and Jeanne Whalen. "Canadians Detained in China after Huawei Arrest Have Now Spent a Year in Custody." *The Washington Post*, December 10, 2019. https://www.washingtonpost.com/world/canadians-detained-in-china-after-huawei-arrest-have-now-spent-a-year-in-custody/2019/12/10/3a55cd4c-1af0-11ea-977a-15a6710ed6da_story.html.

Filipov, David. "Here Are 10 Critics of Vladimir Putin Who Died Violently or in Suspicious Ways." *The Washington Post*, March 23, 2017. https://www.washingtonpost.com/news/worldviews/wp/2017/03/23/here-are-ten-critics-of-vladimir-putin-who-died-violently-or-in-suspicious-ways/.

Filkins, Dexter. "The Twilight of the Iranian Revolution." *The New Yorker*, May 18, 2020. https://www.newyorker.com/magazine/2020/05/25/the-twilight-of-the-iranian-revolution

Fox, Major Amos. "In Pursuit of a General Theory of Proxy Warfare." *The Institute of Land Warfare* 123 (February 2019). https://www.ausa.org/sites/default/files/publications/LWP-123-In-Pursuit-of-a-General-Theory-of-Proxy-Warfare.pdf.

Fruhlinger, Josh. " What is a honeypot? A trap for catching hackers in the act." CSO Online, April 1, 2019. https://www.csoonline.com/article/3384702/what-is-a-honeypot-a-trap-for-catching-hackers-in-the-act.html

Galeotti, Mark. "PUTIN'S HYDRA: INSIDE RUSSIA'S INTELLIGENCE SERVICES." *European Council on Foreign Relations*, 2016. https://www.jstor.org/stable/resrep21577.

———. "The Spies Who Love Putin." *The Atlantic*, January 17, 2017. https://www.theatlantic.com/international/archive/2017/01/fsb-kgb-putin/513272/.

Gallagher, Sean. "Not so IDLE Hands: FBI Program Offers Companies Data Protection via Deception." *ArsTechnica*, December 20, 2019. https://arstechnica.com/information-technology/2019/12/not-so-idle-hands-fbi-program-offers-companies-data-protection-via-deception/.

Gan, Nectar, and Mimi Lau. "China Changes Law to Recognize 're-Education Camps' in Xinjiang." *South China Morning Post*, October 10, 2018. https://www.scmp.com/news/china/politics/article/2167893/china-legalises-use-re-education-camps-religious-extremists.

Georgiopoulos, George. "Greece to Extradite Russian Cybercrime Suspect to France." *Reuters*, December 20, 2019. https://www.reuters.com/article/us-greece-extradition/greece-to-extradite-russian-cybercrime-suspect-to-france-idUSKBN1YO274.

Gertz, Bill. "Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service." *The Washington Free Beacon*, November 29, 2016. https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/.

Goldberg, Jeffrey. "The Obama Doctrine." *The Atlantic*, April 2016. https://www.theatlantic.com/magazine/archive/2016/04/the-obama-doctrine/471525/.

Goudie, Mark. "Going Beyond Malware: The Rise of 'Living off the Land' Attacks." *Crowdstrike Blog*, May 2, 2019. https://www.crowdstrike.com/blog/going-beyond-malware-the-rise-of-living-off-the-land-attacks/.

Graff, Garret M. "Russia Fails to Stop Alleged Hacker From Facing US Charges." *Wired*, November 13, 2019. https://www.wired.com/story/aleksei-burkov-russia-hacking-extradition/.

Green, Kieran Richard. "People's War in Cyberspace: Using China's Civilian Economy in the Information Domain." *Military Cyber Affairs* 2, no. 1 (2016). https://www.doi.org/http://doi.org/10.5038/2378-0789.2.1.1022.

Greenberg, Andy. "China Tests the Limits of Its US Hacking Truce." *Wired*, October 31, 2017. https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/.

Grigsby, Alex. “The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased.” *Council on Foreign Relations*, November 15, 2018. https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

Gundert, Levi, Sanil Chohan, and Greg Lesnewich. “Iran’s Hacker Hierarchy Exposed.” Recorded Future, September 5, 2018. https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf.

Ha, Mathew. “North Korea Turns to Cyber Disinformation Attacks Amid Global Coronavirus Outbreak.” *Foundation for Defense of Democracies*, April 1, 2020. https://www.fdd.org/analysis/2020/04/01/north-korea-turns-to-cyber-disinformation-attacks-amid-global-coronavirus-outbreak/.

Haass, Richard N. *War Of Necessity, War of Choice*. New York: Simon & Schuster, 2009.

———“Sanctioning Madness.” *Council on Foreign Relations* 76 no. 6: 74-85 (Nov-Dec 1997). https://www.jstor.org/stable/20048277

Hachigian, Nina. “China’s Cyber Strategy.” *Foreign Affairs* March/April (2001). https://www.foreignaffairs.com/articles/asia/2001-03-01/chinas-cyber-strategy.

