Digital Dictators: How Different Types of Authoritarian Regimes Use Cyber Attacks to Legitimize Their Rule

by

Casey E. Babb

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

International Affairs

Norman Paterson School of International Affairs
Carleton University
Ottawa, Ontario

© 2022, Casey E. Babb
Abstract

As states and populations around the world have become increasingly interconnected and dependent on digitized technologies and cyberspace, threat actors have been aggressively exploiting these changes to their own advantage. Of particular concern to academics, cyber experts and national security practitioners in the West, has been the rapid proliferation of damaging and disruptive cyber attacks carried out by state-actors – particularly authoritarian regimes – and their proxies. Despite global cyber attacks rising year by year, in terms of both frequency and level of technological ability, available data suggests most of the world’s major cyber attacks are carried out by a relatively small handful of states. Furthermore, it appears as though these states tend to favour certain types of cyber attacks over others. This observation leads to the central research question of this dissertation: *why do certain types of authoritarian regimes tend to favour certain types of cyber attacks over others?* Taking a deductive approach, and drawing from existing theories on authoritarian legitimation and cyber conflict, I have developed a needs-based theory of authoritarian behaviour in cyberspace. More specifically, I suggest that different types of authoritarian regimes will use different cyber strategies to fulfil or service the process, strategy, or outcome they need most to maintain domestic support and legitimacy.
ACKNOWLEDGEMENTS

Victory most certainly has a thousand fathers (and mothers). The writing of this dissertation is not only the culmination of six years at the Norman Paterson School of International Affairs (NPSIA), but really a lifetime of incredible opportunities, and both academic and professional experiences. Through each chapter of this journey, remarkable people along the way have lent me a hand in furthering my personal, academic, and professional growth. There were always people there to question my thinking, challenge me, push me towards new goals, motivate me, and who believed in me. Without these people, this dissertation would not have been possible. That said, I will focus here on those without whose help this specific project would not have come to fruition.

First, I want to start by thanking my dissertation supervisor, who since day one pushed me to think innovatively about my research, and who has given me incredibly valuable guidance over the last number of years: Dr. Alex Wilner. In addition to overseeing my research, Alex has also given me the opportunity to work on and contribute to breakthrough research on a wide range of topics that not only led to other academic endeavours and connections, but which also helped me establish myself as a practitioner within the national security community. More importantly, though, Alex has become a life-long friend, and trusted confidant, on matters both personal and professional. I cannot thank him enough for what he has done for my family and me.

I also owe a great deal of gratitude to Dr. Steve Saideman. Professor Saideman was always available to discuss my research, ways to make it stand out, and strategies to get me across the finish line. He not only taught my cohort how to think about structuring a proper prospectus and dissertation, he taught us how to think differently – how to think more strategically and creatively. I look up to him a great deal, and without his guidance, this work would not have been possible.

The Department of National Defence (DND), the Canadian Network for Research on Terrorism, Security, and Society (TSAS) and the Royal United Services Institute (RUSI) are also owed special thanks for their support and contributions to my Ph.D. research over the years. Both DND and TSAS awarded me generous research grants that supported research projects complementary to this dissertation, and in 2020, RUSI gave me Associate Fellow status where I have had the opportunity to work and collaborate with some of the best in the world on a range of subjects.

Special thanks is also owed to Dr. Brandon Valeriano. Dr. Valeriano’s work on cyber strategy, and cyber conflict writ large had a profound impact on my studies, my interests in specific issues, and the development of this dissertation. He is among the best in the world when it comes to studying cyberspace, and how conflict is and will continue to intersect with the cyber realm, and I am honoured to have had his ear on so many occasions.

My two closest friends, Marcel Parsons and Brandon Mackenzie also deserve thanks for their motivation, support and advice on all matters both personal and professional over the last decade. Both of you have had meteoric career trajectories with inspiring successes along the way, and I want to thank you for setting the bar so high.
To my father Franklin: my thirst for knowledge and my inability to stop questioning the world around us comes from you. You have given me the gift of inquisitiveness, and inspired me to achieve all that I can. Without question, you are the driving force behind this Ph.D.

To my mother, Theresa: when I questioned whether or not I should even do my undergraduate degree, and expressed frustration over the learning curve, it was you who persuaded me to stay the course. Throughout my time at Saint Mary’s, studying in Toronto, and throughout my Ph.D., you have been more than supportive, and I would not be where I am today were it not for you continually pushing me. Thank you for everything you have done.

To my son, Avram: thank you for being such a good boy while I worked on this research. Remember to find inspiration and motivation in others, never stop questioning, never settle, and always finish what you start.

Last but certainly not least, the most important person of all, my wife Ashley. Without your love and support, none of this would have been possible. In the spring of 2016, I sat down with you over coffee and somewhat sheepishly told you I wanted to get my Ph.D. Without hesitation, you told me you would support me, and began making changes in your own life to accommodate my schedule, and this new chapter of our lives. From surprising me with a home office, to buying me endless cups of coffee, to listening to me ramble on about a wide range of unsavoury and unsettling topics, you have been nothing but helpful and encouraging, all the while charting your own career path, and taking care of Avram. I could not have done it without you.

I would also like to make mention of, and dedicate this dissertation to the late great Daniel Pearl. On February 1, 2002 when I was 12 years old, Daniel was murdered by terrorists in Pakistan. At the time, he was serving as the South Asia Bureau Chief of the Wall Street Journal. Daniel’s life and death had a profound impact on me (and countless others) in a number of ways. On some unexplainable level, Daniel’s murder exposed me to the fragility of life and the realities of the global threat environment. However, Daniel’s final moments also exemplified the importance of never shying away from who you are, and remaining dignified even in the most dreadful times.

Daniel – this is for you.
TABLE OF CONTENTS

Abstract 2

Acknowledgements 3

Table of Contents 5

CHAPTER ONE

1. **Introduction: Revising Cyber Strategy** 8
   1.1 Puzzle 8
   1.2 Research Question 10
   1.3 Argument 11
   1.4 Motivation and Significance 13
   1.5 Importance for the Policy Community 17
   1.6 Concepts and Definitions 19
      1.6.1 Autocracy 19
      1.6.2 Legitimacy 22
      1.6.3 Cyber Attacks 23
   1.7 Research Design and Method 25
   1.8 Contribution and Summary of Findings 35
   1.9 Roadmap and Next Sections 39

CHAPTER TWO

2. **Towards a Theory on Autocratic Behaviour in Cyberspace** 40
   2.1 Cyber Strategy 40
2.2 Authoritarian Variance in Maintaining Power 44
2.3 Assessing the Literature: Useful Theories and Glaring Gaps 53
2.4 Explaining my Theory on Why Authoritarian Regimes Vary in Their Use of Cyber 55
2.5 A Note on Scope, Limitations, Intent, and Expectations 59

CHAPTER THREE

3. China: Cyber Attacks and Regime Legitimation 62

3.1 Introduction 62
3.2 Background: The CCP, Cyberspace, and the Origins of Chinese Cyber Power 64
3.3 An Analysis of China’s Cyber Attacks from Hu to Xi 69
   3.3.1 Hu Jintao, Chinese Cyber Attacks, and the Birth of a Chinese Cyber Superpower (2002-2012) 70
   3.3.2 Xi Jinping, Cyber Nightmares, and the Return of a Great Power (2012-current) 76
   3.3.3 Chinese Cyber Attacks and Regime Legitimation 85

CHAPTER FOUR

4. Russia: Cyber Attacks and Regime Legitimation 91

4.1 Introduction 91
4.2 Background: The Kremlin, Cyberspace, and the Origins of Russian Cyber Power 93
4.3 From Moonlight Maze to Guccifer 2.0: An Analysis of Russia’s Cyber Attacks 101
   4.3.1 Russia’s Ascent to Cyber Supremacy 103
   4.3.2 Guns and Gigabytes: Russia’s Integration of Cyber in Warfare 107
   4.3.3 Russian Cyber Attacks and Regime Legitimation 122
CHAPTER FIVE

5. Bitcoin to Bombs: North Korea’s Cyber Strategy and the Preservation of Kim Jong-Un

5.1 Introduction 127
5.2 Background: Juche, Cyberspace, and the Origins of North Korea’s Cyber Power 130
5.3 Kim Jong-Un, Elite Loyalty, and the Making of a Mafia State: An Analysis of North Korea’s Cyber Attacks 136
  5.3.1 North Korean Cyber Attacks and Regime Legitimation 146

CHAPTER SIX


6.1 Introduction 156
6.2 Background: Military Autocracies, Regime Survival, and Legitimation 158
6.3 Soldiers in the Palace: How Military Elites Continue to Justify Coups and Claim Legitimacy in Mali 162
  6.3.1 What Does the Situation in Mali Tell Us? 167

CHAPTER SEVEN

7. Concluding Thoughts and Future Avenues of Research 173

7.1 Conclusion 173
  7.1.1 Key Takeaways 174
  7.1.2 Future Research 179
  7.1.3 Bridging the Gap 185

References 191
CHAPTER ONE

INTRODUCTION:
REVISING CYBER STRATEGY

1.1 PUZZLE

In the spring of 2004, suspicious network activity on Nortel’s servers caught the eye of Brian Shields, one of the company’s cyber security analysts. After some assessments, Shields realized that a computer in Shanghai had hacked into the e-mail account of one of the company’s Ottawa-based executives, where the intruder was using stolen passwords to download highly sensitive and commercially confidential intellectual property (IP) from “Live Link” – a digital warehouse Nortel used to store company information.¹ Over the next six months, Shields found evidence that nearly 1500 documents had been stolen from the company by actors operating through internet service providers in China, and that these highly sophisticated hacks had been happening since at least 2000.² Seized with other commercial priorities at a time when cyber attacks were poorly understood, Nortel management failed to address the threat, allowing China to steal a trove of information over the next five years, until the company went bankrupt in 2009.³ Today, former employees of Nortel, cyber security experts, and Canada’s intelligence agencies argue these state-backed hackers not only destroyed Nortel by stealing their IP, data, and commercial secrets, they also built Huawei – the world’s largest smartphone manufacturer – using made-in-Canada technology.⁴ Why did hackers, purportedly backed by the Chinese

Communist Party (CCP) undertake such a sophisticated economic espionage campaign through cyberspace? Prior to 2000, China-backed cyber attacks were much less sophisticated and were primarily patriotic in nature, designed to quell dissidents and embarrass rivals. What explains this shift in China’s cyber strategy and their outward facing behaviour in cyberspace?

On December 23, 2015, a worker inside a utilities control center in the Ivano-Frankivsk region of Western Ukraine noticed his computer cursor streaking across the screen. Moving methodically towards different buttons wired to electrical circuit breakers, the person controlling the cursor swiftly took an electrical substation offline – leaving thousands in the dark and without heat. Then, after locking the operator out of his computer, the attack continued, hitting over 30 substations, leaving nearly a quarter of a million residents without power. Ukraine’s security and intelligence community was quick to blame Russia, with other intelligence agencies and cybersecurity companies from the U.S. and elsewhere pointing the finger at the Sandworm Team, a notorious Russian cyber group known for targeting entities with a strategic value to the Russian government, including the North Atlantic Treaty Organization, various European governments, and private sector companies. What explains this and other similar attacks carried out by Russia? Why are so many of their cyber attacks coercive and combined with other instruments of traditional power and conflict? Why do countries like China, Russia and other states, differ so markedly in how they target their adversaries through cyberspace?

1.2 RESEARCH QUESTION

Over the last number of years, multiple attacks and intrusions through cyberspace have caused significant damages and disruptions for countries around the world. From the Chinese-led Titan Rain campaign of 2003, which targeted critical U.S. defense infrastructure, to Russia’s hacking of the Democratic National Committee (DNC) in 2016, to North Korea’s 2017 WannaCry ransomware campaign, cyberspace has proven to be an effective and increasingly utilized arena for actors to conduct a wide range of operations against their adversaries. Moreover, data on cyber attacks point to a sharp increase in malicious cyber intrusions and activities in recent years, both in terms of frequency and level of sophistication.

However, after assessing the data, unpacking the literature and analyzing the nature of publicly-known and attributable cyber attacks, it becomes clear that not only are a small handful of authoritarian states responsible for the vast majority of global cyber attacks, but that the states behind these attacks tend to favour certain forms of cyber intrusions over others. For example, China – though known to carry out a wide range of attacks – prioritizes cyber espionage and the theft of sensitive commercial information and IP, while North Korea on the other hand, tends to conduct various types of financially motivated intrusions in addition to their cyber espionage efforts. Russia – another leading actor in cyberspace – uniquely combines a range of intrusive and sophisticated attacks with multidimensional propaganda to delegitimize and manipulate their opponents, undermine democratic institutions and sow discontent abroad. These select examples and this puzzling observation as a whole begs the question: why do certain authoritarian regimes tend to favour certain types of cyber attacks over others?

1.3 ARGUMENT

I argue that the most active hostile state actors in cyberspace – hostile at least from the West’s perspective – are using cyber attacks as a calibrated tool to advance their own strategic agendas, both at home and abroad. More specifically, I suggest that states are carrying out offensive cyber operations as a form of regime maintenance and domestic legitimization, which abroad, often manipulate enemy decision making and augment other, more traditional forms of political signalling and power competition.9

Given that many of the most belligerent actors in cyberspace are countries under authoritarian regimes, this research draws on key works which analyze how authoritarian regimes vary in their behaviour, and why. As such, I argue that the differences we see amongst state-level strategies in cyberspace are a reflection of the unique characteristics of each type of authoritarian regime, and the ways in which those types of regimes seek to manipulate, control and maintain power in their own respective ways. Numerous scholarly works detailed in Chapter 2 tell us what certain types of authoritarian regimes depend on to legitimize themselves (e.g. single party regimes depend heavily on ideological narratives). Using these theories, I expect to see consistencies in the cyber domain, with the regime types I focus on (e.g. single-party, personalist, electoral autocracies, and military regimes), and the countries I analyze, using cyberspace as another medium to advance or obtain whatever it is they need most to legitimize their rule. From this perspective, this dissertation as a whole is an exercise in extending theories drawn from the comparative politics of autocracies, to the cyber domain, and determining if those theories apply in the digital realm.

9 This argument is developed in greater detail in Chapter Three’s theory building exercise, where I explain my needs-based theory on authoritarian regime legitimization in cyberspace.
Unquestionably, many (if not all) Western liberal democracies (e.g. the U.S., the United Kingdom, France, Germany, Canada etc.) carry out regular, extremely sophisticated and damaging cyber intrusions against their adversaries and a wide range of entities as well, though for the purposes of this research, I focus specifically on autocratic regimes. As Clarke and Knake rather pointedly state – “the Internet has become the backbone of authoritarian surveillance states all over the world.” Furthermore, Canada and many of our allies, including the U.S., are particularly interested in and concerned with better understanding, combating, and defending against hostile cyber activities from adversarial nations. For these reasons, I focus on authoritarian regimes.

In attempting to answer the underlying research question of this dissertation, I focus and shed light on the future of cyber warfare, not by assessing doctrines, but by measuring behaviour. Further, this dissertation will also contribute to building a theoretical understanding of why certain countries favour and specialize in particular types of cyber attacks over others, and how the underlying factors and motivations that dictate these choices may impact the methods, abilities and effectiveness of states to defend against them. It also aims to inform policy makers as they develop processes, policies and plans to combat state-led attacks in cyberspace – particularly those attacks emanating from non-democratic, adversarial nations.

---

Finally, after reviewing the literature on how authoritarian regimes vary, this research will validate the core theories throughout this field, illustrating the ways in which cyber attacks have become part of the authoritarian toolkit of regime maintenance and legitimation.

1.4 MOTIVATION AND SIGNIFICANCE

A number of interconnected trends have emerged in recent years, which in large part motivate this research, while simultaneously elevating its significance. First, cyber threats emanating from nation states are not only acute – they are increasing. As Dunn Cavelty and Egloff (2019) note, malicious cyber activities have become so pervasive that there has been a “…‘normalisation’ of cyber conflicts below the war threshold as a constant accompaniment to political conflicts.” Indeed, as numerous subject matter experts have suggested, states’ increasing use of cyber operations as a tool of national power, as well as a means of authoritarian and illiberal regime control and civilian manipulation is raising the prospect of more destructive and disruptive cyber activity. This, coupled with a clear rise in the digitization of most elements of government and commercial business, as well as what appears to be a global civilian migration from the physical world to the cyber domain in nearly all aspects of life, has lead to a stunning proliferation of potential attack surfaces and a surge in cyber vulnerabilities which the West’s rivals have continued to exploit. For example, at the time of writing (April 2021), the U.S. is still reeling from the Russia-backed SolarWinds attack that took place (or was detected) in December 2020. Described by Microsoft President Brad Smith as “the largest and most

sophisticated [cyber] attack the world has ever seen,” the attack gave hackers access to potentially tens of thousands of users, as well as numerous U.S. companies, departments and agencies, including the Departments of Homeland Security, Treasury, Justice, Commerce and others. Likewise, in March 2021, China-backed hackers were able to penetrate Microsoft’s e-mail software, gaining access to the personal information and data on as many as 300,000 users worldwide. Despite state-backed cyberattacks having become common occurrences over the last number of years, these and other relatively recent attacks have shocked many observers in how indiscriminate, far-reaching and brazen they are.

Second, experts have also observed steady democratic backsliding across the globe, with Abramowitz and Repucci suggesting, “the global landscape is characterized by emboldened autocrats and beleaguered democracies.” Moreover, in many instances, this democratic backsliding has been accelerated by authoritarian control of cyberspace and digital freedoms. Echoing this, Freedom House, has noted that “the internet is growing less free around the world, and democracy itself is withering under its influence.”

Third, there has also been an uptick in concerted, authoritarian, state-led efforts to challenge and present viable alternatives to liberal democratic systems of governance worldwide. Nations such as China and Russia, who believe weakening democracy will accelerate the decline

---

of Western global influence, have aggressively exploited the openness of liberal democracies – most often through cyberspace – to bolster their own regimes and the image of authoritarianism.¹⁹ In fact, Chinese Foreign Minister Wang Yi and his Russian counterpart, Sergey Lavrov issued a joint statement in late March, 2021 stating that the U.S.-led international order “does not represent the will of the international community.”²⁰ Speaking on this point Walker and Ludwig (2021) write that “two major powers in particular, China and Russia, have led the way in tightening control domestically, adapting their techniques for the digital era and exerting greater influence abroad with the aim of making the world safer for autocracy.”²¹ Remarkably, their strategies appear to be working, with evidence suggesting there has been a steady increase in the number of people worldwide who appear amenable to living in non-democratic countries or who appear to be untroubled by autocratic developments in their own democratic nations.²²

Fourth, the most active hostile actors in cyberspace are pursuing a strategy of “digital authoritarianism,” as a means to tighten their grip internally, spread propaganda at home and abroad, undercut basic human rights, promote illiberal beliefs and practices beyond their borders,

---

and erode public trust in open societies.\textsuperscript{23} We are seeing this in places like Russia, where the Kremlin continues its campaign of cyber and information warfare against democratic institutions worldwide and where they have repeatedly targeted the social cohesion of the United States and various Europe countries. North Korea has employed similar cyber campaigns. Additionally, in China, where the regime is the world’s worst abuser of internet freedom,\textsuperscript{24} and where the Chinese Communist Party (CCP) has created what Brookings Institute fellow, Chris Meserole described to me as a “cyber-enabled open-air prison,” the country’s “Golden Shield” – or its “Great Firewall” – limits any material or activities that could destabilize the regime.\textsuperscript{25}

Ultimately, we are witnessing a range of autocratic governments, led by China and Russia, and to a lesser extent North Korea, harnessing cyberspace to advance numerous strategic objectives and to strengthen their dictatorial regimes. Yet, how they are doing this in their own unique ways, how these sorts of trends are interrelated, and what connections their strategies have to their respective regime types remains largely overlooked and woefully understudied. Indeed, few scholarly attempts have been made that take even a cursory look at the dynamics between these issues. These trends, and this dearth of knowledge, is what motivates this dissertation and warrants further academic examination.


\textsuperscript{25} Simon Denyer, “China’s scary lesson to the world: Censoring the Internet works,” The Washington Post, May 23, 2016: https://www.washingtonpost.com/world/asia_pacific/chinas-scary.lesson.to.the.world.censoring.the.internet.works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html
1.5 IMPORTANCE FOR THE POLICY COMMUNITY

Over the last decade, cyber issues have steadily grown in importance throughout international security, defence and intelligence communities. After land, sea, air and space, cyber is now widely considered the “fifth domain” of warfare, with every country in the western world identifying cyberspace as a national security priority. As Dunn Cavelty and Wenger (2022) note “In the past decade, cyber security has consolidated its position as one of the top national security issues of the 21st century: The dynamic interaction between technological vulnerabilities and the possibilities of their political misuse creates a problem space with little stability.” From U.S. Presidential speeches, to long-term national defence strategies (e.g. the Third Offset Strategy), to Ministerial mandate letters (e.g. Minister of National Defence), cyber has become a top-of-mind issue for decision-makers at the highest levels of government. As Carvin (2021) notes, this increased focus on cyber has been noticeably pronounced in Canada, with the last few years in particular marking a turning point for cyber policymaking in the country’s national security community. Yet, despite cyber emerging as a focal point in terms of national security considerations, many experts have repeatedly pointed out that policymakers fail to sufficiently understand cyberspace – let alone adversarial use of the cyber domain.

---

Government personnel working on the technical side of cyber security and cyber operations often fail to understand policy, while individuals in the policy making process often fail to understand the technical elements of cyberspace. In addition, high-level political language on cyber – which often catches the attention of and drives government policy development – tends to be unnecessarily catastrophic in nature. It has been nearly a decade since then Secretary of Defense Leon Panetta raised the specter of a “cyber Pearl Harbor” and since former Homeland Security Secretary Janet Napolitano said “cyber 9/11” could happen “imminently.” Unfortunately, this type of conjecture persists, and still, to a certain extent, influences cyber-related policymaking in government. Further, while cyberspace has always been poorly understood and tackled by the policy community, the COVID-19 pandemic has only illuminated government inabilities to appropriately address and respond to hostile cyber activities – often emanating from the same aforementioned nation-states as well as a range of nefarious online actors.

From a policy perspective, Canada and other like-minded countries must improve their understanding of the cyber domain, as well as its intersection with other emerging technologies that are being used for high-tech illiberal purposes. Building an appropriate policy toolkit will require a deeper understanding of the strategic goals authoritarian regimes are pursuing in the digital era — both in their own backyards and abroad — and of the methods they are using in

---

pursuit of their goals.\textsuperscript{33} Going forward, as conflict in cyberspace intensifies, government policymakers will need a nuanced understanding of why our adversaries behave the way they do in the cyber domain if they are to develop something beyond a one-size-fits-all approach to cyber conflict. This dissertation will contribute to that understanding.

\textbf{1.6 CONCEPTS AND DEFINITIONS}

This section provides definitions to the foundational concepts of this research. Though most of the key terms that underpin this dissertation are widely know and commonly understood, I want to avoid any ambiguity, particularly in light of certain conceptual and typological flexibilities that should be kept in mind, which I speak to later in my dissertation.

\textit{Autocracy}

As Hadenius and Teorell (2007) emphasize, in order to develop a typology of autocratic political regimes, we first need a “qualitative (dichotomous) distinction between democracy and autocracy.”\textsuperscript{34} In their work, and in the material of many other scholars looking at authoritarian legitimation, they use the “mean of each country’s Freedom House and Polity scores converted to a scale from 0 (least democratic) to 10 (most democratic)”, and distinguish democracies from autocracies at a score of 7.5. However, any score on the scale by Hadenius and Teorell, or any other researcher that uses a similar metric of differentiating between democracies and autocracies, could potentially be based on entirely different combinations of measured features of Polity IV and Freedom House. Therefore, I avoid this commonly used approach and instead

\begin{flushright}
\end{flushright}
use the same approach as Kailitz (2013) in that I clearly differentiate democracies from autocracies based on the qualitative criteria of whether executive and legislative elections are free and fair, and whether the authorities and/or power of the ruler are actually constrained by an elected legislature and an independent authority. This approach is informed by the well-established and vast scholarship that differentiates autocracy from democracy by focusing on things like variance in institutional structures and basic functional differences between the two types of government.

Fortunately, for this research, defining and conceptualizing democracy has been at the heart of political science for decades. As such, various definitions of democracy (e.g., Alvarez et al. 1996; Beetham 1992; Bollen 1990; Huntington 1991b; Linz and Stepan 1996; O’Donnell 1996; Przeworski 1991; Sartori 1987; Schmitter and Karl 1991; Schumpeter 1950) have influenced the way I identify key democratic characteristics typically absent in autocracies. In this sense, my identification of autocracies has been determined more by what certain countries are not, as opposed to classifying them based on what they are. Further, and as Mauk (2020) notes, most definitions of democracy “revolve around a common core that emphasizes the accountability and/or responsiveness of the ruling vis-à-vis the ruled or the mode through which this accountability and responsiveness are secured: contested elections/the electoral process.35 This consistency throughout the literature also fed into my approach. That being said, arguably the most influential scholarly work on the topic comes from Robert Dahl (1971; 1989; 1998; 2006), who developed a sort of normative conception of an ideal democracy, based on five underlying democratic standards which must be met: “effective participation,

voting equality, enlightened understanding, control of the agenda, and full inclusion of adults.”