Hamid, Rahim, and Aaron Meyer. “Extrajudicial Killing of Ahwazis in Iran Continues Despite UN Condemnation.” *The Washington Institute*, September 13, 2019.

Handel, Michael. *Weak States in the International System*. Psychology Press, 1990.

Harding, Luke. “Russian Law Prevents Extradition.” *The Guardian*, May 22, 2007. https://www.theguardian.com/world/2007/may/22/russia.lukeharding.

Hassold, Crane. “Silent Librarian: More to the Story of the Iranian Mabna Institute Indictment.” *Phishlabs*, March 26, 2018. https://info.phishlabs.com/blog/silent-librarian-more-to-the-story-of-the-iranian-mabna-institute-indictment.

Hawkins, Darren, David A. Lake, Daniel L. Nielson, and Michael J. Tierney. *Delegation and Agency in International Organizations*. Cambridge University Press, 2006.

“How China’s Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World.” *White House Office of Trade and Manufacturing Policy*, June 2018. https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf.

“Human Rights and Democracy Report 2018.” *Foreign & Commonwealth Office*, June 5, 2019. https://www.gov.uk/government/publications/human-rights-and-democracy-report-2018/human-rights-and-democracy-the-2018-foreign-and-commonwealth-office-report.

"Inquiry into U.S. Costs and Allied Contributions to SUpport the U.S. Military Presence Overseas." United States Senate: Committee on Armed Services, April 15, 2013. https://www.armed-services.senate.gov/imo/media/doc/REPORT-FOR-POSTING-4-16-2013-WITH-5-14-2013-CORRECTION.pdf.

Insikt Group. "North Korea Cyber Activity." *Recorded Future*, June 15, 2017. https://go.recordedfuture.com/hubfs/reports/north-korea-activity.pdf.

———. "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3." *Recorded Future*, May 17, 2017. https://www.recordedfuture.com/chinese-mss-behind-apt3/.

———"Despite Infighting and Volatility, Iran Maintains Aggressive Cyber Operations Structure." *Recorded Future*, April 9, 2020. https://go.recordedfuture.com/hubfs/reports/cta-2020-0409.pdf.

"Internet Penetration Rate in Iran Highest among Students: Report." *Tehran Times*, June 29, 2019. https://www.tehrantimes.com/news/437507/Internet-penetration-rate-in-Iran-highest-among-students-report.

"Internet Security Threat Report 2019." *Symantec* 24 (February 2019). https://docs.broadcom.com/doc/istr-24-2019-en.

"Iran Sanctions." *Congressional Research Service*, April 14, 2020. https://fas.org/sgp/crs/mideast/RS20871.pdf.

"Iran: Stop Using Basij Militia to Police Demonstrations." *Amnesty International*, June 22, 2009. https://www.amnesty.org/en/latest/news/2009/06/iran-stop-using-basij-militia-police-demonstrations-20090622/.

"Iranian Offensive Cyber Attack Capabilities." *Congressional Research Service*, January 13, 2020. https://fas.org/sgp/crs/mideast/IF11406.pdf.

"Iran's Ministry of Intelligence and Security: A Profile." Federal Research Division, Library of Congress, December 2012. https://fas.org/irp/world/iran/mois-loc.pdf.

"Iran's Revolutionary Guards." *Council on Foreign Relations*, May 6, 2019. https://www.cfr.org/backgrounder/irans-revolutionary-guards.

Ives, Mike. "What Is Hong Kong's Extradition Bill?" *The New York Times*, June 10, 2019. https://www.nytimes.com/2019/06/10/world/asia/hong-kong-extradition-bill.html.

Jinghua, Lyu. "What Are China's Cyber Capabilities and Intentions?" *IPI Global Observatory*, March 22, 2019. https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/.

Johnson, A L. “Buckeye Cyberespionage Group Shifts Gaze from US to Hong Kong.” *Symantec Enterprise Community*, September 6, 2016. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=92a4528c-2bdb-498f-85c8-4273bfdc66aa&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

Jun, Jenny, Scott LaFoy, and Ethan Sohn. “North Korea’s Cyber Operations: Strategy and Responses.” *Center for Strategic and International Studies (CSIS)*, December 2015. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf.

Keil, Patrick. “Principle Agent Theory and Its Application to Analyze Outsourcing of Software Development,” *ACM SIGSOFT Software Engineering Notes* 30, no.4 (2005): 1-5. 10.1145/1082983.1083094.

Kellogg, Thomas, and Zhao Sile. “China’s Dissidents Can’t Leave.” *Foreign Policy*, July 23, 2019. https://foreignpolicy.com/2019/07/23/chinas-dissidents-cant-leave/.

Kiewiet, D. Roderick, and Matthew D. McCubbins. *The Logic of Delegation*. University of Chicago Press, 1991.