Together, these core elements of a democracy ensure equality for all members of the political community. Moreover, Dahl suggests that there are two overarching characteristics that define a democracy, or what he often referred to as a “polyarchy” and which feed into and inform my own approach to identifying autocracies: political competition and public inclusiveness and/or the right to participate.

From this perspective, only political regimes that are “extensively open to public contestation,” and which are also “highly inclusive,” are considered democracies. Based on these characteristics, democratic political systems should be thought of as those in which the population has equal political rights, and where institutional dynamics are based primarily on free and fair competitive elections, and the ability of the population to participate in those processes. Simply put, democracies provide opportunities for the political community or population to oppose those in government, making the latter accountable to the former. In contrast, autocracy is most often characterized as “the absence of democracy” (e.g., Cheibub, Gandhi, and Vreeland 2010; Geddes, Wright, and Frantz 2014; Svolik 2012), or in other words, the absence and/or violation of at least one foundational criteria of a democracy outlined above. Consequently, government accountability and responsiveness vis-à-vis the political community is typically non-existent and not secured through standard democratic institutional mechanisms. Rather, rulers choices are just that – their own choices based on their own unconstrained power and volition. As a result, autocratic governments and leaders lack the incentive to formulate policies based on or in the best of interest of the population.

To summarize, on the one hand, *democracies* guarantee the political equality of the general population and feature a range of robust institutional mechanisms – based on fair, free, and competitive elections – that form the basis of and are necessary for things such as effective participation, voting rights, and complete inclusion of the eligible political community. This dynamic requires democratic rulers to ensure they remain responsive to citizen demands, and that their policies are crafted in such a way that they benefit the general population. *Autocracies*, on the other hand, tend to lack these characteristics – or at least, some of them. As discussed elsewhere in this dissertation, while certain autocratic regimes (e.g. electoral autocracies) mimic some of the main procedural features of a democracy, the basic principles required for these features to achieve any true democratic purpose are always lacking, or are severely flawed. Subsequently, unlike democracies, autocracies fail to guarantee the political rights of their citizens, as well as adequate opportunity for their citizens to oppose and challenge incumbent rulers.

*Legitimacy*

Just as all other key works on autocratic legitimation have done, legitimation in this dissertation is defined as the process of gaining support, which is based on an empirical, Weberian tradition of “legitimacy belief”.37 Weber attempted to classify political rule without reference to normative judgments that are supposed to be the “right” rule. Legitimation seeks to guarantee active consent, compliance with the rules, passive obedience, or mere toleration within the population. According to Weber, if a political regime is considered legitimate, its participants or the general population has certain beliefs or faith (“legitimitätsglaube”) regarding its power

---

and standing. As Weber notes: “the basis of every system of authority, and correspondingly of every kind of willingness to obey, is a belief, a belief by virtue of which persons exercising authority are lent prestige.”\textsuperscript{38} Because of this approach and the way I frame legitimation in this research, I avoid any normative connotations of legitimacy, and therefore avoid the common oxymoronic argument when it comes to legitimacy, and autocratic regimes being inherently illegitimate. This was precisely Weber’s aim. What Weber attempted, and what is important for this research, is to classify political rule while avoiding reference to the normative judgments or perceptions related to the “right” rule. Like Weber, what I am concerned about is legitimation as a means to guarantee things like active consent, adherence with the rules, passive obedience, or simply mass tolerance amongst the population. Further, Weber distinguishes among three key sources of legitimacy – understood, generally speaking, as the acceptance not only of authority but also of the need to follow the rules and respect its command. As Weber suggests, and as this dissertation indirectly speaks to, people may have faith or follow a particular government or social order because of its legacy or the length of time it has been followed (tradition), because they believe in their ruler (charisma), or because they trust and/or believe in the legality of the regime.\textsuperscript{39} This is how legitimacy is defined within this dissertation.

\textit{Cyber attack}

This research is focused on malicious state-level activities in cyberspace. The prefix “cyber”, simply means digital or computational interactions, which are directly linked to cyberspace – a concept that Valeriano and Maness define as “the networked system of


\textsuperscript{39} Weber, 1964.
microprocessors, mainframes, and basic computers that interact at the digital level.”

Likewise, and importantly, Nye (2011) defines cyberspace as including “…the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications. Cyberspace has a physical infrastructure layer that follows the economic laws of rival resources and the political laws of sovereign justification and control.” This latter point that Nye raises on the layered dimensions of cyberspace, particularly in terms of sovereign justification and control are particularly relevant to this research project and my theoretical framework given the physical or “real world” impacts cyber activities can and do have when it comes to regime legitimacy, control and survival, among other things. From this perspective, cyberspace is not strictly digital in nature. It is a physical, but also social-technological domain – a separate environment, where both hardware (e.g. wires and circuit boards) and information can be attacked and manipulated. However, it is also a nebulous environment that intersects and interacts with other realms. Indeed, it is not an independent domain that acts and impacts in isolation – it is one that is directly interconnected with others. I raise these points because while this research looks at “cyber attacks”, this work is ultimately about cyber activities as a means to impact these other domains. Therefore, conceptually, I approach this idea of a “cyber attack” as capturing a broader range of malicious cyber activities beyond the more traditional definition, often defined as “an attack launched from one or more computers against another computer, multiple computers or networks.”

---

Like Valeriano and Maness, my research is primarily concerned with “the use of computational technologies for malevolent and destructive purposes…”\textsuperscript{43} To note, this includes everything from shutting down and disrupting hard assets and critical infrastructure like power generators, to illicitly accessing financial institutions, to altering online content and information. Because of the broad nature of this conceptual approach which goes beyond basic attack types like “distributed denial of service”, “doxing” or “defacement”, terms or phrases throughout this dissertation such as cyber attack, cyber incident and malicious cyber activity are used interchangeably to capture a wider range autocratic behaviour in cyberspace.

\textbf{1.7 RESEARCH DESIGN & METHOD}

My proposed methodological approach takes its cue from the work of Barbara Geddes. In her 1999 paper, “What do we know about democratization after twenty years?” Geddes essentially distinguished political regimes based on a spectrum of multi-dimensional qualitative benchmarks established by both case and area studies. Geddes differentiated between single-party based regimes, military regimes and personalist regimes. However, in the time since, others such as Hadenius and Teorell (2007), Croissant and Wurster (2013), Kailitz (2013), von Soest and Grauvogel (2017), Maerz (2019) and Tannenberg et al. (2020) have followed suit and taken similar yet modified approaches by introducing new classifications, removing others, and applying slightly different methodologies to better understand authoritarian legitimation strategies and survival.\textsuperscript{44} In line with these works, and focusing specifically on personalist,

\textsuperscript{43} Valeriano and Maness, 2015.

single-party and electoral autocracies based on my analysis of the data, I undertook a multi-step approach to completing this research project. To the best of my knowledge, this dissertation is the first attempt to empirically test if authoritarian strategies in cyberspace align with the legitimation strategies expected of particular autocratic regime types. Relying on a combination of existing data on authoritarian cyber attacks, influential scholarly works on authoritarian legitimation and cyber conflict, and interviews with some of the world’s foremost experts on country-specific cyber activities, I have sought to ensure findings and results are anchored to a sound and structurally logical methodology.

As a first step, I undertook an extensive analysis of existing theories found in the literature on how different types of authoritarian regimes legitimize themselves, and what it is specific regime types rely on most to maintain power. Overall, and despite some variance in terms of typological definitions and classifications, I identified several common themes throughout the literature which form the basis of my theory, and which subsequent sections, including my case studies, are connected to. I will speak to those here briefly, with further detail on regime types and legitimation strategies provided later in this dissertation.

First, throughout the literature, it is widely suggested that personalist regimes, or regimes where power is consolidated and held by one individual, rely particularly heavily on obtaining and distributing resources to a core group of loyalists. Personalist regimes also rely heavily on


These theories are presented in more detail throughout the literature review in Chapter 2, and elsewhere throughout this dissertation.

For specific detail and analysis on how personalist autocracies legitimize their rule, see for example:
the persona and charisma of the leader, and safeguarding the integrity of their image. Indeed, as Tannenberg et al. (2020) write, personalist leaders typically look to develop an “intense personal bond with a devoted following that believes in their extraordinary qualities.” Therefore, and based on my theory, we should expect to see personalist autocracies undertake financially motivated cyber attacks, or cyber attacks which lead to them acquiring resources. Further, cyber attacks which limit attempts to criticize the ruler, or which inflict harm on people or organizations that pose a threat to the leader should also characterize cyber attacks coming from personalist autocracies.

Second, numerous authors have suggested that single-party regimes, or what some refer to as or subsume under the broader category of “closed authoritarian regimes” – rely particularly heavily on ideology to legitimate their rule. These regimes, which generally speaking, refer to those with only one legal party, also rely heavily on their commitments to developmentalist and welfarist goals in making appeals to their populations, which are often also integral elements to their ideological narratives. Subsequently, based on common theories throughout the literature on single-party regimes, we should expect to see these regime types favour cyber attacks, which, in one way or another, contribute to strengthening the ideological messaging of the regime.

Third, electoral autocracies, or those regimes which seek to nominally emulate democratic procedures and elections, typically rely more heavily on performance and rational-

---


legal justifications to legitimize their rule than other regimes do.49 These regimes, which often have at least a minimal level of competition and which tend to permit opposition candidates to participate in elections, usually seek to convince the population that for some important reason – often security related – democratic principles are not possible, or that contrary to popular belief, they do not contribute to the wellbeing of society.50 As such, and despite a less clearly identifiable pattern of legitimation than other regime types, I argue that we should expect cyberattacks emanating from electoral autocracies to be characterized by attempts to poke holes in or weaken true democracies, as well as attacks designed to limit political opposition, dissent, and exposure to other, more liberally democratic forms of governance.

Fourth, military regimes, the vast majority of which no longer exist, typically seek to legitimize their rule using some type of performance-based metric, usually involving the restoration of order and/or addressing a type of internal threat to national security (e.g. an insurgency). In addition, and unlike the other regime types mentioned above, military autocracies are usually less interested in maintaining power over the long-term. Rather, they are often more concerned with maintaining the integrity and functionality of the military as an institution, and in addressing whatever threat they have used to justify their rule, than they are in permanently controlling the government. For these reasons, and in line with my null hypothesis detailed later in this dissertation, I argue we should not expect to see military regimes carry out cyber attacks. Ultimately, these regime types and the theories they are connected to in terms of legitimation, represent the foundation of my theory. With an understanding of the literature and key theories, I

50 Kailitz, 2013.
then undertook the next phase of my research: examining the data to determine who is doing what in cyberspace.

Relying primarily on the Significant Cyber Incidents tracker administered by the Center for Strategic and International Studies (CSIS), as well as data from the Council on Foreign Relations’ Cyber Operations Tracker, and the Dyadic Cyber Incident and Dispute Dataset (DCID) administered by Ryan C. Maness, Brandon Valeriano, and Benjamin Jensen, I closely studied existing datasets on state-level cyber attacks. Taken together, and after having crosschecked the datasets, I identified approximately 350 observations of state-level authoritarian cyber attacks from 2003 to 2021. Although there were some inconsistencies across the datasets regarding which cyber attacks were or were not included (primarily because the scope of each dataset is different), key patterns – which is what I was looking for and what is most important for this research – remained consistent. In other words, across the various datasets, state behaviour remained the same. Fortunately, the datasets referenced above, which are continuously updated, have already coded the various types of cyber attacks (e.g., cyber espionage) with some even explaining the nature or specifics of the attack.\footnote{Center for Strategic and International Studies, “Significant Cyber Incidents”, \url{https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents}} This made analyzing the objective of the cyber attacks and identifying strategic patterns across different regimes much easier.

By relying on these datasets to inform my case-study selection, I identified which authoritarian countries are most active in terms of carrying out cyber attacks. These countries, China, Russia and North Korea, represent approximately 90 percent of all known cyber attacks carried out by authoritarian regimes. They also happen to be among the most widely discussed
countries throughout the literature on authoritarian regime legitimation, with a number of works classifying each regime as one of the regime types referenced above. That said, for the purposes of this project, I have decided to undertake four granular case studies – China, Russia, North Korea, and Mali, where I examine military regimes and cyber behaviour. To note, two of these case studies illustrate within-case variation – with novel findings that I have yet to see throughout the literature. Focusing on three core countries (China, Russia, and North Korea), which were teased out from the data, I then analyzed the specific characteristics of each regime, and the cyber attacks they have carried out to explore and evaluate my proposed theoretical framework. By carrying out a comparative analysis and testing my theory across different regimes with distinct characteristics, I was able to identify patterns, similarities and differences across the most belligerent authoritarian regimes in cyberspace, assessing the relationships of variants between their respective governments. This approach allowed me to clearly isolate the dependent variable of my research (the nature of a country’s cyber attacks), identify potential relationships with my independent variable (the type of regime carrying out cyber attacks), and determine linkages and variance across several countries in terms of whether key theories on authoritarian legitimation strategies hold true in the cyber domain. For each case study, empirical data was drawn primarily from open-source materials as well as from the interviews I conducted, which I speak to below. By using primary sources such as military doctrines (e.g. 2010 Russian Military Doctrine), to the speeches of key rulers (e.g. Xi Jinping), to government statements and foreign media sources, to examining specific cyber attacks, and interpretations of historical grand strategies, among other things, I undertook extensive research and analysis to test the validity of my theory.
While the rationale behind my case-selection is straightforward, some additional detail is warranted to better explain why certain countries were chosen while other authoritarian states were not. Undeniably, the universe of possible case studies goes beyond those which I have selected for this dissertation. Ultimately, choosing China, Russia, North Korea, and Mali, came down to three underlying reasons.

First, there are biases in the data, which, in my opinion, are primarily driven by the predilection of western scholars and policymakers to focus on a select handful of countries. In other words, the overwhelming majority of open-source information and data on state-level cyber behavior is produced in the West where, for several reasons (e.g., Russia’s war in Ukraine, China’s economic espionage, and North Korea’s nuclear ambitions) there is a concentrated effort on analyzing a small handful of countries – the countries detailed in this research. Other authoritarian countries, or countries which are at least commonly identified as “not free” – like Venezuela, Tajikistan, Sudan, Rwanda, Nicaragua, Laos, and many others – may very well carry out cyber attacks or malicious cyber activities designed to preserve their grip on power. However, as noted, scholars and policymakers interested in cyber conflict have largely focused their attention elsewhere, and for this reason, we do not know how these countries behave in cyberspace. Therefore, I was left with a small sub-set of authoritarian states to draw from for my dissertation. In a sense, I have been unable to analyze cyber trends or activities to the degree needed for my research emanating from countries which remain woefully under examined and absent in the data.

Second, there is indeed several other authoritarian regimes active in the cyber domain of which we have an open-source record, which I chose not to study, simply to avoid unnecessary analytic repetition. For instance, Iran is another authoritarian regime active in cyberspace with a
known record of activity. However, Iran is typically described as an electoral autocracy (or some type of electoral autocracy) – a regime type already thoroughly analyzed in my exploration of Russia. With much less publicly accessible and accurate information and data on Iran, its inclusion in this research would have – at best – only added a much more concise chapter confirming or refuting the findings detailed in the chapter on Russia. This duplication of effort was deemed unnecessary. Another example of an autocratic country active in cyberspace which I chose not to study is Saudi Arabia. Most commonly defined as an “absolute monarchy”, Saudi Arabia very infrequently appears in the datasets – usually it carries out attacks or intrusions against specific individuals or organizations critical of the regime or of Crown Prince Mohammed bin Salman. In addition to there being comparatively little information on the country’s behavior or strategies in cyberspace, neither are monarchies thoroughly analyzed or studied in the literature on authoritarian legitimation strategies. All told – issues related to unnecessary duplication, lacking data, or insufficient information on regime type contributed to my case-selection as well.

Third, while I could have potentially analyzed other single-party regimes (e.g., Vietnam) or electoral autocracies, China and Russia are widely considered the two nations driving and accelerating the erosion of liberalism and democracy worldwide. As Repucci and Slipowitz (2022) have stated, China and Russia “…have succeeded in shifting global incentives, jeopardizing the consensus that democracy is the only viable path to prosperity and security… these are the countries fueling the spread of authoritarianism, and challenging western liberal democracy. It is now impossible to ignore the damage to democracy’s foundations and
reputation.” For this reason, I argue it is especially important to study these specific countries, as other nations and leaders around the world will continue to learn from and emulate the strategies – both physical and digital – employed by Moscow and Beijing. From this perspective, the impact and importance of studying certain countries over others also contributed to my case-selection.

In sum, while there are benefits associated with my case-selection, there are also consequences or trade-offs, as well. The most glaring issue, which I discuss above, is the fact that this research focuses on the countries which we already know the most about, while neglecting to assess the cyber strategies and characteristics of other autocratic regimes carrying out attacks in cyberspace. Because of this, several potentially new findings or lessons learned remain unknown in terms of cyber conflict. Moreover, by focusing on the four primary types of regimes found throughout the literature, this research does not contribute to broadening our understanding of other types of autocracies which currently exist, or which may be emerging. Fortunately, though, I remain confident that this dissertation will make a meaningful and initial contribution to the study of how autocracies vary in their use of cyber attacks. Going forward, I hope to undertake additional research on some of these understudied cyber actors and regime types which I was unable to cover in this research.

To note, while there are often some basic uncertainties about cataloging conflict episodes of any sort, this problem is of course multiplied in the cyber realm, where many actions are either covert, or significantly blurred, making attribution challenging. However, as Valeriano, Jensen and Maness (2018) write, “there is reason to believe that publicly documented incidents

---

are a reasonable sample of the entire population of cyber coercive events.\textsuperscript{53} In a similar vein, Wilner (2019) argues that recent technological advancements have allowed countries – particularly the U.S. – to monitor and identify the perpetrators of cyber attacks.\textsuperscript{54} Additionally, cyber security firms now rush to apply attribution markers to every known cyber attack, government personnel regularly leak classified information, and perpetrators often claim responsibility, making attribution much less of an issue – at least at the state level – than many might assume. Overall, the data on cyber attacks is surprisingly thorough. As a final point on the data, it should be acknowledged that while there are a small handful of instances of authoritarian regimes (e.g. Syria) carrying out cyber attacks beyond the three key nations studied in this work, data on those cases is lacking and is insufficient to undertake standalone case studies. Therefore, I speak to the merits of exploring those cases through future research in my concluding section.

To confirm and/or strengthen my analysis, and using purposive non-randomized sampling, I completed a series of 12 semi-structured interviews with the world’s top subject matter experts in cyber conflict throughout Canada, the U.S. and Europe. The objective of the interviews was to gather additional focused qualitative data on the nature, characteristics and strategies undertaken in cyberspace by non-democratic regimes, and to complement existing case-specific literature and analysis. Relying on already well-established relationships with country specific and cyber security experts, I added additional and reliable nuance, analysis and detail to this dissertation. Through a number of funded and complementary research projects I have been involved in as part of this Ph.D. program,\textsuperscript{55} as well as my time working on cyber-

\textsuperscript{55} Research projects have included “The En-Threat Project: An Assessment of Physical and Cyber Terrorist Threats to Canada’s Energy Sector” funded by the Canadian Network for Research on Terrorism, Security and
related files at the Department of National Defence, Natural Resources Canada, and in my current role at Public Safety Canada in their National and Cyber Security Branch, I have developed a network of experts I was able to rely on for this research.

Given the tightknit community of scholars and practitioners in this field, snowball sampling occurred amongst individuals who have either worked with each other and/or who have existing trustworthy relationships. Due to the COVID-19 pandemic, all interviews took place virtually from the National Capital Region, with my proposed methodological approach benefiting from a number of things, including the fact that existing typologies on authoritarian regimes and cyber definitions are already well established. In addition, various works had already paired certain regime types with specific legitimation strategies, and various data repositories exist with significant detail on attack characteristics – with each dataset on malicious cyber activities telling the same story.

1.8 CONTRIBUTION & SUMMARY OF FINDINGS

After having studied the data and undertaken a small-n comparative case study analysis of key authoritarian regimes and their cyber attacks, I have identified a number of noteworthy findings, which at a minimum, represent new and novel affinities in terms of autocratic legitimation and authoritarian behaviour in cyberspace. First and foremost, I found that in general, key theories on authoritarian legitimation remain consistent in cyberspace. Different types of authoritarian states and leaders are pursuing cyber attacks that support whatever those specific regime types typically need or rely on to legitimize their rule: this finding reinforces my needs-based theory on authoritarian behaviour in cyberspace. Further, and in terms overall high-

Society which I completed in partnership with Dr. Alex Wilner, as well as the “AI Deterrence Project”, which Dr. Alex Wilner received funding for from the Department of National Defence.
level findings, I found that China, Russia, and North Korea are responsible for virtually all known cyber attacks carried out by autocratic states, with China and Russia alone being responsible for nearly 70 percent of them. In terms of strategic patterns, I found that on average and regardless of regime type, cyber espionage remains the most common type of cyber attack carried out by authoritarian states. While this does not necessarily challenge conventional wisdom, it is not a commonly discussed finding throughout the literature. In fact, I have come across little material suggesting that cyber espionage is the most frequently pursued strategy for authoritarian regimes in cyberspace.

As for country-specific attack patterns in cyberspace, the results are quite revealing. In the case of China, a single-party regime, over 90 percent of their known cyber attacks take the form of cyber espionage. This is by far and away the most clearly identifiable example of a country preferring a certain type of cyber attack. Moreover, and as I argue in Chapter 3, China has relied on cyber espionage operations and campaigns for two fundamental reasons: to support the grand strategic narratives and visions of the party and specific leaders, and to spy on and silence a wide range of dissidents and entities critical of the regime. These cyber strategies align with key theories on single-party regime legitimation, in that single-party regimes typically rely on narrative and ideologically driven legitimation strategies, which often take the form of delegitimizing and silencing opposition. To note, I also observed within-case variation, with China’s cyber attacks taking on a more personalist nature as Xi Jinping has increasingly consolidated power since assuming power in 2012-2013. In other words, as China’s government has gradually moved away from the collective leadership model of a single-party regime, towards a more personalist dictatorship under Xi, the country’s cyber attacks have become more focused on preserving Xi’s image, and reinforcing aura as the father of the nation.
When it comes to Russia, I have determined that nearly 40 percent of their attacks are criminal in nature, with a clear emphasis on denial of service (DoS), damage, disruption and defacement. While Russia – like other autocratic regimes – prioritizes cyber espionage, they also use cyberspace to inflict harm on their adversaries, signal capabilities and coerce actors, both state and non-state, who pose a threat to the Kremlin. However, unlike other authoritarian regimes, roughly 20 percent of Russia’s cyber attacks are designed to spread disinformation, often times related to manipulating voter decision making, public opinion, and electoral processes and results in rival nations. This is a key finding, not only because Russia is an outlier in this regard, but because it speaks to the fact that Russia, an electoral autocracy, leverages cyber operations to undermine and discredit Western liberal democracies in an attempt to strengthen their own illiberal form of governance at home.\(^{56}\) Scholarly literature on electoral autocracies also suggests that in addition to often refuting the notion that liberty and executive constraints bestow wellbeing to the people, electoral autocracies tend to argue that for some important reason(s) – generally security related – democratic liberties are not possible. In the case of Russia – where the regime perpetuates the idea the country is under constant threat – their behaviour and justification for controlling the information domain in cyberspace aligns with this theory. In addition, and similar to the case of China, Russia’s cyber attacks have become more personalist in nature as President Putin has gradually consolidated his power over the last decade. All told, while Russia’s cyber attacks are more diverse in nature than the other countries profiled in this research, these findings on information warfare, manipulation, election

\[^{56}\) Adam Hulcoop, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert, Tainted Leaks: Disinformation and Phishing With a Russian Nexus (Citizen Labs May 2017).
interference, and the continuation of conflict with adversaries, support existing theories on how electoral autocracies’ seek to legitimize themselves and maintain power.

In the case of North Korea, I found that a third of their cyberattacks are financially motivated. Further, and more telling, is that the “Hermit Kingdom” is responsible for 90 percent of all known financially motivated cyber attacks carried out by authoritarian regimes. I have also confirmed that North Korea is the only known state in the world to use ransomware attacks for financial gain. In fact, as Caesar (2021) recently wrote, “units of [North Korea’s] military-intelligence division, the Reconnaissance General Bureau, are trained specifically for this purpose.” Again, like other countries examined and analyzed in this dissertation, North Korea seems to prioritize cyber espionage, but when it comes to cyber attacks designed to illicitly obtain financial resources, Pyongyang is clearly an outlier. Detailed in the North Korean case-study, I argue that in-part, the regime focuses so heavily on financial cyber attacks because it is a personalist regime, headed by Supreme Leader Kim Jong-un, and as the literature on authoritarian legitimation suggests, personalist regimes are particularly vulnerable when “calamitous economic conditions disrupt the material underpinnings of regime loyalty.”

Finally, in addition to China, Russia and North Korea, I did not find any cases of military regimes carrying out cyber attacks in the data. While there have been recent instances of at least one military regime increasing their internal control of the Internet, this dissertation is interested in cyber attacks carried out abroad. Regardless, because there is value in exploring why military

58 Barbara Geddes, ”What do we know about democratization after twenty years?” Annual Review of Political Science, 2, 1999.
regimes do not appear to carry out cyber attacks, a more concise chapter on military regime legitimation, where I use Mali as a case study, is provided in Chapter six.