Kim, Hyung Eun. “The Prisoner Who Escaped with Her Guard.” *BBC,* February 21, 2020. https://www.bbc.co.uk/news/extra/o8x6gsb0wp/north_korea_prisoner_guard_escape.

Klain, Doug. “Russian Assassinations Send Chillling Message of Impunity.” *Atlantic Council*, March 12, 2020. https://www.atlanticcouncil.org/blogs/ukrainealert/russian-assassinations-send-chilling-message-of-impunity/.

Klimburg, Alexander. “Mobilising Cyber Power.” *Survival* 53, no. 1 (2011): 41–60. http://dx.doi.org/10.1080/00396338.2011.555595.

Köllner, Patrick. “Informal Institutions in Autocracies.” *GIGA Working Paper* 232 (August 2013).

Kramer, Andrew E. “A New Russian Ploy: Competing Extradition Requests.” *The New York Times*, December 20, 2017. https://www.nytimes.com/2017/12/20/world/europe/russia-extradition-levashov.html.

Kramer, Andrew E., and Liz Alderman. “Greek Court Rules for Russia in Fight Over Cybercrime Suspect.” *The New York Times*, September 4, 2018. https://www.nytimes.com/2018/09/04/world/europe/vinnik-greece-russia-extradition.html.

Krebs, Brian. “Four Men Charged with Hacking 500M Yahoo Accounts.” *Krebs on Security* (blog), March 15, 2017. https://krebsonsecurity.com/2017/03/four-men-charged-with-hacking-500m-yahoo-accounts/.

———. “Shadowy Russian Firm Seen as Conduit for Cybercrime.” *Washington Post*, October 13, 2007. https://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html?sid=ST2007101202661.

Law on the Control of the Exit and Entry of Citizens (China) (1986). https://www.fmprc.gov.cn/ce/cgny/eng/lsqz/laws/t42218.htm.

Lewis, James Andrew. “Iran and Cyber Power.” *Center for Strategic and International Studies (CSIS)*, July 25, 2019. https://www.csis.org/analysis/iran-and-cyber-power.

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. John Wiley & Sons Inc, 2019.

Libick, Martin C. "Crisis and Escalation in Cyberspace." *RAND Corporation* (2012). https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf

Libicki, Martin C., David Senty, and Julia Pollak. “Upper-Tier Cybersecurity Professionals and Policy Options.” In *Hackers Wanted*. RAND Corporations, 2014. https://www.jstor.org/stable/10.7249/j.ctt7zvzmj.13.

Lin, Herbert. “Escalation Dynamics and Conflict Termination in Cyberspace.” *Strategic Studies Quarterly* 6, no. 3: CYBER SPECIAL EDITION (2012): 46–70. https://www.jstor.org/stable/10.2307/26267261.

Lin, Patrick, Neil Rowe, and Fritz Allhoff. “Is It Possible to Wage a Just Cyberwar?” *The Atlantic*, June 5, 2012. https://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press, 2015.

Lipton, Eric, David E. Sanger, and Scott Shane. “The Perfect Weapon: How Russian Cyberpower Invaded the U.S.” *The New York Times*, December 12, 2016. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

Logan, Trevor, and Pavak Patel. “Data Visualization: U.S. Sanctions Against Malicious Cyber Actors.” *Foundation for Defense of Democracies*, April 20, 2020. https://www.fdd.org/analysis/visuals/2020/02/28/data-visualization%3A-us-sanctions-against-malicious-cyber-actors.

———. “Washington Uses Sanctions and Indictments Inconsistently When Combating Malicious Cyber Activity.” *Foundation for Defense of Democracies*, April 20, 2020. https://www.fdd.org/analysis/2020/04/15/washington-uses-sanctions-and-indictments-inconsistently-when-combating-malicious-cyber-activity/.

“Mainland Chinese Hackers Attack Hong Kong Government Departments: Security Firm.” *The Straits Times*, September 2, 2016. http://www.straitstimes.com/asia/east-asia/mainland-chinese-hackers-attack-hong-kong-government-departments-security-firm.

Masters, Jonathan. "What are Economic Sanctions?" Council on Foreign Relations, August 12, 2019. https://www.cfr.org/backgrounder/what-are-economic-sanctions

——— “What Is Extradition?” *Council on Foreign Relations*, January 8, 2020. https://www.cfr.org/backgrounder/what-extradition.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press, 2018.

———. “Cyber Proxies and Their Implications for Liberal Democracies.” *The Washington Quarterly* 41, no. 2 (July 5, 2018): 171–88. https://doi.org/10.1080/0163660X.2018.1485332.

———. “‘Proxies’ and Cyberspace.” *Journal of Conflict & Security Law* 21, no. 3 (2016): 383–403. https://doi.org/10.1093/jcsl/krw015.

Meyers, Adam. “Meet CrowdStrike’s Adversary of the Month for March: VENOMOUS BEAR.” *Crowdstrike*, March 12, 2018. https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-march-venomous-bear/.

Mills, John R. “What Ever Happened to the Front Company? Resurrecting Lost American National Security Tradecraft for an Asymmetric World.” *Georgetown Journal of International Affairs* International Engagement on Cyber III: State Building on a New Frontierpr (2013): 125–33. https://www.jstor.org/stable/43134329.

Morgan, T. Clifton, and Valerie L. Schwebach. “Fools Suffer Gladly: The Use of Economic Sanctions in International Crises.” *International Studies Quarterly* 41, no. 1 (March 1997): 27–50. https://www.jstor.org/stable/2600906.

Moskowitz, Jeff. “Cyberattack Tied to Hezbollah Ups the Ante for Israel’s Digital Defenses.” *The Christian Science Monitor*, January 6, 2015. https://www.csmonitor.com/World/Passcode/2015/0601/Cyberattack-tied-to-Hezbollah-ups-the-ante-for-Israel-s-digital-defenses.

“M-Trends 2020.” *FireEye Mandiant Services*, 2019. https://content.fireeye.com/m-trends/rpt-m-trends-2020.

Mueller, John E. “Presidential Popularity from Truman to Johnson.” *The American Political Science Review* 64, no. 1 (March 1970): 18–34. https://www.jstor.org/stable/1955610.

———“The Obsolescene of Major Wars.” *Bulletin of Peace Proposals* 21, no. 3 (1990): 321–28. https://doi.org/10.1177/096701069002100309.

———. *War, Presidents and Public Opinion*. John Wiley & Sons Inc, 1973.

Mumford, Andrew. “Proxy Warfare and The Future of Conflict.” *The RUSI Journal* 158, no. 2 (2013): 40–46.

Nadimi, Farzin. “Iran’s Passive Defense Organization: Another Target for Sanctions.” *The Washington Institute*, August 16, 2018. https://www.washingtoninstitute.org/policy-analysis/view/irans-passive-defense-organization-another-target-for-sanctions.

Nakashima, Ellen. “Russian Hacker Group Exploits Satellites to Steal Data, Hide Tracks.” *Washington Post*, September 9, 2015. https://www.washingtonpost.com/world/national-security/russian-hacker-group-exploits-satellites-to-steal-data-hide-tracks/2015/09/08/c59fa7cc-5657-11e5-b8c9-944725fcd3b9_story.html.

———. “Russia’s Apparent Meddling in U.S. Election Is Not an Act of War, Cyber Expert Says.” *The Washington Post*, February 7, 2017. https://www.washingtonpost.com/news/checkpoint/wp/2017/02/07/russias-apparent-meddling-in-u-s-election-is-not-an-act-of-war-cyber-expert-says/.

Nakashima, Ellen, and Aaron Gregg. “NSA’s Top Talent Is Leaving Because of Low Pay, Slumping Morale and Unpopular Organization.” *Washington Post*, January 2, 2018. https://www.washingtonpost.com/world/national-security/the-nsas-top-talent-is-leaving-because-of-low-pay-and-battered-morale/2018/01/02/ff19f0c6-ec04-11e7-9f92-10a2203f6c8d_story.html.

Nathan, Andrew. “How China Sees the Hong Kong Crisis.” *Foreign Affairs*, September 30, 2019. https://www.foreignaffairs.com/articles/china/2019-09-30/how-china-sees-hong-kong-crisis.

“National Cyber Strategy of the United States of America.” *President of the United States*, September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

“New Data: Volatile Cedar Malware Campaign,” *CheckPoint Blog* (2015). https://blog.checkpoint.com/2015/06/09/new-data-volatile-cedar/.

Nielson, Daniel L., and Michael J. Tierney. "Delegation to International Organizations: Agency Work and the World Bank Environmental Reform." *International Organization* 57, no. 2 (Spring 2003): 241–76. https://doi.org/10.1017/S0020818303572010.

"North Korea: Events of 2018." *Human Rights Watch*, 2018. https://www.hrw.org/world-report/2019/country-chapters/north-korea.

"North Korea: Legislative Basis for U.S. Economic Sanctions." *Congressional Research Service*, March 9, 2020. https://fas.org/sgp/crs/row/R41438.pdf.

"NSA and NCSC Release Joint Advisory on Turla Group Activity." *US Cybersecurity & Infrastructure Security Agency*, October 21, 2019. https://www.us-cert.gov/ncas/current-activity/2019/10/21/nsa-and-ncsc-release-joint-advisory-turla-group-activity.

Nye, Joseph S. "Cyber Power." Harvard Kennedy School: Belfer Center for Science and International Affairs, May 2010. https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf.

"Orpheus Data Shows Downward Trend in Zero-Day Use in Nation-State Operations." *Orpheus*, n.d. https://orpheus-cyber.com/resources/orpheus-data-shows-downward-trend-in-zero-day-use-in-nation-state-operations/.

"OSINT Isn't Evidence - InfoSec Needs to Take A Step Back & Breathe." *Secjuice*, May 16, 2018. https://www.secjuice.com/osint-isnt-evidence/.