1.9 ROADMAP AND NEXT SECTIONS

In the following chapter, several key categories of literature are detailed which include the foundational theories on cyber conflict and cyber strategies, and core theories related to authoritarian variance and regime legitimation. Further, this next chapter also speaks to gaps in the literature, and how this dissertation contributes to filling them. Through this combination of disciplines and delving into the main works throughout each sphere of literature, my dissertation identifies several common themes and connections, which form the basis for my theory on authoritarian legitimation in cyberspace. Following these next sections in Chapter 2, including an overview of my needs-based theory on autocratic variance in cyberspace, I then move into theory testing through individual case studies on China, Russia, and North Korea, with a fourth and more concise chapter on military regimes and Mali.
CHAPTER TWO

TOWARDS A THEORY ON AUTOCRATIC BEHAVIOUR IN CYBERSPACE: UNDERSTANDING WHY DICTATORS VARY IN THEIR USE OF THE DIGITAL REALM

With the intensification of cyber conflict and cyber operations over the last number of years, there has been a proliferation of scholarly cyber-related work. However, on the whole, this literature remains relatively nascent, and has yet to tap into or create connections with other potential spheres of study within the field of political science and the insights that come with them. Further, the overall body of work looking at cyber conflict tends to focus heavily on the theoretical, at the expense of empirical research, with a clear gap when it comes to granular case study research and quantitative/qualitative analysis. My dissertation addresses this gap. In this chapter, I review somewhat disparate literatures from the general body of work produced on cyberspace as a domain of conflict, as well as relevant works related to authoritarian legitimation strategies. Beginning with an overview of relevant works related to cyber deterrence and cyber strategy, I concisely address key works that are of value to or intersect with this dissertation, and which contribute to my theoretical framework. Following these sections, I review the most important material produced on authoritarian legitimation strategies – some of which were recommended to me by leading scholars studying the ways in which authoritarian regimes seek to preserve their rule.

2.1 CYBER STRATEGY

Surprisingly, few scholars have sought to analyze cyber strategy and the determinants of cyber warfare in any comprehensive, methodologically rigorous way. Instead, the vast majority of literature on cyber warfare, strategy, and decision making in cyber conflict is premised on
what Valeriano and Maness characterize as “spectacular flights of the imagination.” More specifically, Valeriano and Maness write that “cyber strategies and analysis at this point are entirely “anti-theoretical” and that “there is a sizable gap between a constructive analysis of a critical international process and the actual evaluation of cyber interactions.” However, over the last decade, a small handful of works have emerged throughout the IR literature, in which attempts have been made to develop theories related to the use of cyber technologies in conflict and warfare. These theories tend to revolve around the ideas of domestic growth influencing international behaviour (Choucri 2012), restraint and regionalism (Valeriano and Maness 2014; Gartzke 2013), opportunity and the exploitation of system weaknesses (Valeriano and Maness 2015) and interstate competition and social constructs (Craig and Valeriano 2016; Stadnik 2019).

Choucri for example suggests that internal or domestic variables, including resources, technology and population, and the degree to which they grow and impact a nation’s abilities to exert influence abroad, is what will determine whether or not a country pursues cyber attacks internationally. Others, such as Valeriano and Maness focus their theories on disproving or tempering the doomsday rhetoric that has permeated through scholarly works and which has driven international policy development. They write that “cyber conflict is literally the least harmful tactic and easiest option for a state during conflict” and that cyber interactions are restrained episodes of regionally isolated disputes amongst rivals. Likewise, Gartzke takes a similar approach, writing that cyber attacks are a form of low-level interstate disputes that are restrained, as those who possess the most advanced capabilities in cyberspace realize the

60 Brandon Valeriano and Ryan Maness, Cyber War Versus Cyber Realities, Oxford, Oxford University Press, 2015; 87.
62 Valeriano and Maness, 2014; 349.
potential consequences to devastating attacks likely outweigh the benefits. In the same way that the use of nuclear weapons and the spectacular attacks they cause are restrained methods of comprehensive deterrence, so too according to Valeriano, Maness, and Gartzke, are the use of devastating cyber attacks, or those which could cripple a nation’s critical infrastructure, access to vital services, or abilities to sustain itself.

Instead of seeing massive, large-scale cyber attacks taking place amongst states, Valeriano and Maness argue that rivalries are the main entities that will use and integrate cyber interactions into their conflict toolkits. They argue that generally, attacks would be carried out in restrained manner, through isolated regional interactions characterized by other ongoing disputes on contentious matters of significance, such as territorial or regime status issues. Additionally, Valeriano and Maness spell out a theory of cyber espionage and the use of cyber terrorism at the state level. From their perspectives, states use some of their least sophisticated, least disruptive abilities in cyberspace to achieve highly surgical objectives in situations where an opportunity or weakness in a rival’s defences presents itself – what we are left with is “spy craft, not warfare.” Operations are undertaken in a very constrained way with the intent of exploiting weaknesses, while at all costs, avoiding any unnecessary escalations in the use of cyber attacks, or other forms of war fighting. Similarly, when it comes to cyber terrorism, Valeriano and Maness write that states will support cyber terrorists when the conditions are conducive to do so, when weaknesses in a target state are identifiable and exploitable, and when there is an opportunity for a smaller, weaker state to punch above its weight, and disproportionately impact a more powerful rival through a non-state actor.

---

64 Valeriano and Maness, 2015; 49.
In line with my own theory, which I detail in the following section, Valeriano and Maness often include social and/or psychological considerations into their theories on cyber strategy and conflict.\textsuperscript{65} They argue that social perspectives and concerns regarding cyber attacks, whether they be real or imagined, dramatically impact and influence how states respond to the threat environment, and that without taking action to securitize itself from these cyber threats, a state could be seen as irresponsible and may open itself up to criticisms or political vulnerability. Similarly, Craig and Valeriano find a relationship between the build-up of cyber capabilities and mutual perceptions of threat and competition between states wherein the fears or perceptions of threats are stoked by the increased discourse regarding the militarization of cyberspace, as well as new military organizations dedicated to cyber, and increased cybersecurity budgets.\textsuperscript{66} In their view, the nature of and response to cyber threats are socially constructed by a wide range of factors, including government messaging, the persuasiveness of media, and popular culture. Furthermore, they argue that the actual attacks themselves and the responses to those operations are socially constructed by the overall situation of interstate rivalry and its history, the system of norms in place at the time, and the nature of fear-based responses in the attacked or threatened society.\textsuperscript{67} Similarly, Dunn Cavelty (2014) suggests that cyber-related issues and/or threats (e.g., cyber crime and cyber espionage) are “represented and treated in a distinct way in the political process: Multiple actors employ different political, private, societal, and corporate notions of security to mobilise (or demobilise) different audiences.”\textsuperscript{68} Others, such as Lupovici have also

\textsuperscript{65} For another, more robust social constructivist take on cyber conflict, see Ilona Stadnik, “US-Russian Relations in Cybersecurity: The Constructivist Dimension”, European Conference on Cyber Warfare and Security, July, 2019.
\textsuperscript{66} Anthony Craig and Brandon Valeriano, “Conceptualizing Cyber Arms Races”, 8\textsuperscript{th} International Conference on Cyber Conflict, NATO CCD COE Publications, 2016.
\textsuperscript{67} Valeriano and Maness, 2015; 51.
applied constructivist thinking to cyberspace, suggesting that perceptions of such things as violence in the cyber realm, as well as the norms created around attribution and retaliation are socially manufactured and created.69 These works dealing with constructivist theories and norms in cyberspace play an important part in my research.

Having covered cyber strategy, as well as the small handful of theories that are most complementary and/or applicable to my own, I will now speak to some of the more relevant material on how authoritarian regimes vary, and how this material is applicable to this dissertation.

2.2 AUTHORITARIAN VARIANCE IN MAINTAINING POWER

Literature on authoritarianism has provided key insights into the internal workings of non-democratic polities. However, this large and growing body of literature, some of which differentiates between authoritarian subtypes, tends to focus disproportionately on institutional composition, while largely ignoring the different legitimation strategies each type of regime favour, despite the fact that “even very coercive regimes cannot survive without some support.”70 Only a handful of works have analyzed authoritarian regimes’ different legitimation strategies (Burnell, 2006; Gerschewski, 2013; Kailitz, 2013; von Soest and Grauvogel, 2017; Haldenwang, 2017; Dukalskis, 2017; Dukalskis and Patane, 2019; Maerz, 2019; and Tannenberg, Bernhard, Gerschewski, Luhrmann and von Soest, 2020), though many others have undertaken granular, state-specific analyses. While material on general authoritarian legitimation strategies vary in nature, intent and methodology, the general underlying assumption and finding of each is that

different types of autocracies also vary in their claims to legitimacy. This also means that different types of autocracies are particularly vulnerable to certain things that could lead to their breakdown (e.g. poor economic performance). Furthermore, these select works all reach relatively similar conclusions in terms of how different authoritarian regimes seek to gain domestic legitimacy, thereby maintaining or preserving their power positions. On that, I have identified three common findings or legitimation strategies throughout the literature on regime maintenance that are integral to the theoretical framework of my research.

First, output-based performance and procedural related claims (i.e. claims related to socio-economic issues, security and governance) are of significant importance to all authoritarian regimes, though to some – namely electoral autocracies – it seems to matter more.\(^\text{71}\) In other words, authoritarian regimes that draw heavily on performance and procedure-based legitimacy are particularly vulnerable to factors that reduce their ability to meet the needs, wants and expectations of the people. Furthermore, as Burnell explains, authoritarian regimes are particularly “vulnerable to whatever causes society to believe that the regime cannot or soon will prove unable to meet people’s needs, wants and aspirations, such as in the event of a major ‘exogenous shock’.”\(^\text{72}\) Risks of growing dissatisfaction with an autocratic regime’s performance (or expected future performance), resulting primarily from a change in society’s wants, needs, expectations and/or aspirations can and has, according to the literature, been a deciding factor in terms of the longevity and resilience of authoritarianism in various states.\(^\text{73}\) In some cases, one external factor that can exacerbate this is exposure to international dialogue, or connectivity with

---


\(^{73}\) Burnell, 2006.
other nations. Foreign criticisms, or perhaps even more importantly, exposure to a better and/or more appealing life can contribute to the erosion of an authoritarian regimes’ legitimacy. In line with some of the theories on cyber deterrence, this idea is particularly useful to my dissertation in terms of how different states use cyberspace as means to oppress and manipulate domestic populations.

Second, virtually all scholars who have assessed governance transition variables believe that poor economic performance increases the likelihood of authoritarian regime collapse.\(^74\) However, certain forms of authoritarian regimes – namely personalist regimes – rely particularly heavily on economic performance as a form of regime legitimation, at least in terms of providing material support to actors with a strategic relevance to the regime, or what Bueno de Mesquita refers to as, members of the “selectorate.”\(^75\) In short, it is a common argument throughout the literature on authoritarian regime maintenance that authoritarian governments, like others, need to be able to provide benefits and resources to their inner circle and active supporters as a means to ensure continued, long-term acquiescence. This is particularly true during periods in time when other factors may otherwise challenge the legitimacy of the regime or ruler.\(^76\) As Barbara Geddes argued, “as long as economies functioned well enough for personalist leaders to provide supporters with access to opportunities and resources, the supporters remained committed to the regime.”\(^77\) This theory, which is validated throughout the literature on authoritarian regime legitimacy, plays a key role in my theoretical framework. Ultimately, as I explain in detail in the following section, I argue that depending on the type of authoritarian regime, cyber-attacks may

\(^74\) Geddes, 1999.
\(^76\) Geddes, 1999.
\(^77\) Geddes, 1999, 139.
be used primarily as a form of obtaining financial resources, and maintaining an acceptable, passable level of economic performance, or at least as a means to line the pockets of elite supporters.

Third, the construction and/or continuation of certain narratives and ideologies are crucial to authoritarian regimes, though again, this legitimation strategy matters more to some than others – specifically single-party regimes. Comparing open electoral authoritarian regimes (those that have at least nominally democratic institutions and elections) versus “closed” regimes (those which prohibit public political contest and participation), von Soest and Grauvogel find that closed regimes rely predominantly on identity-based legitimation strategies wherein, references to the regime’s ideology, its foundational myth and/or the ruler are integral to their strategies of regime maintenance. Furthermore, and relevant to my research is that these aggressive campaigns to drive particular ideological narratives are often exported abroad as a form of domestic legitimation. Speaking to this point specifically, and using the term ‘externalization,’ Dzhuraev (2012) describes how leaders leverage their country’s role in foreign arenas “as tools in manufacturing domestic legitimation.”\textsuperscript{78} Relatedly, the construction or reliance on a specific ideological narrative often feeds into the demonization of foreign entities, or external enemies, even in cases where in reality, these threats and the labeling of these enemies are politically constructed as a form of authoritarian regime maintenance. Explained further in the next section, this common argument is very relevant to my research in that my dissertation shows that cyber strategies of countries where domestic control and narrative/ideological prolongation is crucial, reflect this need.

In addition to these main legitimation strategies, I have also identified what I consider to be four foundational regime types which – while varying to certain degrees – appear to be the primary underlying classifications across most works. These regime types – personalist, electoral, single party, and military – are by no means the only ways authoritarian regimes are classified, but rather they represent the four most prominent and commonly discussed regime types throughout the literature, which have emerged as an outgrowth of Geddes’ introductory work on this topic.

As for the types of regimes found throughout the literature, and as I have noted, personalist autocracies are one of the foundational types commonly discussed. Geddes describes personalist as those where an individual takes power, and continues to garner support from a core base while limiting their influence. Often times, personalist regimes operate on shaky ground, where access to financial resources and the ability to line elite pockets with resources is the underlying strategy to maintain power and mobilize legitimacy. Like Kailitz (2013), who writes that “as soon as the personalist autocrat cannot provide enough “booty” to provide to his personal gang, they will start to look for an alternative,” numerous other scholars have focused on regime performance and prioritizing elite interests as being the fundamental legitimation strategy of personalist autocracies. Kosterina (2017) for example writes that “elites are unlikely to support a costly coup if the leader’s actions do not harm their interests” while Frantz and Kendall-Taylor (2017) write that “if resources dry up, the dictator becomes vulnerable to defections of the regime elite.”

---

propensity of personalistic leaders (e.g. Kim Jong-un) to initiate conflict or pursue belligerent international activities relative to other regime types. Numerous studies have found that personalist regimes are more likely to initiate conflicts than both democracies and other forms of autocratic regimes. As Weeks (2012) notes, “given the treacherous road to power in a personalist dictatorship, these unconstrained leaders are often precisely the types of individuals who seek out international conflict and can survive defeat, only to repeat the cycle.” That said, in addition to this research exploring linkages between theories on authoritarian legitimation and cyber attacks, I suspect this research will also be the first, or among the first, to determine whether a certain autocratic regime type has any connection to the initiation of cyber conflict.

Today, electoral autocracies – sometimes referred to as “competitive autocracies” – are the most widespread form of non-democratic governance. In short, electoral autocracies tend to legitimize themselves by focusing on ‘adequate’ political procedures and exercising a system of governance where there is a perception the person or party in power could conceivably be challenged through an election. As Schedler (2006) notes, electoral authoritarian regimes “violate the liberal-democratic principles of freedom and fairness so profoundly and systematically as to render elections instruments of authoritarian rule rather than instruments of

---


democracy.” As a way of legitimizing their regimes, electoral autocracies will often either directly deny that liberty and executive constraints contribute to the betterment of society, or they argue that as a result of some pressing issue(s) – most often security related – the regime is unable to facilitate those things. Ultimately, the introduction of multiparty elections, regardless of their invalidity and manipulation, gives the authoritarian ruler or regime the pretense of democratic legitimacy. Throughout the literature, this is commonly referred to as the ‘democratic-procedural’ mechanism of autocratic legitimation. Beyond giving the citizenry the impression they have a say in the country’s governance, nominally democratic institutions and practices such as elections and legislatures, assist the regime in managing intra- and inter-elite dynamics and relationships, while also promoting power sharing and co-optation, fragmenting opposition fronts, and limiting the extent to which the regime may need to rely on overt repression. Procedural legitimacy aside, electoral autocracies can, in some instances, help rulers pursue and realize performance-based legitimation through the delivery of certain social services, which is particularly salient for the legitimation of rulers that are not democratically elected, and for their political (and potentially literal) survival. Interestingly though, scholars studying electoral autocracies have noted that the introduction of even partial liberalisation in the political sphere can open a range of risks, including the potential for political change, changing “dormant”

political dynamics, and even ushering in – depending on the level of performance and the acceleration of human development – democratization. For these reasons, electoral autocracies have to strike the right balance between allowing some political participation and openness, but not enough that it threatens their regime. Indeed, as Cassani notes, “socioeconomic progress tends to refocus popular aspirations towards political demands, and gives civil society more bargaining power.”

There are also single-party regimes, which Geddes defines as those where “access to political office and control over policy are dominated by one party, though other parties may legally exist and compete in elections.” Single-party regimes, like the other regime types covered in this dissertation, also vary in terms of their characteristics and composition. However, when it comes to legitimation strategies, the literature suggests that single-party regimes tend to favour legitimation strategies that revolve around narratives and ideologies. Narratives could include “rally-around-the-flag” sentiment (Grauvogel and Von Soest, 2014), international legitimation messaging where the regime purports to support or influence foreign movements or governments (Del Sordi and Dalmasso, 2018; Hoffmann, 2015; Holbig, 2011), as well as delegitimation strategies aimed at preventing opposition actors – both domestic and foreign – from gaining support (Dukalskis and Patane, 2019). Dukalskis and Patane (2019) actually found that single-party regimes are not only the most active autocratic regime types in terms of legitimizing their rule and propping themselves up, but that they also favour delegitimizing their rivals more than any other autocratic regime type as well.

---

89 Geddes, 1999, 121.
Finally, military regimes are the other core regime type found throughout the literature, which Geddes defines as one where a “group of officers decides who will rule and exercises some influence on policy.”\textsuperscript{90} Essentially, a military regime is a form of government wherein the political power resides with the military. According to the literature, military regimes differ significantly from the other regimes discussed in this research in two main ways. First, it is widely discussed throughout the scholarly material on autocracies that military regimes are less interested in holding on to power than other regime types. Rather, they are more concerned with the survival and efficacy of the military as an institution than anything else. Several authors, including Janowitz (1960 and 1977); Finer (1975); Bienen (1978); DeCalo (1976); Kennedy (1974); Van Doorn (1968 and 1969); Geddes (1999); Kailitz (2013); and Kailitz and Stockemeyer (2015), discuss this. Second, military regimes typically base their legitimacy around addressing an internal threat the country is facing, but which is being insufficiently addressed by the civilian government they have taken power from. Often, this takes the form of restoring order, and addressing a specific threat to national security.\textsuperscript{91} Essentially, they base their rule on a performance-based narrative, but as several authors note and as I detail in my chapter on military regimes, they typically lack any long-term justifiable claim to legitimacy – something other regime types do not.

To reiterate, while the literature on authoritarianism is vast, the actual sub-set of work related to regime maintenance and legitimation strategies is quite small, with only a handful of noteworthy papers or studies assessing how different authoritarian regimes vary in this way. Throughout my dissertation, I will provide a more granular and comprehensive analysis of how

\textsuperscript{90} Geddes, 1999.
\textsuperscript{91} Tannenberg et al., 2020.
authoritarian regimes vary in their legitimation strategies will be provided, at least when it comes to specific autocratic regimes (e.g. China). Here though, the purpose has been to identify the most relevant theories in the literature, and to provide the readers with a sense of how this portion of the literature is relevant, and what role it will serve as part of my theoretical framework and research.

Overall, works on cyber strategy and authoritarianism provide insightful lessons and theories which when removed from their silos and applied to one another, lead to new and enriched ways of thinking about why states behave the way they do in cyberspace. However, despite each body of work containing theories and ideas applicable to my own research, there remain a handful of conspicuous shortcomings that deserve mention.

2.3 ASSESSING THE LITERATURE: USEFUL THEORIES AND GLARING GAPS

In sum, when it comes to works on cyber strategy, there has been only a handful of scholarly material produced which attempts to develop a theory of cyber strategy, and which moves the needle slightly closer to an understanding of why countries might pursue certain strategies in cyberspace over others. Of these, few have sought to look at the actual determinants of cyber attacks – rather, they are more so interested in unpacking the characteristics of cyber conflict. Works by Valeriano, Maness and Jensen, which involve theories on restraint, regionalism and rival antagonists, are the most useful in terms of building towards my own theory, and yet they fall short in focusing on why countries behave the way they do in cyberspace. I have identified three specific gaps in particular, which are a hindrance to comprehensively understanding strategic choice and behaviour in cyberspace.
First, despite a rapidly expanding body of scholarly work on cyberspace, there has been little to no empirical work carried out that extends core political science theories to the cyber realm, and no attempts made to comprehensively answer my question related to variance in the use of cyber as an instrument of power. While Valeriano and Maness have produced the most significant empirical research (maybe even the only) on cyber interactions among states, they have not undertaken specific research related to why certain countries appear to gravitate towards specific forms of attacks. Second, with more and more cyber attacks of various sorts emerging by the day and real-world cyber events outpacing the abilities of researchers to keep up, a majority of the literature is based on conjecture and focuses on the “what if,” as opposed to exploring the determinants of behaviour, underlying causes and strategic interactions between states or groups. Third, data within the literature is lacking, or due to the aforementioned reality of events outpacing research, is quite dated. The data is out there, and indeed, it is used for this dissertation, but most works do not attempt to draw from it in any substantive way. Infosec researchers have a dataset specific to Advanced Persistent Threats, the Council of Foreign Relations has an impressive “Cyber Operations Tracker,” CSIS has their “Significant Cyber Incidents” data, which is what I have relied primarily on for this thesis, and Valeriano and Maness have their own dataset. Yet we do not see analysts using data to understand why countries vary in how they engage in cyber attacks.

Cumulatively, the literature on cybersecurity is expanding rapidly and covers a wide range of topics and scenarios, and yet it only offers partial explanations of interstate behaviour in cyberspace. Moreover, it offers little to no analysis on why states gravitate towards or favour some forms of malicious cyber activities over others. Therefore, this research looks to address these gaps and limitations. This project takes theories on how authoritarian legitimation and
regime maintenance strategies vary, and test them against cyber realities. I will also introduce and test a new theory on the proliferation of state-level cyber attacks worldwide, based on the ideas of regime maintenance and domestic legitimation. This dissertation also sheds some additional light on crucial theories covered in this section, particularly those on restraint, rivalry and regionalism. Finally, this research will for the first time take existing datasets on cyber attacks, assess them, and determine what it is exactly the data says about cyber conflict, cyber strategies, and whether or not these theories are confirmed or contested by actual events.

2.4 EXPLAINING MY THEORY ON WHY AUTHORITARIAN REGIMES VARY IN THEIR USE OF CYBERSPACE

In this section, and based on scholarly arguments drawn from the aforementioned literature, I introduce a needs-based theory of cyber conflict and cyber strategy centered on the concepts of regime maintenance and domestic legitimization. Complementary to and influenced by previously discussed theories and literature on how different types of authoritarian regimes tend to vary in their approach to maintaining power, I suggest that different types of authoritarian regimes will use different cyber strategies to fulfil or service the strategy or outcome they need most to maintain domestic support and legitimacy. Using a combination of Geddes’ (1999), Kailitz’ (2013) and von Soest and Grauvogel’s (2017) works in terms of how they define different types of authoritarian regimes, as well as their theories on how different types of authoritarian regimes survive (or not), I extend these theories to the cyber domain, and the preferred cyber strategies and attack patterns of certain countries. More specifically, I focus on electoral autocracies, personalist, single-party, and military regimes.

I expect that if a specific regime type is particularly reliant on output-based performance claims, whether they be security-related (i.e. providing domestic security and protection from
external threats), distributional in nature, woven into the appearance of a regime as a guarantor of stability, or in some other manifestation, that their use of cyberattacks will reflect this. Alternatively, if a specific regime type is particularly sensitive or vulnerable to poor economic performance, or reliant on economic performance as a means of regime legitimation and survival, I anticipate the findings of my research will point to an emphasis on cyber attacks targeting financial resources or cyber activities which lead to economic gain. Likewise, if the ideological cohesion of a regime or the narrative it relies on is inextricably linked to its survival, and is rooted in things such as the vilification of foreign actors and the suppression of dissent or political opposition at home or abroad, I anticipate their cyber strategies will be geared towards mitigating those vulnerabilities and strengthening that legitimation strategy. Finally, if a particular regime bases their legitimation strategy on achieving a short-term domestic objective, I do not anticipate seeing that regime type undertake cyber attacks. Figure 2.1 below offers a basic illustrative description of the logical flow of my theory:

In addition to my theoretical framework relying heavily on the authoritarianism research, previously discussed works on restraint, regionalism, and rivalry also contribute to my theoretical framework, albeit through a slightly different approach. While Valeriano and Maness suggest, and rightfully so, that the cyber threat landscape has been characterized by restrained interactions, and regional disputes amongst rivals, I suggest that they have missed the mark in identifying the underlying reasons as to why this is the case. Whereas Valeriano and Maness point to such things as fear of escalation in conflict, unacceptably large collateral damage, and the potential dangers of inadvertently dragging in uninvolved third parties as key reasons why we

---

see the types of attacks we do, I point to alternative explanations which are informed not by theoretical conjecture, but by empirical realities.

While other scholarly attempts to develop theories on cyber strategy revolve primarily around ideas such as risk aversion and fear, my theory revolves around needs. Instead of fear dictating behaviour, my research will show that cyberspace can be used in a relatively measured and constrained manner to achieve significant results in terms of bolstering domestic legitimacy and support, or at least mitigating threats to the legitimacy of the regime.