Paddock, Richard C. "North Korea, Citing Kim Jong-Nam Dispute, Blocks Malaysians From Exiting." *The New York Times*, March 7, 2017. https://www.nytimes.com/2017/03/07/world/asia/kim-jong-nam-north-korea-malaysia-travel-ban.html?auth=login-email&login=email.

Paddock, Richard C., and Choe Sang-Hun. "Kim Jong-Nam's Death: A Geopolitical Whodunit." *The New York Times*, February 22, 2017. https://www.nytimes.com/2017/02/22/world/asia/kim-jong-nam-assassination-korea-malaysia.html.

Pape, Robert A. "Why Economic Sanctions Do Not Work." *International Security* 22, no. 2 (1997): 90–136. https://www.jstor.org/stable/2539368.

Peleg, Bar, and Josh Breiner. "Israel Extends Extradition Date of Imprisoned Russian Hacker to U.S." *Haaretz*, October 23, 2019. https://www.haaretz.com/israel-news/.premium-israel-extends-extradition-of-imprisoned-russian-hacker-to-u-s-1.8020008.

Peterson, Scott. "Twitter Hacked: 'Iranian Cyber Army' Signs off with Poem to Khamenei." *The Christian Science Monitor*, December 18, 2009.

https://www.csmonitor.com/World/Middle-East/2009/1218/Twitter-hacked-Iranian-Cyber-Army-signs-off-with-poem-to-Khamenei.

Pfaff, Anthony, and Patrick Granfield. "The Moral Peril of Proxy Wars." *Foreign Policy*, April 5, 2019. https://foreignpolicy.com/2019/04/05/proxy-wars-are-never-moral/.

"Policy and Procedures for Determining Workforce Mix." *Department of Defense*, no. Department of Defense Instruction 1100.22 (April 12, 2010). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/110022p.pdf?ver=2019-03-11-081731-063.

Popescu, Nicu, and Stanislav Secrieru. "Hacks, Leaks and Disruptions Russian Cyber Strategies." *Issue* Chaillot Paper, no. 148 (October 2018). https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

Poznansky, Michael. "Revisiting Plausible Deniability." *Journal of Strategic Studies*, 2020. https://doi.org/10.1080/01402390.2020.17345570.

"Probable Cause." *FindLaw*, January 17, 2019. https://criminal.findlaw.com/criminal-rights/probable-cause.html

Ravich, Samantha F., Dmitri Alperovitch, David Maxwell, and Ellen Nakashima. "Cyber-Enabled Economic Warfare: CEEW Threats from Iran and North Korea." Presented at the The Foundation for Defense of Democracies Conference on Cyber-Enabled Economic Warfare, Washington, D.C., November 13, 2018. https://www.fdd.org/wp-content/uploads/2018/11/CEEW-Iran-North-Korea-transcript.pdf.

"Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference." *The White House, Office of the Press Secretary,* September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

"Report of the Group of Governmental Experts on the Developments in the Field of Information and Telecommunications in the Context of International Security." UNGA, July 22, 2015.

"Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interferance in the 2016 U.S. Election." *116th Congress Senate* Report 116-XX (n.d.). https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

Rinehart, Ian E. "The Chinese Military: Overview and Issues for Congress." *The Congressional Research Service*, March 24, 2016. https://fas.org/sgp/crs/row/R44196.pdf.

Rondeaux, Candace, and David Sterman. "Twenty-First Century Proxy Warfare." *New America*, February 2019. https://d1y8sb8igg2f8e.cloudfront.net/documents/Twenty-First_Century_Proxy_Warfare_Final.pdf.

Rose, Janus. "NSA's Hacker-in-Chief: We Don't Need Zero-Days To Get Inside Your Network." *Vice*, January 29, 2016. https://www.vice.com/en_us/article/wnx5bm/nsas-hacker-in-chief-we-dont-need-zero-days-to-get-inside-your-network-rob-boyce.

"Rule of Law Index 2020." *World Justice Project (WJP)*, n.d. https://worldjusticeproject.org/sites/default/files/documents/WJP-ROLI-2020-Online_0.pdf.

"Russian Civil Servant Salaries To Increase for First Time Since 2013." *The Moscow Times*, December 13, 2017. https://www.themoscowtimes.com/2017/12/13/russian-civil-servant-salaries-to-increase-for-first-time-since-2013-a59931.

"Russian Political Prisoners in the Year of 2018: The Situation and Its Trends." *Memorial*, September 28, 2018. https://memohrc.org/en/publicationstypes/bulletin/russian-political-prisoners-year-2018-situation-and-its-trends.

"Russian Spy Poisening: What We Know so Far." *BBC*, October 8, 2018. https://www.bbc.co.uk/news/uk-43315636.