**FIGURE 2.1: An Extended Theory of Authoritarian Legitimation to Cyberspace**

More specifically, given the digital dependencies of state-level critical infrastructure and systems (e.g. energy systems, all major economic activities, core telecommunications, etc.), as well as the reliance global populations have on cyber infrastructure (e.g. social media), autocracies can strike and manipulate whomever they please, using tactical, less carnivorous measures than they maybe otherwise would have favoured. Without using conventional means of
force, countries are now able to manage the escalation of conflict between those they are targeting, while simultaneously realizing large returns on their investments at home – specifically in terms of regime survival. Evidently, cyberspace has become an extremely effective forum through which states can achieve specific goals, or get what they need most to preserve their “right to rule,” through low-cost, low-risk attacks and intrusions.

With these ideas in mind, and drawing primarily from the relatively nascent literature on authoritarian legitimation strategies, I have developed the following hypotheses, which I will explore through my dissertation:

**Hypothesis 1**: If an authoritarian regime is personalist, then the cyber attacks that country carries out are more likely to be characterized by obtaining access to financial resources.

**Hypothesis 2**: If an authoritarian regime is a single-party, then the cyber attacks that country carries out are more likely to be characterized by cyber activities that target entities which challenge that narrative, or which are critical to the continuation of the regime’s messaging.

**Hypothesis 3**: If an authoritarian regime is an electoral autocracy, then the cyber attacks that country carries out should be characterized by output-based claims to legitimacy, such as targeting external threats or enemies, whether they be real or imagined.

**Hypothesis 4**: Military regimes are less likely to carry out cyber attacks.

**Null Hypothesis**: If a regime does not face any significant threats in terms of its survival, or in terms of threats to the legitimacy of the regime, it will not engage in any significant cyber attacks.
2.5 A NOTE ON SCOPE, LIMITATIONS, INTENT AND EXPECTATIONS

Despite Geddes suggesting that autocracies “differ from each other as much as they differ from democracy,” the task of identifying political regimes based on these differences is difficult.\(^{93}\) Indeed, studies of a large number of regimes, including those that inform the basis of my theoretical framework, run the risk of being overly superficial or even misleading given that deep qualitative investigations of all regimes cannot be made. Further, it cannot be assumed that because, for instance, von Soest and Grauvogel classify China as a single-party regime that others could not or would not make the case that China, because of the grandeur and role of President Xi Jinping, ought to be considered a personalist autocracy, or perhaps, a mix of both. These issues apply to virtually all regimes, though to some it is more pronounced. Along these lines, Wahman, Teorell and Hadenius (2013) write “authoritarian regimes are often negatively defined as being regimes that do not meet certain criteria of democracy. Non-democratic regimes are not, however, a homogenous group, but employ different sets of institutions. These varying constellations of institutions may produce different outcomes and create distinct regime logics.”\(^{94}\) However, for the purposes of this research, I use compelling and rational classifications for the small handful of regime types and regimes I examine. This is sufficient in that my approach is only concerned with the general patterns of legitimation, and determining whether or not certain state-level behavioural patterns on cyberspace align with those generalities in terms of legitimation. My case studies also explore works on certain country’s legitimation

---


strategies that add nuance and further contextualize the specific strategies certain autocrats use to prop-up their regimes.

Similarly, legitimation strategies are not easily characterized. At a minimum, and as Johannes Gerschewski (2013) notes, authoritarian regimes do not simply rely on legitimation strategies in and of themselves, or in isolation. Rather, they tend to rely on a combination of legitimation efforts, repression and co-optation to increase their chances of staying in power.95 Others though, such as Maerz (2018) expand on these three pillars and provide a finer-graded picture of authoritarian survival strategy, with configurations like “hegemonic, performance-dependent, rigid, overcompensating and adaptive authoritarianism.”96 However, regardless of this variance, or how different scholarly works approach authoritarian survival strategies, they tend to agree that regimes can and do vary quite markedly in terms of how they institutionalize, combine, and apply strategies of repression, co-optation and legitimation. Further, virtually all works in the nascent strand of regime survival literature on legitimation acknowledge, “recent research efforts have gradually lost sight of the legitimation dimension.”97 In other words, works and theories that emphasize ideas like ideology and terror, socio-economic factors and repression and co-optation continue to dominate the literature, with works focusing on autocratic legitimation taking a backseat.

In addition, there could potentially be other theoretical perspectives that explain authoritarian variance in cyber behaviour. For instance, country size, location, and the relative

---

geopolitical position of a nation within a broader international hierarchy could be contributing factors in terms of why a country behaves one way or another in cyberspace. International legitimacy – as opposed to domestic legitimacy – may be another alternative reason that explains variance in the dependent variable. Indeed, chapters throughout this research do touch on and contain elements of other potential explanatory variables, but primarily, for the purposes of this research, I have focused on undertaking an exercise in extending existing theories to the cyber domain with a view to explain why certain autocracies favour certain types of malicious cyber activities over others.

I raise these points because this theoretical framework and these hypotheses are just that – a framework. There is no single theory or pathway that can explain different authoritarian cyber strategies. Nevertheless, there should be some overarching organizational framework that helps differentiate the ways in which autocratic regimes behave in the digital realm. Further, there should be some attempt or initial research at taking this emerging sphere of scholarly inquiry on authoritarian legitimation, and extending it to a space that takes into account the utility cyberspace and technology writ large will have on the abilities of autocratic leaders to remain in power. As I have noted, in addition to the use of technology to maintain power, autocracies also rely on other more egregious strategies, such as overt repression and violence, to increase their chances of survival. Therefore, the case studies within this dissertation take a comprehensive assessment of the specifics of each regime, adding nuance and contextualization beyond simply taking the regime and linking it with a legitimation strategy found in the literature.

98 I would like to thank both Dr. Michael Manulak at the Norman Paterson School of International Affairs, as well as Dr. Myriam Dunn Cavelty for raising these important points and potential alternative explanations worth pursuing through further research.
CHAPTER THREE

CHINA: CYBER ATTACKS AND REGIME LEGITIMATION

3.1 INTRODUCTION

China has been carrying out cyber attacks against its adversaries for decades. However, the country was not always a formidable threat actor in cyberspace. Indeed, in the late 1990’s, cyber operations emanating from China were relatively low-level, unsophisticated attacks designed to signal patriotism and showcase Chinese abilities to hit targets in the digital realm. Over the last twenty-plus years though, and particularly over the last decade, China has evolved into one of the most advanced and prolific actors in cyberspace, where it has persistently pursued two main strategies. First, the country has exhibited a sustained prioritization of stealing technical expertise, data, intellectual property, and sensitive technologies from rival nations worldwide. Second, cyberspace has proven to be an effective tool the CCP has strategically managed and exploited to control information – domestically and abroad – to protect the regime from criticism, embarrassment and dissent. Speaking to this latter point, Hachigian wrote in 2001, “as Internet users [in China] have multiplied, cyber-police have stepped up their prosecution of Internet content violations. Democracy organizers, human-rights activists, Falun

---


Gong members, scholars, and other dissidents have been arrested for on-line crimes.”\textsuperscript{101} In the years since, China has been able to further exploit its ‘netizens’ and diaspora population’s use of the internet to insulate the CCP and strengthen the regime’s political legitimacy and security at home. These two strategies, fostering technological development and global technological supremacy, along with shielding the CCP from criticism and dissent, are China’s two top priorities in cyberspace. As explained further in the following sections, these objectives, and China’s cyber strategy writ large, is driven by one overarching domestic imperative: legitimizing the regime and protecting the longevity of the CCP.

While many scholarly works comprehensively assess China’s use and abuse of cyberspace, very few seek to unpack why China behaves the way it does in the cyber realm. I argue that exploring China’s history of cyber attacks through the prism of autocratic legitimation is a crucial and overlooked element of the broader puzzle that warrants further examination. Therefore, this chapter on China focuses specifically on how the CCP uses cyberspace as a means of regime legitimation, providing evidence that supports my overarching argument: authoritarian regimes will prioritize and favour certain types of cyber attacks over others, depending on the type of regimes they are. To remind, I have classified China as a single-party regime based on the fact the country has only one party, which represents the \textit{sine qua non} of political power. Further, and as the literature suggests, single-party regimes, including China, rely particularly heavily on ideology and the regime’s ‘foundational myth’ to propagate the country’s societal order, the transcendental nature of the ruling party and/or leader, and the superiority of the nation to legitimize their rule.\textsuperscript{102} As such, we should expect to see China’s...

behaviour in cyberspace characterized by attacks with a particular focus on strengthening the party’s ideological messaging and narratives, which have been the regime’s foundational instrument in maintaining power for decades. Further, we should also expect to see cyber attacks designed to strengthen the image of the leader, or which at the very least, insulate the leader from criticisms or embarrassment, which could bring into question their greatness or right to rule.

This chapter on China is broken into several sections. The first provides a high-level overview of China’s emergence as one of the world’s most formidable actors in cyberspace, with a brief snapshot of how the cyber domain has become a key pillar of China’s strategy to regain its role as a great power. The second section describes the evolution of China’s known cyber attacks before and after Xi Jinping came to power in 2012. The third section explains how China’s cyber attacks align with theories on single-party regime legitimation, and how the country’s behaviour in cyberspace supports my needs-based theory on authoritarian legitimation. All told, this chapter will provide new insight as to why certain autocratic regimes appear to favour certain cyber attacks over others.

3.2 BACKGROUND: THE CCP, CYBERSPACE, AND THE ORIGINS OF CHINESE CYBER POWER

In China, discussions about cyber conflict, cyber warfare, or what they referred to as “information warfare,” emerged in tandem with the digital revolution and the largescale introduction of the Internet. However, China’s focus on the changing nature of conflict really took shape in the immediate aftermath of Operation Desert Storm in 1991. Impressed by American military achievements in the Gulf War, which saw the U.S. using new technologies to

---

103 Special thanks to Professor Stephanie Carvin for her suggestion to look at China’s cyber attack patterns before and after Xi.
their advantage – China’s military leaders began realizing their own future military successes would largely depend on their abilities to develop and apply breakthrough technologies in conflict. Two of these leaders, Qiao Liang and Wang Xiangshui, both colonels in the People’s Liberation Army (PLA), put these theories on paper in their 1999 military strategy book “Unrestricted Warfare” where they discussed the role cyber attacks would have in future conflict. Translated by the U.S. Naval Academy shortly thereafter, Liang and Xiangshui wrote:

Who is most likely to become the leading protagonist on the terra incognita of the next war? The first challenger to have appeared, and the most famous, is the computer “hacker.” This chap, who generally has not received any military training or been engaged in any military profession, can easily impair the security of an army or a nation in a major way by simply relying on his personal technical expertise.  

This futuristic thinking, which went beyond the idea of hacking and also included things such as “network viruses” and “media weapons” set the tone and laid the foundation for what would become an aggressive push by the CCP and PLA to leverage cyberspace, not only as a warfighting domain, but as a tool for controlling and exploiting the information environment to the regime’s advantage, both within China and beyond. Throughout the 1990s, the PLA began emphasizing the notion of “informationization,” and publishing books and papers on information warfare at a frenetic pace. In a rather telling 1997 PLA article on the future of warfare, concepts such as a “computer virus assault” were discussed, alongside the importance of having the

---

abilities to hack into enemy computers to “acquire vital information” and to replace “real information with disinformation.”\(^\text{105}\)

However, as noted, during this period, China also realized that in addition to cyberspace serving direct military and intelligence needs, it could be harnessed as a means of regime security and legitimation. Indeed, it needed to be. As Scobell et al. (2020) suggest, the CCP began exhibiting an acute sense of regime vulnerability around the cyber domain in the late 1990s, in large part as a result of increasing global utilization of cyberspace for everything from trade to communication.\(^\text{106}\) For the CCP, this new technologically driven era brought immense opportunity, but also tremendous risk. On the one hand, the Internet would have to be a pillar of China’s ambitions to further integrate the country into the global economy. On the other hand, this increased integration and exposure abroad, as well as the proliferation of Internet users domestically, presented potentially grave risks to the CCP-PLA-People’s Republic of China system.\(^\text{107}\) Speaking to this point specifically, Barme and Ye wrote in 1997 “…the technology China needs to build the most powerful country on Earth in the 21st Century threatens to undermine the institutions that rule the nation. And Beijing's control freaks are worried.”\(^\text{108}\) Consequently, striking the balance between expanded engagement with the outside world, while also ensuring cyberspace remained free of threats to the regime became a priority for the CCP during their grand strategy period known as “Building Comprehensive National Power” (CNP) which lasted from 1990 until 2003 – the same year Beijing’s “Great Firewall” came into


\(^{107}\) Scobell et al., 2020.

effect. It was during this period of building CNP, where Beijing began focusing on its perceived vulnerabilities in hard power – military and economic – and the ways it could harness cyberspace to address these shortcomings and mitigate external threats. In particular, the regime began prioritizing the modernization of its military forces, with defense budgets seeing double-digit annual growth during this period of strategic realignment.

While the aforementioned period of building CNP represents the formative years of China’s growth as a great power in cyberspace, it was during the country’s next grand strategy period known as “Rejuvenation” where former President Hu Jintao, and to a larger extent Xi Jinping, that the country began focusing on a singular state-centric threat that informed its posture in cyberspace: U.S. hegemony. Not only did China begin viewing the U.S. as an increasing threat militarily, the American way of life and their global promotion of U.S. ideals in terms of democracy, human rights and norms was also perceived as a threat to the regime, party narratives, and communist ideology. For the CCP, cyberspace quickly emerged as a tool China could leverage to counter these perceived threats, insulate the ruling party, and asymmetrically punch above its weight to counter America’s military and their ideas. While China’s perceptions of being militarily inferior to the U.S. were significant, these other soft power vulnerabilities were viewed as more insidious and potentially more destabilizing for the regime over the long-term. As China expert Dr. Oriana Skylar Mastro told me, “the CCP isn’t against the idea of democracy. It just doesn’t want it in China.” In Beijing, the regime was alarmed by what they had seen with the colour revolutions in places like Yugoslavia, Georgia and Ukraine, and they

---

109 Scobell et al., 2020.
111 Scobell et al., 2020.
112 Dr. Oriana Skylar Mastro was interviewed for the dissertation on October 29, 2021.
were not going to allow these types of events – which they perceived as being engineered by the U.S. – to happen in China. Subsequently, high-level strategic documents in the years to follow began to emphasize controlling the information environment, both internationally and within China. For example, the white paper titled “China’s National Defense in 2004” states “the PLA, aiming at building an informationized force and winning an informationized war, deepens its reform, dedicates itself to innovation, improves its quality and actively pushes forward the [revolution in military affairs] with Chinese characteristics with informationization at the core.” 113 In terms of domestic cyber control, China’s 2010 white paper “the Internet in China” discusses the country’s prioritization of “Internet security” and sovereignty in cyberspace. 114 Likewise, their 2015 document “China’s Military Strategy” discusses enhancing the country’s cyber capabilities to maintain “national network and information security” as well as “national security and social stability.” 115

In sum, China’s approach to and abilities in cyberspace were not developed in a vacuum. Rather, the CCP has sought to achieve two key objectives in the cyber domain over the last twenty-plus years – both of which have remained relatively consistent and which were informed by cyber-related developments worldwide. First, Chinese leaders have worked to maintain tight control over the Internet and the flow of information, both inside and outside China, in order to maintain domestic stability, regime legitimacy, and the continuation of CCP governance. Second, policymakers in China realized the economic, military and political potential of exploiting cyberspace as a means of countering U.S. supremacy in these spheres, and in some

instances, leapfrogging their way into great power territory. In other words, the CCP has viewed cyberspace as both a potential threat to the survival of the regime, but also a revolutionary technological domain that must be used to advance CCP’s long-term global ambitions to shape and influence the world order.116 Both of these things – being the control of information and the exploitation of cyberspace to achieve key military, economic, and political objectives that have been integral to CCP narratives – align with key theories from the literature on single-party legitimation. These ideas and objectives have been at the core of China’s cyber strategy since day one. However, in order to better understand how the CCP has used cyberspace to achieve these objectives, a closer look at a critical, yet surprisingly understudied phenomenon is warranted: the evolution and nature of China’s cyber attacks.

3.3 AN ANALYSIS OF CHINA’S CYBER ATTACKS FROM HU TO XI

In 1997, a 100-member cyber corps was stood-up by the Central Military Commission to explore “ways of planting disabling computer viruses into American and other Western command and control defence systems.”117 By 2000, China had created a strategic information warfare unit designed to “wage combat through computer networks to manipulate enemy information systems spanning spare parts deliveries to fire control and guidance systems.”118 Yet, despite these and other initiatives designed to enhance the country’s cyber capabilities, the earliest examples of China’s cyber attacks fell well short of altering their adversaries abilities or advantages, militarily, economically, or politically. In fact, some of China’s first and most

117 Ivo Dawnay, ‘Beijing Launches Computer Virus War on the West’, The Age (Melbourne), 16 June 1997, p. 8
noteworthy cyber attacks may not have even been carried out by the state (though they could have been supported by the CCP). Reporting and analysis on this first tranche of cyber attacks emanating from China is sparse. As such, it remains unclear if there was marginal involvement by the government in supporting these attacks, materially or otherwise. However, given CCP control in China, even in the early 2000s, I still consider and treat these few examples as potentially having some state involvement.

Rather, lone-hackers may have been responsible for a string of China’s earliest cyber attacks, which could explain their relatively marginal impact. For example, after the U.S. inadvertently bombed the Chinese embassy in Belgrade during the conflict in Kosovo, Chinese hackers defaced three U.S. government websites denouncing “NATO’s brutal action.” Then, in 2001, in response to a mid-air collision between a U.S. spy plane and a Chinese fighter jet, which killed the Chinese pilot, Chinese hackers defaced at least one U.S. government website belonging to the U.S. navy. In and around this time, Chinese hackers also targeted Taiwanese, Japanese and other U.S. sites in response to various diplomatic issues. However, it was not long after these periodic, low-level intrusions, that cyber attacks – clearly coming from the state – became destructive, destabilizing, and persistent. In fact, this surge in hostile cyber behaviour became a lynchpin for the CCP and their new leader – Hu Jintao.

_Hu Jintao, Chinese cyber attacks, and the birth of a cyber superpower (2002-2012)_

Scholarly works examining China’s cyber strategy and the country’s increasingly aggressive global posture most often point to the rise of Xi Jinping as the point in time when things began changing in Beijing. As I discuss in the following sections, China’s assertiveness,

---

119 Reporting and analysis on this first tranche of cyber attacks emanating from China is sparse. As such, it remains unclear if there was marginal involvement by the government in supporting these attacks, materially or otherwise. However, given CCP control in China, even in the early 2000s, I still consider and treat these few examples as potentially having some state involvement.
as well as their cyber attacks, did indeed become more pronounced (and personalistic) under Xi, but it was during the reign of his predecessor Hu Jintao, when some of the most significant changes to the CCP took shape. In the cyber domain, these changes and this aggressive behaviour became clear almost immediately.

In 2002, Hu Jintao became General Secretary of the CCP – the paramount leader of China. Although the phrase “who is Hu?” often characterized discussions of his accession, he quickly began spearheading a large strategic reorientation of China’s domestic affairs, as well as its foreign policy.123 From giving his internal security lead Zhou Yongkang free rein to quell dissent, to laying the groundwork for China’s future “Belt and Road” initiative, Hu made his intentions clear both at home and abroad. The days of China hiding and biding were over, and cyberspace was going to play an integral role in the new era of a much more assertive China.124 However, an often overlooked element of examining China’s behaviour in cyberspace, are the origins of this new and more adversarial CCP approach under Hu, which some analysts suggest, were anchored to his “new historic missions” that he publicly detailed in a speech on Christmas Eve in 2004. Framed as a revolutionary realignment of the PLA, the “new historic missions” narrative emphasized things like “providing an important guarantee of strength for the party to consolidate its ruling position,” and “providing a strong security guarantee for safeguarding the period of important strategic opportunity for national development.”125 Echoing earlier sections of this research, Mulvenon (2009) frames Hu’s “historic missions” and the CCP’s realignment of strategic party and military thought as being rooted in China’s domestic challenges in terms of

maintaining regime control and legitimacy, as well as the country’s increasingly global aspirations and entanglements.\(^{126}\) By looking at language contained within the “new historic missions,” it is clear Hu envisioned the future role of the PLA as being inextricably linked to the regime’s political objectives, and by extension, the CCP’s self-preservation and legitimation priorities. For Hu, cyberspace was seen as a new and technologically advanced domain the PLA could use to advance long-term CCP strategies and to – as my theory suggests – deliver on and strengthen key party narratives. However, the other long-term strategic vision attributed to Hu, which I argue more appropriately explains China’s aggressive surge in cyberspace, is his idea of “scientific development.”\(^{127}\) Like Mulvenon (2009), I consider Hu’s “new historic missions” to be a “subordinate manifestation” of his vision for “scientific development.”\(^{128}\) Introduced at the 16th Party Congress in 2002, Hu’s idea of “scientific development” became the overarching grand strategy and narrative of the CCP for advancing a more modern, outward facing, globalized China, while also preserving the foundational pillars of communism that underpin CCP legitimacy. Under Hu, China found itself at an inflection point were the county’s post-revolutionary future offered immense opportunity, but also destabilizing risks to the regime. Hu’s “scientific development,” was his attempt at embracing this new future, while simultaneously preserving core communist CCP narratives and ideologies. Cyberspace allowed him to do that. Importantly, under Hu, CCP leadership began to think, and speak about economic and national security as a reinforcing pair.\(^{129}\) Together, these ideas, being economic and national

\(^{128}\) Mulvenon, 2009, pp. 1.  
security, would be thought of as a single unifying strategy the CCP would promote and pursue to support regime legitimation and the continuation of CCP rule. Echoing this, Chang (2014) writes “China’s [cyber security strategy] is, just as with its overall strategy, primarily driven by the goal of prolonging the power of the Chinese Communist Party, and domestic concerns maintaining internal stability, curbing social and political unrest, and promoting economic growth.”

As for the country’s cyber attacks under Hu, there was an observable surge in malicious cyber activities in the early 2000’s that aligned with his strategic visions outlined above and which support my theory on single-party legitimation. These ranged from attacks targeting dissident groups at home, and abroad, as well as other figures and organizations the regime considered hostile to the CCP, as well as largescale espionage attacks. For instance, in 2002, sophisticated Trojan Horse programs were used to gain access to and steal information from the computer network of the Dalai Lama. Foreign dissident groups also reported having their computer systems and operations aggressively and consistently disrupted. However, it was the “Titan Rain” campaign discovered by U.S. authorities in 2003, which numerous security experts attributed to China, that signalled a change in the regime’s behaviour, and which highlighted the fact cyber espionage would be a key tool in advancing the party’s coercive apparatus and legitimizing the CCP’s rule. During the “Titan Rain” attack, computers in China successfully breached hundreds of unclassified U.S. government and defence contractor networks at places such as the Department of Defense, the Department of Energy, the Department of Homeland

Security, Sandia National Laboratories, Lockheed Martin, NASA, and elsewhere. Although the attack was, at least by today’s standards, uncharacteristically “smash and grab” in nature with the perpetrators taking any files they could gain access to, the message was clear: cyberspace could and would be used by the regime to fulfil and deliver on key narratives and objectives as part of their grand strategies. Pointing the finger at China, and speaking to the sophisticated nature of the attack, Alan Paller, former Director of Research at the SANS Institute said in 2007, “…this [attack] is an order of magnitude more disciplined than anything I have seen…”

Following “Titan Rain” China’s cyber attacks only intensified, with intrusions against the U.S. State Department’s Bureau of East Asian and Pacific Affairs in 2006, the office of Congressman Frank Wolf (who had been a particularly outspoken critic of the regime), the U.S. Bureau of Industry and Security, and the U.S. Naval War College – all within the same year. China’s cyber espionage campaign continued throughout 2007 as well, where for example, the regime breached the Pentagon’s Joint Strike Fighter project and stole data related to the F-35, carried out cyber espionage operations against the British Foreign Office, and attacked the computer systems of the French ministry of defense. While China’s cyber espionage efforts carried on relentlessly, hitting everything from Barack Obama’s presidential campaign in 2008, to Coca-Cola Co. in 2009, it was China’s attacks against Google and RSA in 2010 that caught

---

the attention of cyber experts and national security practitioners worldwide. As Greenberg (2021) described the attacks, they were “a harbinger of our future.”\textsuperscript{137} Publicly disclosed by Google in a 2010 blog post titled “A new approach to China,” the company stated they had evidence to suggest, “a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists.”\textsuperscript{138} However, additional evidence found the PLA-affiliated hackers known as the “Elderwood Group” also sought to identify Chinese intelligence operatives under U.S. government surveillance, as well as obtain trade secrets and commercially confidential information from companies including Adobe, Juniper, Rackspace, Symantec, Northrop Grumman, Morgan Stanley, and Yahoo.\textsuperscript{139} Similarly, that same year PLA-affiliated hackers carried out an attack against the global security company RSA. Stealing the company’s secret digital keys known as “seeds,” the intruders were able to acquire the company’s crown jewels of cybersecurity protection: codes they provided to their clients, “including tens of millions of users in government and military agencies, defense contractors, banks, and countless corporations around the world.”\textsuperscript{140} At the time, many considered the attack to be the most sophisticated and most damaging cyber attack ever carried out. Between the attack on Google, dubbed “Operation Aurora,” and the intrusions against RSA, as well as a slew of reportedly thousands of other attacks,\textsuperscript{141} Chinese cyber prowess had quickly become a top national security priority for governments around the world. Hu’s cyber army had arrived, their capabilities were clear, and people were taking notice. The following year, in 2011, a U.S. report to Congress on

\textsuperscript{140} Greenberg, 2021.
\textsuperscript{141} Ian Steadman, “Reports find China still largest source of hacking and cyber attacks,” Wired, April 24, 2013: https://wired.co.uk/article/akamai-state-of-the-internet
foreign economic collection stated, “Chinese actors are the world’s most active and persistent perpetrators of economic espionage” and that there had been a recent “onslaught of computer network intrusions” that had originated in China.142

Over the decade that Hu ruled China, he introduced largescale, long-term strategic plans, and created enduring party narratives, which relied heavily on PLA tactics and operations in cyberspace. By analyzing the data, speaking with subject matter experts and studying extensive open-source material from 2002-2012, it is clear that China’s cyber attacks during this period almost always took the form of cyber espionage as a means to propel the country forward economically, militarily and politically. Further and particularly connected to my theory on authoritarian legitimation, this prioritization of cyber espionage allowed Beijing to establish its domestic discourse power by delivering on key party narratives and grand strategic visions. In the decade to follow (2012-current) espionage has remained China’s preferred activity in cyberspace, but under Xi, the CCP and PLA have become more emboldened, brazen, ruthless and persistent with their cyber attacks. In large part, China’s increasingly assertive and confrontational behaviour in cyberspace since Hu is a reflection of Xi Jinping – the most powerful and personalistic leader China has had in decades. To echo Dr. Mastro – “in the broader military realm – including cyber – everything changed from Hu to Xi.”143

Xi Jinping, cyber nightmares and the return of a great power (2012-current)

In the years leading up to Xi’s takeover of the CCP, many international analysts and officials predicted that for the most part, things would remain as they were under Hu. In fact, in

---


143 Quote taken from interview with Dr. Mastro on October 29, 2021.
August 2011, when Xi was still Vice President of China, then U.S. Vice President, Joe Biden characterized the trajectory of U.S.-China relations as “…nothing but positive.”\(^\text{144}\) The year prior, leaked U.S. cables went as far as describing Xi as “Mr. Clean.”\(^\text{145}\) As Page (2020) notes, this assessment of Xi “was one of the biggest strategic miscalculations of the post-Cold War era.”\(^\text{146}\) Even in the earliest days of Xi assuming leadership, it became clear things would be different, military, economically, and politically. Making his intentions clear within a month of becoming leader, Xi presented his “Chinese Dream,” and his “Two Centennial Goals”: doubling the country’s 2010 gross domestic product by 2021, (which it is has done) and becoming a “fully developed, rich, and powerful” national by 2049 – the 100th anniversary of the CCP.\(^\text{147}\) To Xi, the cyber domain has been a key tool in realizing these objectives, delivering on the legacy narratives he presented at the beginning of his presidency, and legitimizing his rule.

While both Hu and Xi viewed cyberspace as a pathway to advancing their political and ideological goals, Xi has leveraged the cyber domain to consolidate power, protect his own image, and control the Chinese people inside and outside the mainland in ways Hu, and most other Chinese leaders, could not have imagined. Ryan Hass, a Senior Fellow with the Brookings Institute told me “…as a practical matter Xi is much more risk tolerant and comfortable with friction than Hu was.” Further, Hass went on to explain that Hu was more of an optimist, whereas Xi has a “jaundiced view of other countries tolerance of China’s rise.” As Hass suggested, Xi’s tolerance for risk and his skeptical worldview translates into differences in cyber

\(^{144}\) The White House, “Remarks by Vice President Biden and Chinese Vice President Xi at a U.S.-China Business Roundtable,” Office of the Vice President, August 19, 2011.


behaviour between the two leaders. In this sense, and as I explain further in section 4.4, China’s behaviour in cyberspace under Xi reflects the fact that Xi, while still leading a single-party regime, is much more of a personalist autocrat than his predecessor. Hass touched on this point as well, telling me “Hu was a function of a collective leadership system,” whereas Xi Jinping has “systematically dismantled the collective leadership model and placed himself at the core… he’s the first leader since Mao to consolidate power in his office in his personage.” Therefore, we should expect to see China’s cyber attacks under Xi more focused on preserving his ‘chosen from above’ image, and his aura as being the guiding force behind the country’s major achievements – at least more so than his predecessor. Echoing this, Shirk (2018) notes that while many Chinese citizens and observers expected the country to maintain its gradual progression towards greater institutionalization and political accountability, just as other authoritarian regimes had done, things quickly took a U-turn under Xi – “personalistic rule is back” she wrote.

Nowhere is Xi’s personalistic authoritarian grip on power more pronounced than it is with the PLA. As Tai Ming Cheung has observed, “no other Chinese Communist Party leader, not even Mao Zedong, has controlled the military to the same extent as Xi does today.” From relying on the PLA to maintain domestic stability online, to having it carry out cyber attacks against a range of foreign entities perceived as posing a threat to Xi’s reputation or the regime, China’s military has, for all intents and purposes, acted at the sole direction of Xi throughout the last decade. In fact, by early 2014, Xi had personally taken charge of a new government body

148 Ryan Hass was interviewed virtually for this dissertation on November 4, 2021.
responsible for overseeing the country’s cybersecurity, where, at its first meeting, he expressed his desire to turn China into a “great cyber power.”\textsuperscript{151} This desire quickly turned into a reality.

In terms of cyber attacks carried out under Xi, the first noteworthy intrusion that caught the attention of policymakers and cyber experts was China’s hacking of the \textit{New York Times}, which lasted for four months, beginning in the fall of 2012. The attacks coincided with a \textit{Times} investigation revealing that relatives of Wen Jiabao, China’s then-prime minister, had accumulated a multi-billion dollar fortune.\textsuperscript{152} Similarly, prior to this, and before Xi had even assumed his role as General Secretary, China carried out cyber attacks against Bloomberg, after they published reports regarding the wealth accumulated by Xi’s relatives.\textsuperscript{153} In 2013, the \textit{Wall Street Journal} also reported they had been hacked by China as part of a campaign to spy on reporters covering issues related to China.\textsuperscript{154} These were the first and most significant attacks of their kind carried out by China overseas, designed to spy on and punish people and organizations for embarrassing the regime. That same year, China also began its most significant intrusion yet: a hacking operation against the U.S. Office of Personnel Management (OPM), the agency responsible for managing the government's civilian staff. Carried out over two separate intrusions, with the first being in 2013 and the other in 2014, Chinese hackers were able to exfiltrate the personal records of over 22 million government personnel, as well as the personal information on potentially thousands of media personnel who may have visited or had access to

\textsuperscript{151} William Wan, “China seeks role as ‘cyber power,'” the Washington Post, February 28, 2014: 
\textsuperscript{152} Nicole Perloth, “Hackers in China Attacked The Times for Last 4 Months,” the New York Times, January 30, 2013: 
\textsuperscript{153} Perloth, 2013.
\textsuperscript{154} Siobhan Gorman, Devlin Barrett and Danny Yadron, “Chinese Hackers Hit U.S. Media,” the Wall Street Journal, January 31, 2013: 
https://www.wsj.com/articles/SB1000142412788732392610457827620952260718
U.S. government buildings. At the time, the OPM breach was the largest and most significant theft of sensitive personal information in history. In 2014, Canada, like many other countries, was also hit by a significant cyber attack traced back to the Chinese government, in which hackers gained access to the computer network of the National Research Council (NRC), where they stole troves of sensitive intellectual property, costing the NRC hundreds of millions of dollars – and the attacks kept coming. By May 2014, barely eighteen months after Xi took office, China’s cyber attacks had become so relentless and costly, that the Obama Administration unsealed an indictment charging five members of the PLA’s cyber unit for their attacks against a range of U.S. entities. Unfortunately, this public shaming by the U.S. had little effect. In 2015, a distributed denial of service (DDoS) attack originating from China hit the website Github in what was at the time, one of the most advanced attacks of its kind ever carried out. By hijacking advertising and analytics traffic meant for Baidu, a Chinese search company, and then redirecting that traffic to Github, the attackers were able to overwhelm the website, causing it to shutdown. The reason? Anti-censorship groups were using Github to circumvent China’s domestic internet restrictions, providing users in China access to materials and publications prohibited by the CCP, including the New York Times. As Mikko Hypponen, former Chief Research Officer at the security firm F-Secure noted: the attacks were meant to send a message

---

to the operators of Github – “either you kick out…The New York Times, or we’ll keep this up.”

By September 2015, it was clear the U.S. (and other nations) had had quite enough. During Xi’s first visit to Washington, D.C., President Obama stood next to him at the White House, and made the bold move of threatening sanctions against China unless Xi and the CCP stopped their aggressive cyber espionage campaign. At a Rose Garden news conference, Obama declared “we will apply [sanctions], and whatever other tools we have in our tool kit, to go after cybercriminals either retrospectively or prospectively.” Shortly thereafter, during the same diplomatic visit, Obama and Xi reached an agreement for both countries to curb their cyber attacks against the other, though Obama remarked warily – “the question now is, are words followed by actions?” Remarkably, for the next eighteen months, Xi’s words and his commitment to scale back China’s cyber attacks were followed by action. Indeed, a FireEye study found there had been a “notable decline in China-based groups’ overall intrusion activity against entities in the U.S. and 25 other countries” – including Canada. However, in line with intelligence assessments at the time, the report noted that this decline in China’s cyber attacks actually began a year prior – likely a result of Xi reining in the PLA, a move to further consolidate his power. Regardless, the victory was fleeting. By 2017, shortly after President Trump took office, China’s cyber attacks began increasing again. Though a definitive explanation for the increase in attacks was never publicly provided, observers and subject matter

---

159 Mozur, 2015.
experts suggested deteriorating trade relations might have been the cause (or a symptom). Others argued that increased U.S. export controls in key technological domains (e.g. biotechnology and aerospace) and tightened rules on inward Chinese investments into America’s tech sphere – moves the PPC considers to be part of a “containment” strategy – led China to again, as Sanger put it “…steal what they cannot buy.”

In the time since, China has carried out some of its most significant intrusions. For example, in 2017 the company Equifax was hacked, which saw the data of roughly 150 million Americans (and 20,000 Canadians) compromised, only a few months after Canada struck its own agreement with China, aimed at curbing economic cyber espionage against Canadian targets. Then, in 2020, in the midst of a global pandemic, the regime focused its attention on stealing COVID-19 research from companies and institutions around the world working to develop a vaccine. Further, in 2021 the regime hacked an estimated 250,000 Microsoft servers around the world – giving them the ability to steal emails and install malware on the computers of tens of thousands of individuals they can now spy on. The regime has also increased its efforts to silence dissidents and critics around the world who have spoken out against Xi’s human rights violations against the country’s ethnic minorities, with attacks targeting Uyghur, Hong Kong and Tibetan dissidents. Leaked party documents speak to how crucial this new era of Chinese transnational repression is to Xi and the regime. In fact, and in line with the underlying argument of this research, internal CCP material highlights the “overseas struggle” against perceived party

---

enemies as being a priority. Speaking on China’s approach to silencing critics, Executive Vice Foreign Minister, Le Yucheng, explained in December 2020 that China “cannot submit to the unscrupulous suppression by hostile anti-China forces but naturally fights back.” Le went further, stating, “China’s diplomacy has always been free from all cowardice or obsequiousness and firmly determined to defend national interests and dignity.” This struggle also extends to enemies of Xi.

For instance, in July 2020, a Chinese student studying in Australia who manages a Twitter account critical of the General Secretary said she had received video calls from a Chinese police officer, who, standing next to her father, warned her “remember that you are a citizen of China.” In October 2020, then U.S. Assistant Attorney General John C. Demers, alongside FBI Director Chris Wray, delivered remarks announcing charges against eight agents of the CCP carrying out these types of acts against individuals living in the U.S.. Describing operation “Fox Hunt” – the CCP’s global anti-corruption campaign – Demers said, “some of the individuals [targeted through this international CCP operation] may well be wanted on traditional criminal charges and they may even be guilty of what they are charged with. But in many instances the hunted are opponents of CCP Chairman Xi – political rivals, dissidents, and critics.” This and other examples, speak to the fact that over the last decade, the utility of cyberspace for the CCP has evolved dramatically. Where the domain was once primarily

---

exploited to advance the country’s national interests as part of various grand strategies and narratives, it is now increasingly used in equal part to protect Xi, strengthen his legitimacy, and ensure his – and the PPC’s – political survival. As Hass (2021) notes, China is working to advance a number of interlocking objectives related to this overseas struggle – which I argue, all depend on cyberspace. Of particular relevance to this research is China’s effort to create a “chilling effect” on “any individual, Chinese or foreign, who advocates views or policies that challenge Chinese interests, broadly defined.”168 In this sense, China is looking to create the impression, especially throughout its expatriate community, that no person is beyond the reach of the CCP. Moreover, China is trying to influence countries around the world – notably authoritarian ones – that they too can securitize their regimes in the same way the CCP has.

Ultimately, for China, the more countries that embrace the CCP model of addressing security threats – whether they be real or perceived – the more likely it is that China will be able to legitimize its domestic security apparatus abroad.169

In this final section, I provide further analysis on how the preceding information on China’s cyber attacks and behavior in cyberspace align with some of the key theories on autocratic legitimation, both in terms of single-party regimes, as well as personalist dictatorships in the case of Xi. Through this final section, it should become clearer how the examples I have used from the empirical record support my needs-based theory on autocratic legitimation in the cyber domain.

---

168 Ryan Hass, ”How China is responding to escalating strategic competition with the US,” Brookings Institute, March 1, 2021: https://www.brookings.edu/articles/how-china-is-responding-to-escalating-strategic-competition-with-the-us/#footnote-35
Chinese cyber attacks and regime legitimation

The literature tells us that single-party regimes tend to rely particularly heavily on messaging, and advancing key narratives, ideologies and myths to legitimize their rule – at least relative to other regime types. In an attempt to extend this theory to authoritarian behaviour in cyberspace, I argue that we should therefore expect to see single-party regimes – such as in the case of China – pursue cyber attacks that perpetuate and strengthen certain narratives the regime relies on to maintain power. Moreover, single-party regimes as well as personalist autocracies often emphasize the centrality and abilities of a specific leader to legitimize the government’s rule. Based on this suggestion and my own theory, autocratic regimes where a specific individual plays a particularly crucial role in governance, will pursue cyber attacks that look to bolster the image of the ruler and/or which seek to limit criticism or embarrassment. Both of these expectations have – to varying degrees – proven to be true in China, with their mix of single-party and personalist rule under Xi. We see this in at least two main ways.

First, as my theory suggests, China has primarily used their cyber attacks as a means of strengthening the regimes messaging and reinforcing party narratives. Although observers often argue China’s economic espionage attacks are designed to simply acquire information and assets that are useful to the regime, I argue that these types of Chinese cyber attacks are as much about ensuring grand CCP strategies, narratives, and ideological visions are achieved and fulfilled. In other words, while China’s cyber espionage attacks are designed to economically leapfrog international competitors and enhance the country’s indigenous technological development, they are also about convincing China’s 1.4 billion people that regime messaging regarding long-term trajectories are being realized, and that the CCP is best poised to govern the nation. Indeed – economic growth and prosperity has been a pillar of CCP messaging over the last twenty years,
and through cyber attacks, not only has the regime stolen their way up the economic ladder, they have convinced the people of China they are reliable, and true to their word. Whether it was Hu Jintao’s prioritization of “scientific development” or Xi Jinping’s “Chinese Dream,” there have been numerous high-level concepts, narratives, and plans in China over the last twenty-plus years that have, in large-part, depended on the success of the country’s cyber attacks. From this perspective, China’s cyber attacks align with the key theories on autocratic regime legitimation with their emphasis on ideological claims and reliance on party narratives.

Unlike other regimes who focus on things such as acquiring direct financial resources or destabilizing democratic institutions and creating disorder, China is focused squarely on delivering on its narratives and strengthening belief in party ideologies, which form the basis of the CCP’s justification as China’s rightful political authority. As Cassani (2017) notes: “only a handful of regimes still make explicit reference to an infallible ideology, and most of them cluster in Eastern Asia – namely, China, Vietnam and North Korea.”170 Academic works by Tannenberg et al. (2020), Dukalskis (2017), von Soest and Grauvogel (2017) and others have all pointed to the significance of ideological claims and party narratives for single-party authoritarian regimes. Indeed, in many instances, they use China as their example. For instance, looking specifically at China (along with North Korea and Burma), Dukalskis (2017) notes that “framing events in support of the governing ideology, offering myths of founding and greatness” and, among other things, “promising deliverance from struggle to a better future are all integral elements of the CCP’s abilities in maintaining power.”171 Moreover, in a China-specific study on

---

regime legitimation, Holbig (2013) finds that ideology “…plays an indispensable role in the quest to legitimize authoritarian rule in contemporary China.” Holbig also writes “…the Chinese party-state, in its quest to legitimize authoritarian rule, has invested heavily in the continuous adaptation of official ideology to a changing domestic and international environment.” As my theory suggests, and as the empirical record illustrates, China has adapted and used the cyber domain to ensure these core elements of legitimation are realized amidst – as Holbig describes it – changing environments. Further reinforcing my theory, and going back to this idea of economic growth being crucial to CCP narratives and party ideology, is the notion that economic performance is also important to single-party regimes. However, as von Soest and Grauvogel note, “successful economic performance can translate into claims for legitimacy only when the regime is framed as being in the pivotal role to having achieved this success.” Yet, I argue that successful economic performance can also translate into a viable legitimacy claim if a father-like figure of the nation is portrayed as being responsible for that performance. We see this in the case of Xi.

Second, in addition to the single-party dynamic, I have also shown that China’s cyber attacks have, to a certain extent, evolved with the rise of Xi Jinping. Throughout the last decade, as Xi has consolidated power and moved the country closer towards personalistic authoritarian rule, the country’s cyber attacks have become increasingly focused on protecting Xi and legitimizing his right to rule. As Geddes, Franz and Wright (2014) suggest, a personalist regime is one wherein “discretion over policy and personnel are concentrated in the hands of one man,

173 Holbig, 2023, pp.16.
military or civilian.” China under Xi fits this definition. In fact, Xi has become so powerful, and has taken over so many branches of the government, that he is now both military and civilian. Some have gone as far as calling him “the Chairman of Everything.” Where cyber attacks under Hu were, for the most part, about advancing the country into a new era, propelling the party forward, and bringing key party narratives to fruition, cyber attacks under Xi are, to a much greater extent, about protecting Xi, legitimizing his winner-takes-all approach to governance, and safeguarding his ‘personalist cult.’ In a sense, for Xi, cyber attacks against dissidents or any entities critical of his rule or the CCP have been used as a means of risk mitigation. Xi himself has suggested that threats in cyberspace risk “brewing” into actual real-world risks at home which could destabilizing his leadership, party progress, and national unity. Moreover, for Xi, “defusing ideological risks on the internet” is considered a priority area of modern warfare and political survival.

Further, China’s cyber attacks under Xi are also consistent with legitimation strategies of personalist dictators in that personalist rulers often rely on performance-based claims to legitimacy such as strong economic performance. This is in line with von Soest and Grauvogel’s (2015) finding that the rulers in the twelve post-Soviet countries they examined (e.g. Russia and Belarus) – many of which are personalist – focus their legitimation claims on their positions as “guardians of high levels of economic growth and citizens’ socio-economic well-being.” The

same can be said for Xi. As discussed, China’s most belligerent and sophisticated cyber attacks have been linked to Xi’s strategic visions of returning the country to greatness and becoming an economic superpower. Guriev and Treisman (2015) echo this in stating that the CCP, throughout China’s road of rapid growth (which has happened primarily under Xi), has focused heavily on economic strength and emphasizing “consumption and provision of public goods.”

Likewise, Tannenberg et al., note that personalistic regimes, “because their rule relies upon the neo-patrimonial distribution of resources,” can and often do base their legitimacy claims on their abilities to provide access to resources. I argue that in the case of China under Xi, this access to resources is framed as collective national access to resources and prosperity during a period of immense economic growth, which Xi presents himself as being the guarantor of. As Xi himself said in 2013, “if our party can’t even handle food-safety issues properly, and keeps on mishandling them, then people will ask whether we are fit to keep ruling China.”

All told, for the CCP and particularly for Xi Jinping, cyberspace has proven to be an incredibly efficient tool for regime legitimation, where the party has sought to guarantee active consent, compliance and belief in the rules and party narratives, belief in Xi’s cult of personality, passive obedience, and toleration under authoritarian rule. To echo Rousseau, “the strongest is never strong enough to be always the master, unless he transforms strength into right, and obedience into duty.” In China, cyberspace has enabled the regime to do precisely that. From using cyber attacks to deliver on party narratives and propel the country towards (re)gaining global superpower status, to shielding Xi from criticism, embarrassment, and opposition, China

---


181 The Economist Intelligence Unit, “Beware the Cult of Xi,” The Economist, April 2, 2016: https://www.economist.com/leaders/2016/04/02/beware-the-cult-of-xi

has harnessed cyberspace in ways most other countries have not. To conclude, this section validates my needs-based theory on cyber attacks, and confirms what I expected to see in terms of China’s cyber attacks and key theories from the literature on autocratic legitimation. In the following chapter, I undertake a similar study, and explore how the Russian government – particularly under President Vladimir Putin – has used cyber attacks to legitimize its rule, while providing novel connections between the literature on electoral autocracy legitimation and Russia’s behaviour in cyberspace.
CHAPTER FOUR

RUSSIA: CYBER ATTACKS AND REGIME LEGITIMATION

4.1 INTRODUCTION

Russian cyber attacks on military and civilian targets in the West have become commonplace. Yet, despite the importance of this issue, the excellent scholarship already published on this topic, and the destruction Russian-attributed cyber attacks have caused worldwide, there has been little effort in exploring whether Russia’s regime type contributes to the way the state behaves in cyberspace. I argue that Russia’s cyber attacks are better understood by looking at the type of regime operating in the Kremlin, and by analyzing how the Russian government has continued to use the cyber domain as a means of regime legitimation.

As mentioned in previous sections, I classify Russia as an electoral autocracy given the country’s use of nominally competitive multiparty elections where opposition parties can – at least legally speaking – compete for power. However, unlike free and open elections in democratic nations, elections in electoral autocracies are characterized by rulers using a range of “coercive and unfair” tactics to disadvantage their opponents and ensure continued political victory.183 Interestingly, numerous authors differentiate between “hegemonic” and “competitive” electoral autocracies,184 with the former ensuring that any opposition activity is “severely constrained” with “widespread intimidation of the opposition and severe electoral fraud.”185

---


184 As I do, Andreas Schedler subsumes ‘competitive’ and ‘hegemonic’ authoritarian regimes under the broad category of electoral authoritarianism.

Further, and of particular importance to this research, is the idea that hegemonic electoral autocracies tend to approach their procedure-based claims to legitimacy more cautiously than other forms of autocracies given their overt oppression of democratic norms. As a result, their procedure-based claims to legitimacy are often woven into a broader narrative. Explained throughout this chapter, we see these oppressive tactics and this reliance on a broader narrative used consistently in the case of Russia. Indeed, in September 2021, Russia’s ruling “United Russia” party – led by President Vladimir Putin – won another landslide vote, in what some are calling “the most repressive since Soviet times.” That said, and based on key theories throughout the literature which emphasize that electoral autocracies rely heavily on procedural and performance-related legitimacy claims, Russia’s cyber attacks should be characterized by attempts to strengthen regime messaging related to procedures and performance (e.g. economic and security). Moreover, and similar to what I illustrated in the China case study, Russia’s government has become increasingly personalist in nature under President Vladimir Putin. Therefore, Russia’s cyber attacks should mirror China’s to a certain extent, in their attempts to strengthen the image of Putin as the ‘father of the nation’ and to limit his exposure to any embarrassment, criticism or dissent.

The following chapter on Russia is broken into several sections. The first provides a high-level overview of Russia’s rise as a cyber-superpower, and how the regime conceptualizes cyberspace in terms of conflict and regime security. The second section explores the empirical record of Russia’s cyber attacks, with emphasis on how Russia’s behaviour in cyberspace has increasingly reflected President Putin’s personalist rule. Finally, the third section explains how

186 Von Soest and Grauvogel, 2017.
Russia’s cyber attacks align with the core theories on electoral autocracy regime legitimation, and how the country’s behaviour in cyberspace supports my needs-based theory on authoritarian legitimation.

4.2 BACKGROUND: THE KREMLIN, CYBERSPACE, AND THE ORIGINS OF RUSSIAN CYBER POWER

Since the beginning of the 21st century, Russian military doctrine has progressively emphasized the idea that threats emanating from cyberspace – or what in Russia is more commonly considered the information domain – will play a crucial role in future conflict. Based on an analysis of the literature, I have identified two underlying factors that have contributed to this evolution in thinking, and Russia’s emergence as a cyber superpower – major events with destabilizing potential and a “siege mentality.” On the former point, numerous authors have noted this shift in thinking has been accelerated by at least three distinct events: the Second Chechen War of 1999, the Russo-Georgian War of 2008, and the 2011-2013 Moscow Protests. In the Second Chechen War, for instance, Russia was able to dominate traditional media with its messaging, but was unable to prevent the rebels’ use of the Internet to generate international support and sympathy for the struggling “freedom fighters.” Subsequently, Russia began exploring ways to harness the Internet to influence audiences – both at home and abroad. According to Giles (2016), Russia began using disinformation campaigns at home, alongside cyber operations against Chechen information efforts to gain information superiority.