Ryzhkov, Vladimir. "Controlling Russians Through Travel Bans." *The Moscow Times*, May 26, 2014. https://www.themoscowtimes.com/2014/05/26/controlling-russians-through-travel-bans-a35830.

Salehyan, Idean. "The Delegation of War to Rebel Organizations." *Journal of Conflict Resolution* 54, no. 3 (2010): 493-115. https://doi.org/10.1177/0022002709357890.

Sales, Nathan. "Tehran's International Targets: Assessing Iranian Terror Sponsorship." *The Washington Institute*, December 11, 2018. https://www.washingtoninstitute.org/policy-analysis/view/tehrans-international-targets-assessing-iranian-terror-sponsorship.

Sanger, David, David Barboza, and Nicole Perlroth. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." *The New York Times*, February 18, 2013. https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?emc=na&_r=2&.

Sanger, David E. "As Russian Hackers Probe, NATO Has No Clear Cyberwar Strategy." *The New York Times*, June 16, 2016. https://www.nytimes.com/2016/06/17/world/europe/nato-russia-cyberwarfare.html.

———. “North Korea’s Internet Use Surges, Thwarting Sanctions and Fueling Theft.” *The New York Times*, February 9, 2020. https://www.nytimes.com/2020/02/09/us/politics/north-korea-internet-sanctions.html.

Sanger, David E., and Nicole Perlroth. “U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks.” *The New York Times*, May 10, 2020. https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html.

Santora, Marc, and Hana de Goeij. “Russian Accused of Hacking U.S. Technology Firms Is Extradited.” *The New York Times*, March 30, 2018. https://www.nytimes.com/2018/03/30/world/europe/russian-hacker-us-czech-republic.html.

Schelling, Thomas. *Arms and Influence*. Yale University Press, 1966

Schultz, Kenneth A. “Looking for Audience Costs.” *The Journal of Conflict Resolution* 45, no. 1 (February 2001): 32–60. https://www.jstor.org/stable/3176282.

Schweller, Randall L. “Unanswered Threats: A Neoclassical Realist Theory of Underbalancing.” *International Security* 29, no. 1 (2004): 159–201.

Schwirtz, Michael, and Joseph Goldstein. “Russian Espionage Piggybacks on a Cybercriminal’s Hacking.” *The New York Times*, March 12, 2017. https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html.

Sifton, John. “Mystery Surrounding Kim Jong Un Highlights North Korea’s Totalitarianism.” *Human Rights Watch*, April 29, 2020. https://www.hrw.org/news/2020/04/29/mystery-surrounding-kim-jong-un-highlights-north-koreas-totalitarianism.

Snyder, Glenn H. *Alliance Politics*, Cornell University Press, 1997.

———. “The Security Dilemma in Alliance Politics.” *World Politics* 36, no. 4 (July 1984): 461–95. https://www.jstor.org/stable/2010183.

Soldatov, Andrei, and Irina Borogan. “Russia’s New Nobility: The Rise of the Security Services in Putin’s Kremlin.” *Foreign Affairs* 89, no. 5 (October 2010): 80–96. https://www.jstor.org/stable/20788646.

“‘Special Measures’: Detention and Torture in the Chinese Communist Party’s Shuanggui System.” *Human Rights Watch*, December 6, 2016. https://www.hrw.org/report/2016/12/06/special-measures/detention-and-torture-chinese-communist-partys-shuanggui-system

Starbuck, William. *The Production of Knowledge: The Challenge of Social Science Research*. New York: Oxford University Press, 2006.

Starks, Tim. "Potential Rift with China over Hacking Charges." *Politico*, November 28, 2017. https://www.politico.com/newsletters/morning-cybersecurity/2017/11/28/potential-rift-with-china-over-hacking-charges-034433.

Strengthening the Long Arm of the Law: How are Fugitives Avoiding Extradition, And How Can We Bring Them To Justice?, Pub. L. No. 108–128, § Committee on Government Reform (2003). https://www.govinfo.gov/content/pkg/CHRG-108hhrg92899/html/CHRG-108hhrg92899.htm.

Sultoon, Samantha, and Justine Walker. " Secondary Sanctions' Implications and the Transatlantic Relationship." *Atlantic Council*, Semptember 2019. https://www.atlanticcouncil.org/wp-content/uploads/2019/09/SecondarySanctions_Final.pdf

"Terrorist Designations and State Sponsors of Terrorism." *U.S. Department of State, Bureau of Counterterrorism*, n.d. https://www.state.gov/terrorist-designations-and-state-sponsors-of-terrorism/.

The International Coalition to Stop Crimes against Humanity in North Korea. "The Situation of Detainees in Gulag System (Kwan-Li-so) of the Democratic People's Republic of Korea," April 3, 2012. https://www.fidh.org/IMG/pdf/icnk_gulag_petition.pdf.

Thornton, Rod. "The Changing Nature of Modern Warfare." *The RUSI Journal* 160, no. 4 (September 4, 2015): 40–48. https://doi.org/10.1080/03071847.2015.1079047.

Trapp, Kimberley N. *State Responsibility for International Terrorism*. OUP Oxford, 2011.

"Treasury Sanctions Iranian Organizations and Individuals Supporting Intelligence and Cyber Targeting of U.S. Persons." *U.S. Department of the Treasury*, February 13, 2019. https://home.treasury.gov/news/press-releases/sm611.

"Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups." *U.S. Department of the Treasury*, September 13, 2019. https://home.treasury.gov/index.php/news/press-releases/sm774.

Treverton, Gregory F. Covert Action (I.B. Tauris & Co Ltd (1988)

"UK Condemns Cyber Actors Seeking to Benefit from Global Coronavirus Pandemic." *Foreign & Commonwealth Office*, May 5, 2020. https://www.gov.uk/government/news/uk-condemns-cyber-actors-seeking-to-benefit-from-global-coronavirus-pandemic.

United States Council of Economic Advisors. *Economic Cost of Malicious Cyber Activity,* Executive Office of the President of the United State*s,* 2018. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

"Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and the United States Policy." *The Commission on the Theft of American Intellectual Property*, February 2017. http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf.

"US Fury after France Releases Iranian Prisoner Wanted on US Sanctions-Busting Charges." *The Telegraph*, March 22, 2020. https://www.telegraph.co.uk/news/2020/03/22/us-fury-france-releases-iranian-prisoner-wanted-us-sanctions/.

"US Sanctions on Russia," January 17, 2020. https://fas.org/sgp/crs/row/R45415.pdf.

Verizon. "2019 Data Breach Investigations Report," 2019. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

Vijayan, Jai. "APT28, Turla Nation-State Groups Deployed Multiple 0Days in Recent Attacks." *Dark Reading*, November 5, 2017. https://www.darkreading.com/threat-intelligence/apt28-turla-nation-state-groups-deployed-multiple-0days-in-recent-attacks/d/d-id/1328854.

Walker, Cliver, and Dave Whyte. "Contracting out War?: Private Military Companies, Law and Regulation in the United Kingdom." *The International and Comparative Law Quarterly* 54, no. 3 (July 2005): 651–89. https://www.jstor.org/stable/3663453.

Walker, Nigel. "China's Policy on Its Uighur Population." *House of Commons Library*, March 6, 2020.

Ward, Alex. "Read: Mueller Indictment against 12 Russian Spies for DNC Hack." *Vox*, July 13, 2018. https://www.vox.com/2018/7/13/17568806/mueller-russia-intelligence-indictment-full-text.

Warrell, Helen, and Henry Foy. "Russian Cyberattack Unit 'Masqueraded' as Iranian Hackers, UK Says." *Financial Times*, October 21, 2019. https://www.ft.com/content/b947b46a-f342-11e9-a79c-bc9acae3b654.

"Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments." *Symantec*, June 20, 2019. https://www.symantec.com/blogs/threat-intelligence/waterbug-espionage-governments.

Weeks, Jessica L. “Autocratic Audience Costs: Regime Type and Signaling Resolve.” *International Organization* 62, no. 1 (2008): 35–64. https://www.jstor.org/stable/40071874.

“What Is an Advanced Persistent Threat (APT)?” *CISCO*, n.d. https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html#~how-to-prevent-an-apt.

"What is an Indictment?" *FindLaw*, January 23, 2019. https://criminal.findlaw.com/criminal-procedure/what-is-an-indictment.html

Wirtz, James J. “Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy.” *NATO CCDCOE*, 2015. https://ccdcoe.org/uploads/2018/10/Ch03_CyberWarinPerspective_Wirtz.pdf.

Withnall, Adam. “North Korea Death Squads Publicly Executing People in Schools, Markets and by Rivers, Report Says.” *Independent*, June 11, 2019. https://www.independent.co.uk/news/world/asia/north-korea-executions-firing-squad-kim-jong-un-death-sentence-a8953211.html.

Woodcock, Andrew. “‘Traitors Must Be Punished’: Putin Dismisses May’s Demand for Skripal Suspects as Pair Meet at G20.” *Independent*, June 28, 2019. https://www.independent.co.uk/news/uk/politics/vladimir-putin-theresa-may-skripal-g20-summit-japan-salisbury-attack-a8978786.html.

Work, JD. “Evaluating Commercial Cyber Intelligence Activity.” *International Journal of Intelligence and CounterIntelligence 33*, no.2, January 16, 2020. https://doi.org/10.1080/08850607.2019.1690877.

“World Report 2018: North Korea - Events of 2017.” *Human Rights Watch*, 2018. https://www.hrw.org/world-report/2018/country-chapters/north-korea.

“World Report 2020 - North Korea: Events of 2019.” *Human Rights Watch*, 2020. https://www.hrw.org/world-report/2020/country-chapters/north-korea.

“World Report 2020: Events of 2019.” *Human Rights Watch*, 2020. https://www.hrw.org/sites/default/files/world_report_download/hrw_world_report_2020_0.pdf.