---


Russo-Georgian War, the Georgians – like the Chechens – were able to punch above their weight and dominate reporting on the conflict, with continued emphasis on Russian airstrikes against civilian targets. Ultimately, the realization that Russia may have won the physical war but lost psychological one, led to conversations about creating Information Troops who could “manage the information war from within the military.” Then, in 2011, and perhaps most connected to this research in terms of Russia’s classification as an electoral autocracy, protests erupted in Moscow over unfair elections and the Putin-Medvedev tandemocracy. In this case, Russia’s leaders realized the transformative and destabilizing potential social media could have on the regime. At this point, the Arab Spring protests had already demonstrated the impact social media could have on regime change, leading the Kremlin to fear the same could happen in Russia. As a result, and realizing that auto-generated social media posts were not sufficient in shaping public opinion, the government began investing heavily in enhancing its human capacity to alter the information domain. On this point, Keir (2016) has said that during this time, Russia realized that “dominating mass consciousness online requires the engagement of actual humans.” Together, these three events dramatically shaped Russia’s approach to cyber conflict and the urgency in which they began making moves to strengthen their abilities in cyberspace.

In addition to these major events shaping Russia’s approach to cyberspace, the Kremlin’s perception of threats emanating from the information domain and the aforementioned “siege mentality” has also dramatically impacted the country’s cyber posture. In fact, Russia’s thinking on and approach to cyber conflict and information superiority derives from its traditional

---

191 Giles, 2016.
“besieged fortress” mentality, where it looks to defend itself against constant internal and external threats. Dr. Bilyana Lilly with the RAND Corporation spoke about this as well, telling me “Russia always has this besieged fortress mentality… they see the U.S. as the aggressor and that they are under constant threat. Responding to these threats and this aggression in cyberspace allows the Kremlin to address these perceptions, while also avoiding conventional warfare with the West – something they think they would lose.” This mentality, and this way of perceiving the outside world, has been an enduring psychological Soviet tradition for decades. Speaking to Russia’s mindset, Hakala and Melnychuk (2021) note: “as a vast country with significant natural resources but few natural borders, Russia has repeatedly had to mobilize its society to counter foreign aggressions. This has contributed to a profound sense of insecurity whereby the security of Russia can best be guaranteed by exerting control beyond its borders, in its perceived “sphere of influence.” Likewise, Dr. James Lewis with the Center for Strategic and International Studies told me “the Russian’s are still as paranoid as they ever were… but now through cyber they have started harnessing that to focus on the messaging around that mentality.”

For Russia’s military strategists and political leaders, this mentality has been extended, even hardened, in the cyber domain. As many Russia experts have noted, just as it does in the physical world, Moscow considers this struggle as constant and everlasting in cyberspace.

---

195 Dr. Bilyana Lilly was interviewed virtually for this dissertation on November 19, 2021.
197 Dr. James Lewis was interviewed for this dissertation virtually on November 3, 2021.
Crucially, this idea aligns with the theory that electoral autocracies often rely on security-related reasons to justify the absence of democratic principles – something discussed throughout this chapter. Moreover, and as I covered in previous sections, electoral autocracies also typically rely on performance and procedural claims to legitimize their rule. These claims could take the form of performance from a security-related perspective, whereby the regime portrays itself as the guarantor of national security and well-being, or the ability to apply clear and impartial procedures for resolving and addressing complaints and disputes of various types, among other things. Therefore, this idea that Russia continually sees itself as being on the defensive – which appears consistently throughout the literature – is an important element of my theory when it comes to the Kremlin’s behaviour in cyberspace. More specifically, I argue that this siege mentality, and this narrative of constantly being on the defensive that the Kremlin perpetuates, forms the basis of Russia’s performance legitimacy claims where the regime – and increasingly President Putin – positions itself as being the only thing standing between the Motherland and Western hegemony. Further, I argue that this mentality and the narratives that comes with it, also serves as justification for a number of Russian policies, including its electoral procedures, and why it cannot operate like its liberal democratic adversaries.

For the last two decades, this mentality is what has most heavily influenced Russia’s approach to cyberspace, with military strategists and political leaders viewing the domain as one which must be leveraged in modern warfare, but which also presents immense risks to national security and regime survival. This thinking in terms of threats to the regime has appeared in numerous high-level strategic documents throughout this timeframe. For example, the 2000

\(^{199}\) Diamond, 2002.
National Security Concept suggested Russia’s national security was being threatened by countries seeking to dominate the information sphere. Likewise, Russia’s 2010 Military Doctrine elevated information warfare as a threat to the nation, while the 2016 Information Security Doctrine reemphasized this idea. More specifically, the 2016 doctrine concentrated on the proliferation of cognitive-based threats emanating from the information space, orchestrated and carried out by foreign actors, and the effects these actions can and do have on social values and stability. These and other documents and speeches speak to Russia’s mentality when it comes to carrying out information operations in cyberspace. Moreover, and as I explain in greater detail later in this chapter, these materials also form a core pillar of the Kremlin’s narrative when it comes to justifying their autocratic form of governance, their right to rule, and the regime’s overall claims of legitimacy.

In addition to cyberspace and information operations gaining prominence in some of Russia’s guiding strategic documents, the way Russia actually conceptualizes warfare has also evolved quite dramatically over the last twenty-plus years. What we have seen is a shift away from broad agreement that the baseline threshold of warfare is armed violence, to the idea that it now includes other, non-military measures such as the control and manipulation of information in cyberspace and beyond. However, as Lilly and Cheravitch (2020) note, this change in

---


thinking became most pronounced between the early 2000s and the Crimea crisis which began in 2014. According to Jonsson (2019), throughout this timeframe, a consensus formed among Russian leaders and influential military theorists that the line between war and peace had become increasingly blurred, and that nonviolent elements of conflict could be so effective they should be considered as destabilizing or threatening as violent measures, thereby rendering them equally as integral to warfare. Likewise, General Valery Gerasimov, Russia’s Chief of the General Staff of the Armed Forces, wrote about the potential that protests modeled after the Arab Spring could presage future conflict, despite their reliance on non-violent methods. Colonel Chekinov and Lieutenant General Bogdanov – two well-known military scholars in Russia – also contributed to this shift in thinking, arguing that the aggressor in a conflict will always use non-military measures first. According to Chekinov and Bogdanov, and crucial to my theory on Russian behaviour in cyberspace, these non-military measures include manipulating information flows to public institutions in the target country, including the media, cultural institutions, religious and non-governmental organizations, and foreign-sponsored movements. Speaking at the 2019 conference of the Russian Academy of Military Sciences, General Gerasimov again raised the prospect of combined asymmetrical and classic warfare measures, highlighting that “coordinated use of military and non-military measures” had become crucial in modern conflict, even suggesting that non-military measures had become paramount to traditional armed methods. Some of the key doctrinal papers mentioned earlier also indicate an evolved understanding of war and conflict. For example, the 2010 Russian Military Doctrine discussed the fact that the combination of military and non-military measures had become characteristic of

---

204 Chekinov and Bogdanov, 2013.
205 Gerasimov, 2019.
modern warfare. Further, the updated 2014 doctrine reinforced this concept, identifying it as the primary characteristic of modern military conflict, discussing things such as the “integrated use of military force” with “political, economic, informational and other non-military measures.” Similarly, the 2013 Foreign Policy Concept identified scientific, economic, and information technology factors as important as military capabilities in terms of influencing people and politics in a target state – theories we see in practice when it comes to Russia’s cyber attacks. Not only do these speeches and strategic documents highlight Russia’s changed thinking in terms of modern conflict and the origins of Russia’s rise as a cyber-power, they emphasize a key element of Russia’s approach to cyber operations, which forms the basis of my theory on Russia’s cyber strategy and electoral autocracy legitimation in cyberspace writ large – manipulating the information space at home and abroad for strategic gain.

In sum, and like China, Russia’s approach to and abilities in cyberspace were not developed in a vacuum. Rather, the Kremlin’s cyber strategy and its rapid growth as a formidable actor in the digital realm was influenced by two main things: several destabilizing events and – as Oleksiejuk (2020) puts it – “the belief of the Russian elite that the whole western world is a threat to Moscow’s security and sovereignty.” Together, these factors are what have shaped the country’s conceptualization of the information domain, as well as the nature of its tactics and strategies in cyberspace. Discussed in detail in section 5.4, this latter factor, being the

---

country’s threat perceptions and constant sense of vulnerability, is fundamental to my theory. Moreover, as I illustrate throughout this chapter, this part of the Russian psyche is something the regime – particularly President Putin – has continually exploited to his advantage in portraying himself as the country’s guarantor of safety, security, and stability. Further, and as the literature on electoral autocracies suggest we should see, the regime has pointed to this idea of being on the defensive as a reason it cannot operate like an advanced liberal democracy. Indeed, in their view, countries determined to inflict harm on Russia are liberal democracies. Finally, and as we will see in the empirical record, Russia’s cyber attacks – much more so than any other autocracy – seek to poke holes in Western liberal democracies. As Diamond said in 2016, President Putin has undertaken a “sophisticated campaign to sabotage democracy and bend it toward his interests, not just in some marginal, fragile places but at the very core of the liberal democratic order.”\(^\text{210}\) As I argue, all of these factors are interconnected, and aligned with key theories throughout the literature on how electoral autocracies seek to legitimize their rule. However, in order to better understand how Russia has used cyberspace to achieve certain strategic objectives in support of regime survival, an overview of some of the country’s most notable cyberattacks is needed. In this next section, I will detail some of these attacks with an emphasis on their attacks against democracies, making clear connections between the data, the literature on electoral autocracies, and my own needs-based theory of authoritarian legitimation in cyberspace.

4.3: FROM MOONLIGHT MAZE TO GUCCIFER 2.0: AN ANALYSIS OF RUSSIA’S CYBER ATTACKS

For over twenty years, and like other authoritarian regimes, the Russian government has been carrying out a range of sophisticated, damaging, and disruptive cyber operations against a diverse mix of targets whose insecurity is seen as strategically beneficial to the Kremlin. However, unlike its autocratic peers analyzed in this research, and as mentioned earlier in this work, Russia’s approach to cyber conflict has been unique in several ways. To start, data on Russian cyber attacks show that the country does not pursue one uniform attack strategy – at least not to the extent we have seen with other nations (e.g. China). Instead, Russia capitalizes on specific opportunities and areas of vulnerability as they emerge, employing the attack type best suited for each scenario.\(^{211}\) These range from cyber attacks in support of military operations (as in the case of conflict with Georgia and Ukraine), against regional rivals and adversaries the Kremlin seeks to influence (e.g. Baltic countries), and more broadly, international operations designed to sow discontent and fear.\(^{212}\) Moreover, the record on Russian cyber attacks illustrates the country’s outlier conceptualization of cyberspace when it comes to the indivisibility between the technical and psychological utility of cyber operations. We see this in operations ranging from attacks on critical infrastructure (e.g. electrical grids) to spreading disinformation in foreign countries (e.g. the U.S., France and Germany) during elections. Indeed, and related to this latter point, more than any other country found in the data or analyzed in this research, Russia carries out cyber operations with the intent of manipulating people, and inflicting strategically beneficial cognitive effects.


While this element of altering public opinion and decision-making in target nations stands out in the data and throughout this chapter, I argue that the totality of their cyber operations tells a cohesive story – one that aligns with my needs-based theory on authoritarian legitimation in cyberspace. In short, and most importantly, Russia’s cyber attacks suggest the country relies on cyberspace to undermine and sabotage liberal democracies worldwide. This is not something we see – at least not to the same extent – with other regimes. Not only does this strategy hurt the Kremlin’s opponents, it strengthens the regime’s narrative that the West’s conceptualization of good governance is flawed, and that alternative forms of authority – such as the one in Russia – are more viable. Further, in target countries, it weakens people’s belief in their own systems, creates cynicism about their democratic governments, erodes public trust and confidence in institutions, and crucially, gives the Kremlin and President Putin an aura of power, sophistication, and legitimacy. Furthermore, the regime has opportunistically but very strategically used cyberspace as a means of waging continual conflict with the West, reinforcing the country’s siege mentality and narrative of being on the defensive. In other words, Putin and the Kremlin have been able to antagonize Russia’s rivals in such a way that those rivals are compelled to respond. By operating in cyberspace, this enables the Kremlin to agitate and deny attribution, while facing international measures it knows it can handle, but which still feed into its defensive narrative. This, I argue, plays into President Putin’s strategy of branding himself the protector of the nation. As Decker (2015) notes, “Putin positions himself as the defender of traditional values against the “corrupt” and “decadent” West.”213 Further to my point, Decker explains, “[Russians] think of Putin as a guardian — as an autocrat, lining up squarely within the

---

tradition of Russian leaders tasked with defending the country from external aggression.”

When it comes to cyber attacks, Putin has been able to carry out numerous operations against his opponents, perpetuating the idea Russia is constantly under threat and engaged in conflict – even if that conflict is short of all-out war. Again, these theories align with what we should expect to see in terms of how electoral autocracies often seek to legitimize their rule through performance and procedure-related claims. Also, when it comes to Putin, and similar to China, I have observed within case variation in terms of Russia’s cyber attacks. As the country has progressively moved away from being an electoral autocracy to more of a personalist regime under President Putin, their cyber attacks have become more focused on preserving Putin’s image as the country’s saviour, and the only person who can protect the nation, restore the country’s sovereignty, and return Russia to great-power status. To illustrate this variation, and to more clearly connect Russia’s cyber attacks to the literature and to my own needs-based theory on authoritarian behaviour in cyberspace, additional analysis on Russia’s record of cyber operations is required. I begin this analysis with Russia’s 1996 espionage operation dubbed “Moonlight Maze.”

Russia’s Ascent to Cyber Supremacy

In the summer of 1998, an information technology specialist working for the company “ATI-Corp” noticed a suspicious connection running from their network, to Wright Patterson Air Force Base in Dayton, Ohio. The connection itself was not particularly peculiar, but the timing of it was. The user was connecting in the middle of the night on a weekend. When asked, the user responsible for that account confirmed they had not been online. Shortly thereafter, Computer

---

214 Decker, 2015.
Emergency Response Teams were mobilized, with the U.S. Air Force being the first to respond.\(^\text{215}\) Identifying further connections to the Air Force base, investigators realized they were dealing with an intruder who – on at least one occasion – had made their move from a server in Moscow. As the investigation progressed, the FBI and other involved parties realized this was not a one-off intrusion – it was a largescale, coordinated attack, carried out with a level of sophistication they had not seen before. Victims included the Army, national laboratories in Los Alamos and Albuquerque, NASA, the Pentagon, the U.S. Department of Energy, and others throughout Canada, the U.K., Brazil and Germany. The severity of the attack was unprecedented, with one of the associated investigations concluding that “the data taken during this period, if printed out, would stretch as high as the towering obelisk of the Washington Monument.”\(^\text{216}\) What made it so sophisticated at the time was that hackers’ method of using third party servers to route communications to avoid detection. Further, and as we will see in other Russian cyber attacks, the hackers also created back doors in the systems they were targeting, with the purposes of coming back later – something they did for nearly two years.\(^\text{217}\) With a clear emphasis on obtaining sensitive defence-related data, including maps of military installations, troop configurations, and military hardware designs, this attack signaled a new era of digital espionage. Indeed, Rid and Buchanan (2015) described it as “the very first large-scale state-on-state computer network intrusion set in history.”\(^\text{218}\) Interestingly, and in line with Russia’s emphasis


\(^{218}\) Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” The Journal of Strategic Studies,
on information superiority discussed earlier in this research, Jensen, Valeriano, and Maness (2019) suggest Russia views cyber espionage as “an additive means of accessing networks for future coercion and stealing sensitive information,” and that “used in conjunction with broader propaganda campaigns, espionage can…influence public opinion.” That said, while Moonlight Maze was by no means Russia’s last cyber espionage attack, many of Russia’s most significant cyber operations beyond that campaign were more explicit in terms of altering the information environment, undermining institutions, manipulating targets, and coercing adversaries. Dubbed “Web War One,” Russia’s first landmark attack of this nature occurred in Estonia, in 2007.

On the evening of April 27, 2007, several government websites in Estonia were knocked offline. In addition, sites including the official presidential webpage, as well as the website of parliament and numerous ministries, were defaced. Hackers also publicly shared tips for taking out the country’s financial and media sectors through coordinated distributed denial-of-service attacks. Part of a broader disagreement between Russia and Estonia regarding the relocation of a pro-Soviet monument in Tallinn, the attacks continued for over three weeks, alongside largescale protests at the Estonian embassy in Moscow, violent clashes between ethnic Russian nationalists and Estonian protestors in Tallinn, and economically disruptive measures designed to hurt Estonian businesses. In terms of cyber conflict, it was a first. As Davis (2007) wrote the same year of the attack, "never before had an entire country been targeted on almost


every digital front all at once.”

Using a range of methods, including overwhelming servers with site visits causing them to shut down, to posting pro-Russian messages and attack instructions in Russian-language chat rooms, to infiltrating individual Estonian websites, the attackers used a multi-front approach to hit their target, causing the country to – albeit briefly – be cut off from the rest of the world. However, in terms of actual damage to critical cyber systems and Internet accessibility, the attack was relatively harmless. Instead, and in-line with Russia’s approach to cyber conflict discussed earlier in this chapter, the damage was – as Segal (2016) notes “highly psychological, putting Estonia's digital vulnerability in stark relief.”

Likewise, Pamment et al. (2019) note that “a key objective [of the attack] was to test and demonstrate cyber capabilities, as well as to sow confusion and uncertainty.” For the Kremlin, this attack was in many ways a trial run of future attacks, where this combination of propaganda, denial tactics, and defacement would be used concurrently to coerce rivals, adversaries, and targets perceived as posing a threat to the country’s interests. Indeed, it is a particularly important example of Russian cyber attacks for this research, as it was the first noteworthy example of Russia – an electoral autocracy – using cyberspace to disrupt and undermine democratic institutions in other nations. Further, it was the first major Russian cyber attack that highlighted Russia’s use of cyber attacks to inflict psychological harm on its targets – something it continues to prioritize today. Following the attacks in Estonia, Russia used similar tactics in Georgia, in 2008. The difference this time though, was that Russia’s digital attacks were combined with traditional military action – another first in cyber history.

---


Weeks before the first shot was fired in the Russo-Georgian War of 2008, Russian cyber attacks hit several government, media, financial, transportation, and communication websites in Georgia.\textsuperscript{224} All told, fifty-four websites suffered denial-of-service or defacement attacks, with the average access outage lasting just over two hours – the longest lasting six. Over a third of Georgia’s Internet networks experienced access or functionality issues during the campaign, with attack activity peaking at the same time Russia invaded South Ossetia from August 8-10.\textsuperscript{225} Yet, while Russia’s cyber attacks on Georgia did not result in a decisive victory, they again, as White notes “reinforced the Russian interpretation of cyberspace as a tool for holistic psychological manipulation.”\textsuperscript{226} Further, and in line with my theory on the Kremlin’s siege mentality and prioritization of performance-related claims to legitimacy, the conflict with Georgia allowed the Kremlin to claim it was preventing “encroachment” by the North Atlantic Treaty Organization (NATO), the same year NATO – an organization Russia views as part of its enduring conflict with the West – agreed Georgia would become a member. In the time since, and building off of lessons learned from their 2008 cyber campaign against Georgia, Russia continues to pursue information operations in the country through cyberspace with, as Shaishmelashvili (2021) writes, the main message being “integration with Western institutions is detrimental to the traditional Georgian identity.”\textsuperscript{227} Ultimately, over the last decade, and relying on this narrative, Russia has used cyber operations to achieve its main objectives: preventing Georgia’s formal

\textsuperscript{226} White, 2018, pp. 2.
\textsuperscript{227} Giorgi Shaishmelashvili, “Russia’s Permanent War against Georgia.” Foreign Policy Research Institute, March 2, 2021: https://www.fpri.org/article/2021/03/russia-permanent-war-georgia/
inclusion into NATO, challenging Georgia’s strategic partnership with the U.S., and creating a military presence in the South Caucasus. In sum, Russia’s use of cyber attacks during the 2008 Russo-Georgian war was a landmark event for several reasons. First, it proved to the Kremlin that cyber attacks could be a useful force multiplier in advance of and during an armed conflict. Second, it proved to be a valuable tool Moscow could use to cultivate and maintain tension over a prolonged period. Third, and most relevant for this research, it served as a harbinger of what Moscow would do to other regional neighbours, and what eventually, it would start doing to its Western foes: psychologically manipulating its opponents, using cyberspace to erode public trust in democratically elected governments and institutions, and bringing into question the strength of Western liberal democracy – all integral elements of Moscow’s legitimation strategy.

From 2008 until around 2014, Russian cyber attacks – at least in terms of what is available in the data – appear to be relatively inconsequential. In fact, in some instances, lone hackers were responsible for the most damaging intrusions, including the theft of millions of credit and debit card numbers, causing hundreds of millions in damage. Further, in 2009, weeks before the Copenhagen Climate Summit, servers at the Climate Research Institute at the University of East Anglia were hacked by unknown persons. The intruders stole thousands of private emails and files dating from 1991 to 2009, and released them publicly on a Russian server where they claimed the files showed scientists had conspired to inflate the severity of the climate crisis. However, it should be noted that in Russia, attribution is particularly

228 Shaishmelashvili, 2021.
challenging given the Kremlin’s longstanding ties to criminal hacking groups.\textsuperscript{231} As Dr. Brandon Valeriano told me: “attribution can be an issue in the case of Russia – while the government might directly support hackers, it might also just turn a blind eye to them, which is actually quite different.”\textsuperscript{232} Nevertheless, there was a noticeable downturn in Russian cyber attacks throughout this period, which I argue is likely attributed to the aforementioned Putin-Medvedev tandemocracy where, barred from serving a third consecutive term as President, Vladimir Putin assumed the role of Prime Minister under President Dmitry Medvedev. Though Putin likely remained the paramount leader during this period of political cooperation, I argue this downturn in cyberattacks was a result of Putin’s responsibilities, power, and influence being divided with Medvedev. Regardless of how inconsequential that division may have been, Putin was not the only leader of Russia from 2009-2012. However, by 2013, with Putin once again the unitary leader of Russia, there was a noticeable uptick in Russian cyberattacks. From Finland’s Ministry of Foreign Affairs being hacked for espionage purposes, to intruders infiltrating the U.S. Department of State, to the Ukraine government being hacked, among others, it appears that Russian cyber attacks became more persistent once Putin regained power. As Putin sought to increasingly consolidate his power, bolster his sphere of influence, mitigate perceived physical insecurities, and deliver on the country’s expansionist goals, the country’s cyber attacks became particularly pervasive. This surge in cyber attacks became especially noticeable in 2014 – the same year Russia invaded Ukraine, and annexed Crimea.

Before the first Russian troops entered the Crimean peninsula in February 2014, Russian cyber operations had crippled the country’s telecommunications infrastructure, disabled

\textsuperscript{232} Dr. Brandon Valeriano was interviewed for this research on October 29, 2021.
important Ukrainian websites, and disrupted the communication abilities of senior Ukrainian officials.\textsuperscript{233} In addition, throughout the ground invasion, Russia used a range of cyber operations to gain the upper, accelerate their military objectives, isolate Kiev and, as Valeriano, Jensen, and Maness write – “demonstrate the futility of the Ukrainian state.”\textsuperscript{234} For example, in early 2014, networks in Ukraine were hit with a barrage of DDoS attacks emanating from Russia. There were also brazen attacks on several pro-Ukrainian targets, including DDoS attacks on numerous NATO websites, on the German Ministry of Defense, Germany’s Parliament, and Chancellor Angel Merkel’s website. Further, defacement attacks hit a range of Polish and Ukrainian websites throughout 2014 with pro-Russian narratives. These included attacks on Poland’s stock exchange, on a range of Ukrainian government websites during then Vice President Joe Biden’s visit to Kiev, and on several electronic billboards in Ukraine.\textsuperscript{235}

In addition to the aforementioned attacks, Russia carried out an even more significant intrusion during the conflict in Ukraine – one with a particularly strong nexus to my theory on the Kremlin’s legitimation strategy. This cyber operation involved Russia combining cyber espionage, alongside disruption, and propaganda, to undermine the legitimacy of Ukraine’s democratic election in 2014.\textsuperscript{236} For Russia, this combination of tactics proved to be a useful, low-cost, low-risk strategy in fundamentally altering internal and external confidence in the election, as well as in the procedures and performance of the Ukrainian government – a move the Kremlin

\begin{itemize}
\item \textsuperscript{233} Emilio J. Iasiello, “Russia’s Improved Information Operations: From Georgia to Crimea.” Parameters, the U.S. Army War College, Issue 7, Volume 2, 2017.
\item \textsuperscript{234} Valeriano, Jensen, and Maness, 2018.
\item \textsuperscript{236} Valeriano, Jensen, and Maness, 2018.
\end{itemize}
has repeatedly pursued to bolster the image of its own procedures and performance – something we know through this research is crucial for electoral autocracies and their legitimation. As Clayton (2014) describes, in May 2014, hackers broke into Ukraine’s central election computers where they deleted troves of important files, destroying the operability of the vote-tallying system. The following day, the hackers stated they had destroyed the election’s network infrastructure, leaking emails and documents online as proof they had successfully crippled the country’s ability to sufficiently carry out the election.237 In addition, the hackers installed a sophisticated type of malware, giving them the ability to manipulate (or at least try to) the actual results, showing a decisive victory for the pro-Russian, ultra-nationalists. In addition, and in line with Russia’s cyber strategies discussed earlier in this dissertation, hackers also carried out a range of “false flag operations” – a tactic used to both conceal the identity of the attackers, and undermine the legitimacy of the target. Again – a strategy Moscow consistently uses to erode the merits of its democratic rivals as a means of legitimizing its own procedures, performance, and illiberal form of government. In short, false flag operations are a form of covert action carried out to sow confusion, deceive the target, and manipulate their perception of the environment.

In the case of the Russo-Ukrainian War, in 2014, “Anonymous Ukraine” – a hacking group linked to the Kremlin working against Ukrainian independence – claimed to have obtained documents showing the U.S. Army attaché in Ukraine was working with his Ukrainian counterpart to carry out its own false flag operations, designed to make Russia look responsible.238 Then, in March 2015, the hacking group known as “CyberBerkut” released

documents they claimed were hacked from the Ukrainian government and U.S. defense contractors, showing U.S. plans to move weapons into Ukraine with the help of European allies.\textsuperscript{239} That same month, in another attempt to discredit the Ukrainian government, CyberBerkut released documents online they claimed were evidence that Ukraine was sending weapons to the Islamic State, including surface-to-air missiles.\textsuperscript{240} Exploiting existing conspiracy theories that Jewish billionaire George Soros is part of some deep-state cabal, the group also released materials they said were hacked from the Soros Foundation, showing Soros was working with the Americans to provide military support to Ukraine.\textsuperscript{241} Throughout the conflict with Ukraine, which continues to this day, Russia also physically sabotaged vital underwater sea cables connecting the Crimean Peninsula with Ukraine, used planted malware on Ukrainian military targets to geo-locate and strike them, sabotaged critical infrastructure such as electric grids, and manipulated social media to propel the Kremlin’s narratives, among other things.\textsuperscript{242}

While analyzing Russia’s cyber strategy and activities throughout the 2022 war in Ukraine remains a moving target, the Kremlin has already undertaken a range of operations that mimic much of what we have seen in previous years and invasions. Indeed, as recently as May 10, 2022, U.S. Secretary of State Anthony Blinken said in a statement “in the months leading up

\begin{footnotesize}
\textsuperscript{242} Chris Baraniuk “Could Russian Submarines Cut off the Internet?” BBC, October 26, 2015: \url{http://www.bbc.com/news/technology-34639148}  \\
\end{footnotesize}
to and after Russia’s illegal further invasion began, Ukraine experienced a series of disruptive cyber operations, including website defacements, distributed denial-of-service attacks, and cyber attacks to delete data from computers belonging to government and private entities – all part of the Russian playbook.”

Likewise, Cattler and Black (2022) recently wrote, “all available evidence indicates that Russia has employed a coordinated cyber-campaign intended to provide its forces with an early advantage during its war in Ukraine.”

Moreover, and counter to claims made in the initial days and weeks of the conflict that Russia had abandoned its cyber arsenal in Ukraine in favour of armed kinetic attacks, Cattler and Black rightly point out that “on the day the invasion began, Russian cyber-units successfully deployed more destructive malware—including against conventional military targets such as civilian communications infrastructure and military command and control centers—than the rest of the world’s cyberpowers combined typically use in a given year.”

Confirming Russia’s cyber assault on Ukraine, Microsoft released a report on April 27, 2022 detailing hundreds of destructive cyber attacks, in combination with “…broad espionage and intelligence activities” as well as disinformation campaigns designed to “…shake confidence in the country’s leadership.”

Taken together, Russia’s ability to utilize cyberspace in so many different ways during a single conflict – a conflict that rages on to this day – has marked a turning point in terms of cyber warfare. Further, from an information superiority perspective, Russia’s campaign was and is a watershed example of how the digital domain can be leveraged to obfuscate the environment and

---


245 Cattler and Black, 2022.

shape the narrative in favour of one side. Going back to my theory on legitimation, Inkster (2016) notes, the cyber operations Russia used throughout the conflict with Ukraine relied on “the fact that Western governments simply lack resources that would be required…to refute or debunk the huge number of stories put out…thereby giving a veneer of legitimacy to Russian fabrications.”

In 2014, the same year the Russo-Ukrainian War began, and less than two years after Vladimir Putin regained his position as the unitary leader of Russia, Moscow expanded its information operations on democratic nations beyond the Eastern Bloc. For instance, in 2014, far right French candidate Marine Le Pen and her party the Front National received a nine million euro loan (approximately $13 million CAD) from the Kremlin to finance her campaign, after French banks had refused, citing her party’s history of antisemitism and extremist positions.

Also in 2014, the website of Poland’s electoral commission’s was taken offline, rendering it unable to publish election results, ultimately undermining the credibility of the vote. The following year in 2015, the computer network of Germany’s Parliament was taken offline, in what one German hacking expert called “an embarrassing” episode for the government. In 2016, reports surfaced that Russian hackers had undertaken a disinformation campaign in 2014 to influence the Scottish independence referendum. Moreover, in advance of Finland’s 2015

---

parliamentary elections, fake Twitter accounts created to appear as legitimate Finnish government users began tweeting fringe content designed to – as one Finnish official put it – “muddy the waters” of the election.\textsuperscript{252} These examples only represent a fraction of Russia’s election meddling. Indeed, Way and Casey (2018) identified 16 elections Russia sought to influence between 2015-2018 alone – the majority of which they targeted through cyberspace.\textsuperscript{253}

One of these cases, and the final example of Russian cyber attacks discussed in this chapter, was Moscow’s manipulation of the 2016 U.S. Presidential election. This case, perhaps more than any other example, exemplifies Russia’s approach to cyber conflict and the Kremlin’s strategic objectives in disrupting democratic elections and institutions. Further, this specific Russian cyber campaign reinforces several key elements of my theory on how electoral autocracies behave in cyberspace. For these reasons, this case warrants special attention.

As illustrated throughout this chapter, Russia has targeted several countries in the near abroad with cyber attacks designed to alter the information environment in the Kremlin’s favour. Typically, these operations have been carried out as a means to shape rival behaviour, erode public trust in democratic institutions and procedures in target countries, and influence public opinion and regime support in Russia, among other things. However, despite their significance, these types of Russian cyber attacks fell short of war, and were for the most part, contained within Europe. For these reasons, Russia’s meddling in the 2016 U.S. election appear to have caught American officials off-guard. As I mentioned in Chapter 1, overt cyber catastrophes tend to dominate policy and political discussions when it comes to cyber – not the type of clandestine

\textsuperscript{252} Committee on Foreign Relations: United States Senate, 2018.
\textsuperscript{253} Lucan Ahmad Way and Adam Casey, “Russia has been meddling in foreign elections for decades. Has it made a difference?” The Washington Post, January 8, 2018: https://www.washingtonpost.com/news/monkey-cage/wp/2018/01/05/russia-has-been-meddling-in-foreign-elections-for-decades-has-it-made-a-difference/
espionage operations Russia favours. As Lipton, Sanger, and Shane wrote in 2016 “American officials did not imagine that the Russians would dare try those techniques inside the United States. They were largely focused on preventing what former Defense Secretary Leon E. Panetta warned was an approaching ‘cyber Pearl Harbor.’”

According to Valeriano, Jensen, and Maness, “the focus on the spectacular rather than the mundane blinded the United States to a critical insidious threat to the stability of the American system.” For these reasons, U.S. officials failed to realize that Russia was attacking them – not from afar – but from within.

Russia’s cyber campaign to undermine the 2016 U.S. election began long before voters took to the polls. In March 2015, the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) kick-started the operation by sending out thousands of phishing emails containing malicious links to diplomatic and military targets. Undetected for over a year, the hacking groups – Cozy and Fancy Bear – were able to penetrate the computer networks of the Democratic National Committee (DNC) where they monitored DNC communications, accessed sensitive files, and exfiltrated them for dissemination and manipulation. One hacker in particular – “Guccifer 2.0” – claimed responsibility for the penetration. According to Sanger and Corasaniti (2016), the files included “a trove of opposition research against Donald J. Trump.” In addition, the hackers were able to access emails and documents from Hillary Clinton.

---


Clinton and her campaign team, including former White House Chief of Staff and campaign lead, John Podesta. Throughout the course of the election, the hackers leaked these documents strategically, finding opportune times to ensure they had as much impact on shaping public opinion as possible. For example, Podesta’s emails were leaked the same day a recording was released where President Trump remarked on his ability to grab women. In September 2017, Facebook also publicly acknowledged that they had sold over $100,000 dollars worth of online ads to a Kremlin-linked company. Using hundreds of fake accounts, the Internet Research Agency made thousands of posts on polarizing social issues including gay rights, gun control, and race.\textsuperscript{259} Some estimates suggest as many as 70 million Americans – or roughly, 30 percent of adults in the U.S. saw the ads.\textsuperscript{260}

Together, these activities illustrate a three-pronged cyber approach to Russia’s meddling in the 2016 Presidential election: hacking or using insider threat actors to access computer networks, exfiltrating the information, spreading it, and manipulating it, and amplifying the message and reach of the content using troll farms or fake accounts. As Valeriano, Maness, and Jensen note, this process can be thought of as the “acquire, release, and spread method” – a strategy that “allows the aggressor to target the enemy and manipulate critical audiences through digital means.”\textsuperscript{261} However, it should be noted that while sophisticated, Russia’s cyber strategy during the 2016 U.S. election benefited from having a U.S. presidential candidate – Donald Trump – parroting much of the dis- and mis-information the Russians were spreading. In fact, Trump’s campaign so frequently spread false information that cyber expert Clint Watts said in


\textsuperscript{260} Kevin Poulsen, Spencer Ackerman, and Ben Collins, “Russia’s Facebook Fake News Could Have Reached 70 Million Americans.” The Daily Beast, September 8, 2017: https://www.thedailybeast.com/russias-facebook-fake-news-could-have-reached-70-million-americans

\textsuperscript{261} Valeriano, Maness, and Jensen, 2018, pp. 132.
2017: “It’s hard to distinguish sometimes: did the Russians put it out first or did Trump say it and the Russians amplify it? That’s where you get into some trickery about it.”

All told, and in line with my theory, Russia’s main goal in 2016 was to cognitively affect U.S. voters and American society, exploiting and exacerbating existing social fissures, while at times, creating new ones. Simultaneously, the Kremlin also sought to illustrate to the Russian people the futility and corruption inherent in democratic institutions, performance, and procedures. As I will expand on further in the next section of this chapter, this also reinforces my theory on electoral autocracy legitimation in cyberspace. As Dickinson (2021) writes: “the aim of all this is not to defeat the West, which Russia recognizes as impossible. Instead, Moscow seeks to secure its own position by undermining the allure of the liberal traditions and democratic institutions that allow the Western world to dominate the global imagination.”

In addition to these multifaceted, highly publicized and analyzed cyber campaigns, the Kremlin has also carried out countless cyber operations designed to limit criticism, embarrassment, and information that could de-legitimize President Putin’s ‘right to rule.’ To remind, the literature on authoritarian legitimation strategies tells us that personalist autocracies typically rely on the qualities of the leader as the basis for legitimacy claims. Further, personalist autocracies also rely heavily on performance-based claims to legitimacy. However, these goal-oriented agendas vary from country to country. As I have argued in this chapter thus far, President Putin’s performance-based goals are intertwined with Russia’s siege mentality, the country’s perception as constantly being on the defensive, and his abilities in elevating the

---


country to great-power status. Similar to what I detailed in the previous chapter on China and Xi, President Putin has leveraged the cyber domain to quell any attempts to question his legitimacy. These attacks have become more pronounced over the last decade as Putin has gradually consolidated his power and moved the regime towards greater personalist rule since re-gaining his role as President in 2012. This transition to a personalist autocracy is perhaps most evident in Russia’s 2020 constitutional reforms that include an amendment permitting him to run for the presidency again in 2024 – and to stay in power until 2036. As Russian opposition politician Alexander Solovyev said in 2020, “[Putin] is setting himself up to be sort of a father of the nation, an ayatollah, a demigod.”

Indeed, similar to changes we saw in China from Hu to Xi, Russia also underwent immense change as Putin succeeded former President Boris Yeltsin in 2000. Yevgeny Volt, former head of the Heritage Foundation’s Moscow Office discussed this change in 2007 saying, “[Yeltsin] was sincere in his aspiration to freedom and his rejection of totalitarian regimes. Putin, considering his former activities, his background, could not have appreciated Yeltsin's rule, with its rights for mass media, for oligarchs, for civil organizations.” While Yeltsin sought to modernize the country politically, economically, and socially, including as Winston (2000) puts it “the wholesale import of Western-style political machinery” Putin has progressively forestalled those changes, even reverting them. At the same time, Putin has sought to increase his control of Russia and the Russian people – often using cyberspace to achieve these objectives,


insulate himself from criticism and dissent, and preserve his image as Russia’s saviour. For instance, in 2011, Russia’s online blogger community faced a slew of damaging cyberattacks after publishing content that was critical of Putin and the regime. Further, in 2016, reports surfaced that Kremlin-backed hackers had gained access to a philanthropic website run by George Soros, where they manipulated documents making it appear as though Putin critic and anti-corruption activist Alexi Navalny (now forcibly held in Russia) had received financial support from Soros. In reference to this cyber operation, Navalny said, “the focus of discussion is switched from ‘Putin’s corruption’ to ‘opposition and its shadow money.’” More significant, in 2017 a team of researchers uncovered evidence that a journalist critical of Putin and the regime had their documents hacked, exfiltrated, manipulated, and then re-released in an effort to discredit the critic. As the authors noted, the operation was likely a product of “Russian domestic policy concerns, particularly around offsetting and discrediting what are perceived as “outside” or “foreign” attempts to destabilize or undermine the Putin regime.” Moreover, the authors also found evidence that the operation was designed to discredit reports detailing corruption within Putin’s inner circle. Also in 2017, it was reported that hundreds of journalists had been the victims of Russian cyber attacks. These included attacks against New York-based author Masha Gessen who wrote the book “The Man Without a Face: The Unlikely

266 David Winston, “From Yeltsin to Putin,” the Hoover Institute, April 1, 2000: https://www.hoover.org/research/yeltsin-putin
269 Groll, 2016.
271 Hulcoop et al., 2017.
Rise of Vladimir Putin,” as well as Roman Shleynov, a Russian journalist who covered the 2016 Panama Papers scandal which embroiled Putin in an embarrassing episode regarding his wealth. Similar to the 2017 attacks that sought to discredit journalists, in 2021 Microsoft reported it had found evidence that a Russian intelligence agency had hacked into the computer networks of the U.S. State Departments Agency for International Development to gain access to “human rights groups and other organizations of the sort that have been critical of President Vladimir V. Putin.” In March and April of 2021, numerous U.S. think tanks and international organizations were targeted by Russian entities with a spear-phishing campaign. Pretending to be Leonid Volkov, chief of staff to Alexei Navalny – Putin’s most well known and outspoken critic – the hackers (or possibly pranksters with links to the Kremlin) tried to coax several organizations critical of Putin into embarrassing on-camera conversations with a Volkov impersonator. Reports have also found that “hundreds” of Russians have been hired to pump out pro-Putin messages and narratives online within Russia – “no Russian triumph under [Putin’s] rule was too small to warrant a celebratory tweet, meme or post” one insider wrote after infiltrating the group.

I interviewed Russia expert Keir Giles about Putin’s approach to cyber conflict. Speaking about much of what I have just covered, Giles told me that for Putin and the Kremlin, their approach to cyberspace is largely driven by a “war on history.” Interestingly though, according to Giles, and as the empirical record shows, the bulk of the Kremlin’s cyber attacks to legitimize Putin are defensive or responsive. For instance, Giles told me the Kremlin will “pursue people who post inconvenient facts on social media that don’t accord with the

---


government’s approved view of history…but in terms of pro-active means to portray a positive imagine of the regime, there is far less of that.”\textsuperscript{275}

In this final section, I provide further analysis on how the information throughout this chapter on Russia’s cyber attacks and behavior in the digital realm align with some of the key theories on autocratic legitimation, both in terms of electoral autocracies, as well as personalist dictatorships in the case of Putin. With this final section, it should become clearer how the examples I have used from the empirical record support my needs-based theory on autocratic legitimation in the cyber domain.

\textit{Russian cyber attacks and regime legitimation}

The literature tells us that electoral autocracies rely primarily on performance and procedure-based claims to legitimacy – at least relative to other regime types. Further, the literature also tells us that personalist regimes rely heavily on the qualities of the leader to boost support among regime elites and the general population. We are also told that personalism-based claims to legitimacy often represent a discursive mechanism emphasizing the centrality of the leader in terms of certain grand achievements and agendas, such as economic prosperity, national unity, and security.\textsuperscript{276} With these theories in mind, I suggest we should see these legitimation strategies play out in the cyber domain. In other words, the expectation is that electoral autocracies will find ways to emphasize their performance and procedures in the digital realm, while personalist-based autocracies will focus more on perpetuating certain narratives about the qualities of the leader and on the centrality of the leader in delivering on specific goal-oriented agendas. In the case of Russian cyber attacks and the Kremlin’s behaviour in cyberspace, these

\textsuperscript{275} Keir Giles was interviewed virtually for this dissertation on November 12, 2021.  
\textsuperscript{276} Von Soest and Grauvogel, 2018.
theories have held true. As noted in chapter 1, while we cannot say definitively at this point that there is a direct correspondence between these regime types and specific trends in cyber behaviour, I have illustrated new and novel affinities that warrant further examination.

First, the Russian government has consistently undertaken cyber operations to destabilize, discredit, undermine, and erode global confidence and belief in western liberal democracies. The Kremlin’s primary objective with these operations has not been to hurt democracies in and of themselves, but rather, to strengthen the image of their own illiberal policies and procedures at home and abroad. By making the free and open societies of their adversaries in the West appear weak, Putin and the Russian government have been able to perpetuate the veneer of being more legitimate and more stable than their democratic rivals. When I interviewed CATO Institute Senior Fellow and cyber expert Dr. Brandon Valeriano, he told me that in some ways, Russia’s attacks on Western democracies are not intended to “destabilize the west, but to demonstrate how unstable democracy is to the east.”

Moreover, and also in line with my needs-based theory on autocratic legitimation in cyberspace, the Russian government has also used cyberspace to maintain low-risk conflict below the threshold of armed warfare, thereby allowing the Kremlin to perpetuate the neurotic Soviet tradition of perceiving itself as under siege or on the defensive. As Dr. James Lewis has said, it is important for Russia to “tear us down to prove that we're just as bad and corrupt as they are.” As I have illustrated in this chapter, the Kremlin has relied heavily on cyberspace to achieve this strategic objective. Linking this back to theories on electoral autocracies and legitimation, not only does this approach strengthen belief in the Kremlin’s undemocratic procedures, it gives the Kremlin the appearance of protecting the

277 Dr. Brandon Valeriano was interviewed virtually for this dissertation on October 18, 2021.
278 Alex Lockie, “Russia has a grand plan to undermine the West’s democracies — and it's working.” Business Insider, October 30, 2016: https://www.businessinsider.com/russia-undermine-west-democracies-2016-10
country from hostile actors in the West – namely the U.S. – who continue to encroach on Russia, challenging its sphere of interests. In sum, Russia – a country typically defined as an electoral autocracy throughout the literature – has used cyberspace much more than any other country found in the data to attack and undermine the institutions and procedures of actual democracies around the world. This is a puzzling observation which I believe my theory, at least in part, sheds new light on.

In addition to this, and similar to what I detailed in the previous chapter on China, I have observed within-case variation where Russia’s cyberattacks have become increasingly focused on protecting President Putin’s image as he has gradually consolidated power. Importantly, several scholars have noted this shift towards greater personalist rule under President Putin, as well as how claims to legitimacy have also changed during this transition. More specifically, and as the authors note, Russia’s government has taken on a more personalist tone since 2012 – just after Putin regained the Presidency following the Putin-Medvedev tandemocracy referenced earlier in this chapter. Additionally, by 2012, the country’s economic situation had deteriorated significantly, at least relative to Putin’s earlier years in power, thereby making it harder for the regime to focus on economic performance-based claims to legitimacy. Instead, the focus of legitimation became Putin himself. As von Soest and Grauvogel suggest, “Russia’s regime has…taken a very strong populist approach, and President Putin has been termed “leader of the nation.” Further, and related to theories on personalist autocracies and legitimation, Putin has portrayed himself as a stoic leader who – above all else – works for the good of the Russian

---


people, and who has, as Holmes (2010) puts it “succeeded in giving [the Russian people] back a sense of pride and identity.” Putin has also increasingly focused on tapping into the country’s collective memory to generate support and boost his own legitimacy. As Olimpieva (2016) has suggested, Putin has sought to take lessons learned from past conflicts, blend them with narratives regarding Russian victimization and suffering, and apply them to current and future confrontations. In other words, Putin has strategically constructed a narrative wherein the wars of the past have never really ended – they have only evolved and taken shape – and only he can fight those fights and protect the Motherland. As this strategy has become more pronounced, and as the qualities of Putin’s person and his image as saviour of the nation have become a more important source of legitimacy than other forms of performance (e.g. economic), Russia’s cyber attacks have also become more focused on preserving this image.

To conclude, for the government of Russia, and increasingly for President Vladimir Putin, cyberspace has become an invaluable tool that can and has been used for regime legitimation. From using cyberspace to carry out espionage operations, to campaigns designed to weaken liberal democracies, to attacks on a range of entities critical of Putin, the cyber domain has progressively evolved into a favoured tool of the Kremlin to maintain certain Soviet traditions and narratives, while simultaneously exercising a new and technologically enabled form of Russian power and influence. Throughout this chapter, I have illuminated connections between key theories on autocratic legitimation, and authoritarian behaviour in cyberspace. However, like Chapter 4, this work is only a first step in connecting these areas of study, and on

---

linking the empirical with the theoretical. Further and more granular analysis is required if we are to better understand the correlation between regime type in Russia, and Russian cyber attacks – though the findings and theories discussed in this chapter provide a valuable starting point. In the following chapter, I undertake a similar though more concise study of authoritarian legitimation and cyber behaviour in North Korea under Kim Jong-un. The purposes of this next chapter is to determine the extent to which theories on personalist regime legitimation strategies translate to cyberspace.
CHAPTER FIVE

BITCOIN TO BOMBS: NORTH KOREA’S CYBER STRATEGY AND THE PRESERVATION OF KIM JONG-UN

5.1 INTRODUCTION

Although the authoritarian regime in North Korea led by Kim Jong-un fails to provide basic necessities and technological comforts to its citizens, Pyongyang has aggressively worked towards developing advanced capabilities in cyberspace which few nations in the world possess. While North Korea focused primarily on undertaking DDoS attacks against South Korea in the mid 2000s, the regime has steadily improved its digital capabilities to create a complex and advanced toolkit of disruptive cyber tactics that have been used to consistently target a range of entities worldwide, and to achieve key strategic objectives for Kim and his regime. More specifically, while North Korea’s cyber activities have – like other nations – varied in terms of type and scope, the country has uniquely focused on carrying out cyber attacks as a means of acquiring money and other forms of financial assets (e.g. crypto currency) and, as observers commonly point out, fueling the country’s nuclear program. Indeed, as Kim (2018) notes: “unlike their counterparts elsewhere, who might seek to expose security vulnerabilities, steal corporate and state secrets, or simply sow chaos, North Korean hackers have a singular purpose: to earn money for the country, currently squeezed by harsh international sanctions for its rogue nuclear program.”^{283} Similar, Dr. James Lewis told me that North Korea has two goals in cyberspace – “harassing South Korea, and occasionally other countries like the U.S. is a key objective, but their primary goal is to generate revenue for the Kim regime.” That being said,

while works analyzing North Korea’s cyber activities overwhelmingly focus on its financial motivations in the digital domain, with specific emphasis on the regime’s weapons program and desire to obviate international sanctions, very few have sought to assess the linkages between North Korea’s regime type, and the strategic importance of financial resources.

As mentioned in previous sections, I classify North Korea as a personalist autocracy given the fact that a single person controls access to political office, makes all critical policy decisions, and exercises absolute control over the security forces.\textsuperscript{284} Further, as the literature tells us, personalist rulers may be backed and supported by either the military or a regime party, but ultimately, neither of these organizations exert any substantive power. Rather, that power rests with one individual ruler.\textsuperscript{285} As Brooker (2008) suggests, a personalist autocracy is essentially an (almost) ‘institutionless polity.’\textsuperscript{286} Weeks (2012) speaks to this as well, writing “a defining feature of personalist regimes such as North Korea under [the Kim family], Iraq under Saddam Hussein, the Soviet Union under Stalin, Syria under the Assads, and Libya under Gaddafi is that their leaders do not face a strong, organized domestic audience able to exert ex ante or ex post constraints on their policy choices.”\textsuperscript{287} Crucially, works on authoritarian regime structure and legitimation also indicate that personalist regimes are often comprised of and dependent on patronage networks, access to, and the distribution of, financial resources.\textsuperscript{288} Indeed, as Kailitz

\textsuperscript{284} Barbara Geddes, “What Do We Know about Democratization after Twenty Years?” \textit{Annual Review of Political Science} 2: 1999, pp. 115–44.