Wright, Robin B. *The Iran Primer: Power, Politics, and U.S. Policy* (Washington DC: United States Institute of Peace Press, 2010).

Wroughton, Lesley. “U.S. Court Orders North Korea to Pay $501 Million in U.S. Student’s Death.” *Reuters*, December 24, 2018. https://www.reuters.com/article/us-northkorea-usa-warmbier-idUSKCN1ON132.

Xu, Beina, and Eleanor Albert. “Media Censorship in China.” *Council on Foreign Relations*, February 17, 2017. https://www.cfr.org/backgrounder/media-censorship-china.

Yang, Kahyun, and Jim Finkle. “North Korea Says Its Supporters May Be behind Sony Attack.” *Reuters*, June 12, 2014. https://www.reuters.com/article/us-sony-cybersecurity-northkorea/north-korea-says-its-supporters-may-be-behind-sony-attack-idUSKBN0JL05120141207.

Zegart, Amy B. *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton University Press, 2007)

Zetter, Kim. "Hacker Lexicon: What are CNE and CNA?." *Wired,* July 6, 2016. https://www.wired.com/2016/07/hacker-lexicon-cne-cna/.

Zhang, Phoebe. “China’s Civil Servants Find There Is a Price to Pay for Corruption-Busting Salary Boost.” *South China Morning Post*, April 19, 2019. https://www.scmp.com/news/china/society/article/3006754/chinas-civil-servants-find-there-price-pay-corruption-busting.

Appendix

1) Cases Considered based upon searches within New York Times Archives and US Department of Justice Search Function between 2010 to 2019

Target Country	Potential sponsoring state	Explicit/Discrete	Title
US	China	Discrete	Office of Personnel Management breach
US	Russia	Discrete	USA vs Roman Valerevich Seleznev
US	China	Discrete	Anthem security breach
US	China	Discrete	US vs Su Bin
US	Russia	Discrete	Russia arrests Russian hacker for treason
US	Unknown	Discrete	USA vs Harold T. Martin III
Multiple	Russia	Discrete	Indictment of Evgeniy M. Bogachev
US	Russia	Discrete	USA vs Peter Levashov
US	China	Discrete	US Indictment against 3 Chinese nationals for CNE against 3 US companies
US	Iran	Discrete	USA vs Behzad Mesri
US	China	Discrete	US vs Wu Yingzhuo, Dong Hao and Xia Lei
US	Russia	Discrete	USA vs IRA
Saudi Arabia	Iran	Discrete	Attack on Saudi petrochemical firms
US	?	Discrete	Two Members of Syrian Electronic Army Indicted for Conspiracy
US	Iran	Discrete	USA vs SamSam Group
US	Russia	Discrete	Florida voting system breach
Saudi Arabia	Iran	Explicit	Attack on Saudi Armanco
US	Iran	Explicit	USA vs Mersad Group and ITSec Team
US	China	Explicit	USA vs "Comment Crew"
US	Russia	Explicit	Breach of White House Email System
US	Russia	Explicit	USA vs DMITRY DOKUCHAEV, a/k/a "Patrick Nagel," IGOR SUSHCHIN, ALEXSEY BELAN, a/k/a "Magg," and KARIM SARATOV, a/k/a "Kay," a/k/a "Karim Taloverov," a/k/a "Karim Akehmet Tokbergeno
US	Iran	Explicit	USA vs Mabna Institute
US	North Korea	Explicit	USA vs PARK JIN HYOK

Multiple	China	Explicit	USA vs two Chinese nationals, Zhu Hua and Zhang Shilong
US	China	Explicit	Mariott Data Breach
US	Iran	Explicit	USA vs Monica Witt
US	Iran	Explicit	Hackers target Trump 2020 reelection campaign
US	China	Discrete	Chinese hack on US Postal Service

Method:

"Explicit" was signified by the words "behalf of [insert state]" within the DoJ or New York Times sources.
"Discrete" was signified by mention of how the operation/target could benefit military or governmental purposes.

The author included cases deemed as likely to have been conducted by a cyber proxy according the definition in Chapter 2. Utilized three word searches:

1	Cyber, indictment
2	Cyber, behalf, proxy
3	Cyberattack, indictment

2) Language Analysis Methodology for Figure 4.5

When codifying the terms used in Figure 4.5, I conducted a language analysis upon the sources cited within citation 265.

For "Internal Focus", I searched for words such as "domestic" or "internal" and its variants.

For "External focus", I searched for "foreign" or "external", and its variants.

For "Offensive Focus", I searched for "offensive", and its variants.

For "Defensive Focus", I searched for "defensive", and its variants.

For "Intelligence focus", I searched for "intelligence collection" or "intelligence operations", and its variants.

For “Executory focus”, I searched for “execution”, “conduct”, and its variants.

For “Policy Focus”, I searched for “policymaking”, and its variants.