\textsuperscript{287} Weeks, 2021, pp. 330.

writes “as soon as the personalist autocrat cannot provide enough “booty” to his personal gang, they will start to look for an alternative. Eventually the personalist autocrat is alone in his fight to survive.” Likewise, Tannenberg et al. (2020) find that “personalistic regimes, because their rule relies upon the neopatrimonial distribution of resources, delivering the goods to key constituencies is seen as a kind of performance on the basis of which legitimacy claims can be made.” In a 2020 study, Stockemer and Kailitz also suggest that leaders in authoritarian regimes with the ability to acquire and/or generate disposable financial resources, can invest more heavily in themselves and important institutions such as state security forces (e.g. the military and police) creating further distance between themselves and the population, thereby increasing the longevity of the regime.

Further, and as covered in previous chapters, we also know that personalist regimes tend to focus on the qualities and attributes of the ruler, and on perpetuating and preserving the notion that the ruler possesses an extraordinary personality and abilities, and that they have been chosen ‘from above’ to fulfil a certain mission. Often, as in the case of North Korea, personalist autocrats also suggests they have obtained traditional authority through hereditary succession. With these theories in mind, the intent of this final case study on North Korea is to determine whether they hold true in the digital realm. Ultimately, with North Korea identified as a personalist autocracy, the regime’s cyber attacks should be characterized by attempts to acquire

---

financial resources as a means of regime legitimation. In addition, and similar to what I illustrated in both the China and Russia case studies, North Korea’s cyberattacks should attempt to strengthen the image of Kim as the ‘father of the nation’ and to limit his exposure to any humiliation, condemnation or rebellion.

The following chapter on North Korea is broken into several sections. The first provides a high-level overview of North Korea’s rise as a formidable threat actor in cyberspace, with detail on how the country’s cyber arsenal has steadily grown from the days of Kim Jong-il to his son, Kim Jong-un. The second section explores the empirical record of North Korea’s cyber attacks, with emphasis on how Pyongyang’s behaviour in cyberspace has become increasingly focused on cyber attacks designed to acquire money. Finally, the third section explains how North Korea’s cyber attacks align with the core theories on personalist autocracy regime legitimation, and how the ‘Hermit Kingdom’s’ behaviour in cyberspace supports my needs-based theory on authoritarian legitimation.

5.2 BACKGROUND: JUCHE, CYBERSPACE, AND THE ORIGINS OF NORTH KOREA’S CYBER POWER

For decades, North Korea has undertaken a range of activities designed to signal the country’s national power and provoke international responses.293 Falling short of armed conflict, these acts of aggression typically highlight the regime's nuclear ambitions, as well as their prioritization of asymmetric capabilities – notably, the country’s ability to inflict harm in cyberspace – a signal that has become increasingly important to Pyongyang. More specifically though, North Korea’s objectives in carrying out these acts of aggression and increasing their

abilities to operate in cyberspace reflect the fact that North Korean military strategists realize there would be a significant imbalance between the country’s conventional warfighting capabilities and the opposing side, should an armed conflict arise. However, as Pinkston (2016) notes, North Korea’s objectives in strengthening and using asymmetric capabilities – particularly its cyber capabilities – have gradually taken on increased utility beyond preparing for future military conflict. Indeed, the country has undertaken cyber espionage operations, influence operations, and cyber crime activities – all of which have helped the country punch above its weight militarily, project power internationally, control its population domestically, and stave off total economic collapse. In fact, the country’s asymmetric cyber capabilities have been an enduring element of the country’s economic and technological survival since the 1980s.

It was in the 1980’s that North Korea – under the leadership of Kim Jong-il – that the country undertook its first serious steps in creating a comprehensive cyber framework. In 1983, the regime developed its first computer assembly plant, and by 1985, it had opened an electronic computation college. The following year, in 1986, the Pyongyang Informatics Center opened with the objective of creating software and automated systems and technology for a variety of industrial purposes. The same year, the regime hired two-dozen Soviet cyber experts to train “cyber-warriors” at the country’s Mirim Command Automation College (later changed to the Kim Il Military College). By 1990, the country had also established the

---

295 Pinkston, 2016.
297 Ibid.
298 Ibid.
government’s official information technology research center – the Korea Computer Center. However, North Korea’s focus on accelerating its proficiencies in cyberspace were – like China and Russia – fueled by witnessing the U.S. and other countries use electronic warfare technologies in other conflicts – specifically, the first Gulf War in 1991, and NATO operations in the Balkans in 1995. In 1995, the same year NATO was using electronic warfare tactics to confuse Serbian defenses, Kim reportedly said, “if warfare was about bullets and oil until now, warfare in the 21st century is about information. War is won and lost by who has greater access to the adversary’s military technical information in peacetime, how effectively one can disrupt the adversary’s military command and control information, and how effectively one can utilize one’s own information.”

It was clear the Korean People’s Army (KPA) were now going to increase their focus on the cyber domain. Moreover, in a separate speech, Kim went further, saying “if the Internet is like a gun, cyber-attacks are like atomic bombs”; and “modern war is decided by one’s conduct of electronic warfare,” thus “cyber units are my detached force and backup power.” The following year, in 1996, the country’s first known Internet link, connecting North Korea and the outside world was created through the Pyongyang office of the United Nations Development Program. Following this, and with a sizeable amount of infrastructure in place and research underway, the country began working on kwangmyong, North Korea’s national intranet, centralizing connections between government departments and agencies, academic institutions, and research centres, while simultaneously setting the stage for the Kim regime to increasingly control the country’s information domain.

---

299 Ibid.
While these key developments shed light on when and how North Korea laid the groundwork for their current cyber capabilities, it is important to note that unlike China and Russia, North Korea and the KPA does not publish official military or other strategic doctrines. Therefore, knowledge about the country’s cyber doctrine must be pieced together and inferred using open-source media, academic journals, the limited defector testimony that is available, and by analyzing North Korea’s history of cyber operations. Yet, with the little we know about the strategic motivations behind North Korea’s cyber behavior, experts and observers typically suggest the regime’s utilization of cyberspace has been driven by two main things over the last thirty years.

First, and as I have already discussed, since the 1980s the regime has known that winning a conventional war on the Korean peninsula has become unrealistic, and that the military balance between the North and South had shifted in favour of the latter – especially given the South’s growing alliance with the U.S. and other Western nations.302 From this perspective, cyberspace enables North Korea to asymmetrically punch above its weight in terms of conflict, but it also serves as a tool the regime has used to fund and bolster the country’s nuclear program – something experts suggest the regime views as a vital strategic deterrent given the country’s inferior military capabilities. As Post (2021) explains, “Kim consistently expresses concerns about regime survival and fear of a U.S. attack, and recent U.S. regime change operations in other states only strengthen this fear.”303 Moreover, according to Post, “Kim continues to build and enhance his nuclear weapons capability in reaction to real and proximate threats to his very

survival. The United States frequently conducts exercises with South Korea and Japan, and North Korea frequently decries these exercises as hostile and reckless. Kim sees these exercises as practice events for an eventual attack on North Korea.”

Given this dynamic, the Kim regime relies heavily on financially motivated cyber attacks to ensure its nuclear arsenal is well funded.

Second, but less commonly discussed throughout the literature, is the fact that the Kim dynasty, starting with Kim Il Sung, through to Kim Jong Il, and now Kim Jong Un – have officially emphasized the importance of science and technology for the country’s survival under its unique ideology, Juche. Juche, meaning “self-reliance,” is the official state ideology of North Korea, and is often described by the government as Kim Il Sung’s “original, brilliant and revolutionary contribution to national and international thought.” Its guiding principles include things such as, “man is the master of his destiny,” that the North Korean masses are to act as the “masters of the revolution and construction,” and that by becoming self-reliant and powerful, a nation can achieve true socialism. Further, three articles from country’s Constitution suggest that science and technology are crucial for the nation’s socialist economic activities and security. Indeed, as Park (2019) notes, “since the establishment of the North Korean state, [the Kim family] has pursued advancement in science and technology to achieve its ultimate goal: regime survival.”

Even more important to this research is the critical role juche plays in regime legitimation. To echo Beauchamp (2018) “North Korea’s repressive government survives in no

304 Ibid.
small part because it has convinced its people of the legitimacy of its government. As hard as it may be for Americans to grasp, millions of North Koreans appear to truly believe their government’s pronouncements. And the tool the state has used to convince of them of these ideas is a unique official philosophy called juche.”

That being said, and as I argue throughout this chapter, and as the empirical record of the country’s cyber attacks illustrate, cyberspace has proven to be a valuable tool the Kim family has used to drive home and deliver on the foundational elements of the country’s juche philosophy as a means of regime legitimation. From projecting power globally, fueling the perception of confronting foreign threats, creating nationalism, elevating the Kim family to God-like status, and importantly, generating mass amounts of money, cyberspace has become – as Kim Jong Un has himself stated – “an all purpose sword.”

In sum, despite a lack of official documentation, North Korea has clearly invested in cyber capabilities and established critical cyber infrastructure to support important state objectives. Specifically, the regime has used cyberspace as a tool to address its conventional military weaknesses, while also using the digital realm to deliver on integral elements of the country’s juche philosophy. These have been the primary drivers of North Korea’s growth as a powerful threat actor in cyberspace. As I have done in previous chapters, the following section will analyze North Korea’s record of cyber attacks, with emphasis on its most noteworthy operations. The intent here is to illustrate how the country has used cyberspace to achieve certain strategic objectives in support of regime survival and legitimacy. More specifically, in the

---

following section, it will become clearer how crucial acquiring financial resources has been to the regime, and how making money has been a key driver of the country’s cyber strategy. In the third and final section of this chapter, I will bridge the gap between North Korea’s empirical record of cyber attacks and key theories from the literature on how personalist autocracies legitimize their rule.

5.3 KIM JONG-UN, ELITE LOYALTY, AND THE MAKING OF A MAFIA STATE: AN ANALYSIS OF NORTH KOREA’S CYBER ATTACKS

Despite North Korea having laid the groundwork for its current cyber capabilities and operations over thirty years ago, publicly available data on the country’s record of cyber attacks suggest Pyongyang did not carry out its first significant cyber operation until 2009, making it a late bloomer in comparison to China and Russia. However, over the course of the last decade, North Korea has rapidly improved its cyber capabilities, undertaking a range of networked operations that have steadily evolved throughout the years. From DDoS and website defacement attacks, to espionage operations, to financially motivated campaigns, Pyongyang has – like the other countries analyzed in this research – used cyberspace to deter foreign aggression, coerce its adversaries, and project power at home and abroad without inviting a conventional response, among other things. However, just as observers were initially skeptical and dismissive of the country’s nuclear program, North Korea’s cyber strategy is sometimes viewed as chaotic or irrational.311 Nevertheless, I argue that the country’s behaviour in cyberspace, particularly its unique emphasis on financially motivated cyber intrusions, paints a clear picture that aligns with

and supports theories on personalist authoritarian legitimation and my own needs-based theory on authoritarian legitimation in cyberspace.

In short, and most importantly, North Korea’s cyber attacks suggest the country has relied on cyberspace as an economic lifeline, enabling the regime to evade the full effect of international sanctions and fund government priorities, including its missile and nuclear programs. In addition, the country’s use of cyberspace to acquire money has allowed the regime to continue operating in near total isolation from the rest of the world, maintain the perception the regime is not beholden to foreign powers, perpetuate and fuel nationalistic ideals, and create an environment characterized by total fealty to the ruler – all of which are key to the legitimacy of the regime. Moreover, and again, something we see in the literature on personalist autocratic legitimation strategies, Byman and Lind (2010) point out that North Korea has co-opted an “elite selectorate” in order to prevent coups and ensure key persons, particularly those within the security establishment, remain loyal.\footnote{Daniel Byman and Jennifer Lind, “Pyongyang’s Survival Strategy: Tools of Authoritarian Control in North Korea.” International Security, Vol. 35 (1), Summer, 2010.} As North Korean defector Kang Mi-jin has said, North Korea’s financial hackers consider what they are doing to be “directly related to the fate of the Kim regime.”\footnote{Jon Herskovitz and Jeong-Ho Lee, “A Growing Army of Hackers Help Keep Kim Jong Un in Power.” Bloomberg, December 21, 2021.} In order to illustrate the importance of financially motivated cyber attacks to the Kim regime, and to more clearly connect North Korea’s cyber attacks to my theory, additional analysis on the country’s record of cyber operations is required. I begin this analysis with an overview of some of the country’s earliest known cyber operations, which typically took the form of denying service, website defacement, or damaging organizations and digital infrastructure in South Korea and the U.S. From here, I analyze North Korea’s surge in
financially motivated cyber attacks, illustrating how the country has prioritized these attacks as a means of making money.

Several works point to North Korea’s July 2009 DDoS attack as the first instance of the regime using cyberspace to inflict harm on its adversaries. This campaign, known as the “4th of July attack,” targeted the South Korean Presidential Office, the Ministry of National Defense, and the National Assembly, as well as U.S. offices and institutions including the White House, the Pentagon, the office of the Secret Service, the Treasury Department, and the Washington Post, among many others. While sources such as the *New York Times* described North Korea’s military infrastructure (presumably including its digital infrastructure) as “decrepit” and U.S. officials and computer experts characterized the attacks as “unsophisticated,” and “elementary,” this attack was a harbinger of Pyongyang’s future cyber attacks.\(^\text{314}\) Indeed, less than two years later in March 2011, North Korea launched another DDoS campaign known as the “Ten Days of Rain” attack. Again, South Korea’s Presidential Office, the Foreign Ministry, the National Intelligence Service, and several large South Korean financial institutions as well as U.S. Forces Korea were hit with malware, rendering their websites and networks inoperable. All told, up to 40 websites and 11,000 users were infected.\(^\text{315}\) A 2011 McAfee analysis of the attack found that “several steps were taken to ensure that the mission was executed without interruption, within the predefined attack window – and following, ensuring that all vehicles of attack would be destroyed, thus limiting forensic analysis.”\(^\text{316}\) It was clear North Korea’s abilities were quickly improving. That same year, North Korean hackers attacked South Korea’s Nonghyup Bank,


destroying 273 of the bank’s 587 servers, causing them to crash, and disrupting the abilities of 30 million customers of Nonghyup to access their accounts for several days.\textsuperscript{317} Kim Youngdae, a South Korean prosecutor working on the case, described the attack as “an unprecedented act of cyberterror.”\textsuperscript{318} Two years later, on March 20, 2013, North Korea carried out its “Dark Seoul” attack, hitting the country’s financial sector again, as well as South Korea’s two largest broadcasters – knocking key financial and media websites offline for days, and in some cases, weeks.\textsuperscript{319} Three months later, on the 63\textsuperscript{rd} anniversary of the outbreak of the Korean War, which began on June 25, 1950, the website of South Korea’s Presidential Office, and several official media sites were hit with another DDoS attack, knocking key government websites offline. In addition, North Korea also exfiltrated sensitive files containing personal data on U.S. and South Korean military personnel, including those from the U.S. Army’s 3\textsuperscript{rd} Marine Division, 25\textsuperscript{th} Infantry Division, and 1st Cavalry Division.\textsuperscript{320} Following the attack, a South Korean official said the intrusion undermined the country’s image by attacking “symbolic” government websites.\textsuperscript{321}

In addition to these DDoS attacks, North Korea has also undertaken a range of espionage operations in cyberspace designed to acquire information on South Korea’s strategies in a range


\textsuperscript{318} Ibid.


\textsuperscript{320} Martyn Williams, “Hackers attack North, South Korean websites.” North Korea Tech, June 25\textsuperscript{th}, 2013: https://www.northkoreatech.org/2013/06/25/hackers-attack-north-south-korean-websites/

of domains, as well as their military capabilities. Named “Kimsuky,” North Korea’s first major espionage operation took place in September 2013. Targeting South Korean think tanks including the Sejong Institute, the Korea Institute for Defense Analyses, the Ministry of Reunification and the Hyundai Merchant Marine shipping company, the operation was described by some as “extraordinary in its execution.” Using a complex mix of malware distributed into network systems using spear-phishing emails, the hackers stole important credentials from their targets, including account passwords and security details, enabling them to access highlight sensitive information relevant to the North Korean regime. Then, in 2014, South Korea’s nuclear power plant operator Korea Hydro and Nuclear Power (KHNP) had their networks hacked, where intruders stole documents containing reactor designs and manuals, as well as the credentials of 10,000 KHNP employees – some of the stolen information was even posted online, with hackers demanding money to keep the remaining documents private. In 2016, another significant intrusion took place, where North Korean hackers targeted the U.S. - South Korean Combined Forces Command, South Korean Joint Chiefs of Staff, and the Defense Integrated Data Center. Infecting over 3,000 computers, the hackers were able to steal 235 gigabytes of classified information. Crucially, they also gained access to the U.S.- South Korean combined Operations Plan 5015 (OPLAN 5015) which detailed a response strategy to a North Korean invasion of the South, as well as plans to “decapitate” Kim Jong Un during wartime. A 2017 article in the New York Times also stated the hackers obtained “reports on key South Korean and

U.S. military personnel, the minutes of meetings about South Korean-U.S. military drills and data on military installations and power plants in South Korea.”325 North Korean hackers also accessed computers of Daewoo Shipbuilding & Marine Engineering Company, stealing classified blueprints for South Korean warships, as well as information on the country’s 3,000-ton submarine, and its ballistic missile and vertical launch systems.326 The North Korean hacking group known as Kimsuky has also undertaken multi-year campaigns to obtain information on sanctions and nuclear security experts, retired South Korean officials, several academic institutions, and other persons and organizations with a nexus to North Korea and the Kim regime.327 That being said, and in light of disruption and espionage attacks remaining part of North Korea’s strategic cyber toolkit, the country’s main focus in cyberspace has been generating money for the Kim regime – something I argue we should expect to see given the importance financial resources have to personalist autocracies.

While North Korea’s cyber activities have had a financial element to them for many years, there has been a surge in financially motivated cyber attacks since about 2017. Indeed, as John Demers, head of the National Security Division of the U.S. Department of Justice has said, North Korean hackers “have become the world’s leading bank robbers.”328 While dollar figures vary from source to source, experts suggest Pyongyang has been able to generate billions of dollars from their illicit cyber activities. For example, in August 2019, the U.N. Panel of Experts

327 Klingner, 2021.
estimated the regime had made $2 billion from their cyber crimes. Others suggest however, that North Korea is able to generate anywhere from $860 million to $1 billion each year from its malicious cyber activities. Remarkably, a study conducted by cybercrime company Group-IB found that North Korea could be responsible for upwards of 65 percent of all online global cryptocurrency theft. Rapidly improving the scale and level of sophistication of its financially motivated cyber attacks, North Korea has undertaken intricate online bank heists and hacking operations, they have stolen funds through fraudulent bank transfers and Society for Worldwide Interbank Financial Telecommunications (SWIFT) transactions and complex ATM cash-outs, as well as largescale ransomware attacks where hackers have demanded payment in cryptocurrency.

That said, the first North Korean cyber attack that signalled the regime’s intensified interest in making money was the 2016 heist of the Bangladesh Central Bank. On February 4, 2016, North Korean hackers used SWIFT credentials of Bangladesh Central Bank employees to send nearly 40 fraudulent money transfer requests to the Federal Reserve Bank of New York asking the Reserve to transfer millions of the Bangladesh Bank’s funds to accounts in Southeast Asia. Managing to get $81 million sent to Rizal Commercial Banking Corporation in the Philippines through four separate transfer requests, as well as an additional $20 million sent to Pan Asia Banking, the hackers walked off with tens of millions of dollars. However, if it had not been for a typo (“foundation” vs “fandation”), well-trained bank employees, and a faulty printer,

which caught the attention of bank employees, the hackers could have drained accounts worth nearly a $1 billion.\footnote{BBC, “The Lazarus heist: How North Korea almost pulled off a billion-dollar hack.” BBC News, June 21, 2021: \url{https://www.bbc.com/news/stories-57520169}} Then, a year later in 2017, the North Korean sponsored hacker group known as Lazarus carried out the largest cryptocurrency theft in history in what has come to be known as the “WannaCry” campaign. Exploiting a vulnerability in old Windows software and using it to freeze and prevent access to files, hackers hit over 300,000 computers in 150 countries worldwide, where they demanded between $300-$600 million in Bitcoin.\footnote{Zeeshan Aleem, “The WannaCry hack shows North Korea’s emergence as a cyber powerhouse.” VOX, December 19, 2017: \url{https://www.vox.com/world/2017/12/19/16794970/wannacry-north-korea-bosser-cyberattacks}} During the WannaCry attack, critical infrastructure in several countries was disrupted, with over a dozen hospitals in the U.K. alone forced to shut down a range of operations including non-urgent procedures.\footnote{Russell Brandom, “UK hospitals hit with massive ransomware attack.” The Verge, May 12, 2017: \url{https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin}} However, as Wilner et al. (2019) suggest, there was a social dynamic to this attack too, wherein North Korea sought to disrupt and embarrass its adversaries. Indeed, the attack generated little money for the regime, with “only 0.07 percent of WannaCry victims” having paid the ransom.\footnote{Alex S. Wilner, Anna Jeffery, Jacqueline Llor, Kathleen Matthews, Krystene Robinson, Alexandra Rosolska, and Catherine Yorgoro, “On the social science of ransomware: Technology, security, and society.” Comparative Strategy, Vol. 28, No.4, 347–370, 2019.}

That same year, North Korean hackers stole tens of millions of dollars from ATMs in Africa and Asia where fraudulent ATM withdrawals were carried out simultaneously in dozens of countries.\footnote{Matthew Pennington, “NKorea said to have stolen a fortune in online bank heists.” Associated Press, October 3, 2018: \url{https://nationalpost.com/pmn/news-pmn/nkorea-said-to-have-stolen-a-fortune-in-online-bank-heists/wcm/ff41750b-ece3-4e2a-b04c-7ca34d18c537/}} These seemingly basic attacks continued to yield high returns for the regime over the next number of years, with India’s Cosmos Bank falling victim to a heist of over $13 million
in 2018, which was carried out by “money mules” who made over 14,000 withdrawal transactions using cloned ATM cards in over two dozen countries.\textsuperscript{337} As Buchanan (2020) explains “hackers gain access to the credentials of a bank’s customer, and then a money mule shows up to an ATM and withdraws money from that account. With no bank teller to talk to or physical branch to enter, the chance of arrest is substantially lower.”\textsuperscript{338} Later that same year, North Korean hackers stole tens of millions of dollars from the Mexican bank Bancomext by gaining access to insufficiently protected networks and employee credentials, while circumventing lacking validation checks.\textsuperscript{339} South Korean cryptocurrency exchanges were also infiltrated in 2018, with North Korean hackers making off with nearly $40 million in virtual coins stolen from Coinrail, as well as another $30 million stolen from Bithumb.\textsuperscript{340} North Korean hackers have also carried out largescale hacks of cryptocurrency exchanges in Slovenia, Indonesia, Japan, the U.S., and elsewhere. In 2020, a United Nations (U.N.) report found that from 2019 to November 2020, North Korean hackers had stolen approximately $316.4 million in crypto assets to support the Kim regime.\textsuperscript{341} Yet, while the totality of North Korea’s cybercrime remains unknown, the U.N. and U.S. government have suggested the regime has raked in over

$2.3 billion through cyber attacks.\textsuperscript{342} Dozens of other publicly known attacks support this figure, and the fact Kim is now disproportionately focused on having his cyber army carry out operations that make him money, fund what Berlinger and Cohen (2017) refer to as his “personal piggy bank,” and keep his inner circle of influential elites happy and in line.\textsuperscript{343} Indeed, Dr. Sheena Greitens with the University of Texas at Austin has said that money North Korea illicitly obtains is “income that goes directly into the pockets or the bank accounts of the North Korean leadership,” while other analysts have reiterated my suggestion that Kim relies on money as a means of funding the lavish lifestyles of the country’s elite.\textsuperscript{344}

Worth noting is that the Kim regime has long depended on illicit activities as a means of generating money for the regime – activities that go far beyond cyberspace. I raise this because it speaks to the underlying hypotheses found in the literature that personalist regimes heavily depend on access to money to legitimize themselves and to stave off regime collapse. It also supports my needs-based theory on authoritarian legitimation in cyberspace in the sense that I argue authoritarian regimes primarily rely on cyber attacks to achieve whatever it is they need most to convince their people of their ‘right to rule’ and to protect themselves from threats to regime survival. In the case of North Korea, earlier criminal efforts to acquire money for the regime have included sophisticated counterfeit currency campaigns, which U.S. officials believe, have brought in tens of millions of dollars per year for Kim, as well as the largescale production and export of drugs like methamphetamine and opium.\textsuperscript{345} The regime has also produced and sold

\begin{itemize}
\item \textsuperscript{342} Herskovitz and Lee, 2021.
\item \textsuperscript{344} Berlinger and Cohen, 2017.
\item \textsuperscript{345} Tara-Francis Chan, “A $100 counterfeit 'supernote' found in South Korea could have been made in North Korea.” Business Insider, December 13, 2017: https://www.businessinsider.com/counterfeit-supernote-found-in-south-korea-2017-12; Greg Walters, “North Korea’s Counterfeit Benjamins Have Vanished.” VICE, March 16, 2016: https://www.vice.com/en/article/vb8pk9/north-koreas-counterfeit-benjamins-havevanished; Mike Ives, “Crystal
mass quantities of cigarettes, trafficked endangered species products, and undertaken insurance fraud schemes. In recent years though, cyberspace has proven to be the most efficient and most lucrative tool the Kim regime has used to generate money, convince North Korean elites Kim Jong-II is a reliable source of income, and to prove to the broader population he has been able to deliver on economic self-sufficiency – a key pillar of juche. In this next and final section, I provide further analysis on how the information throughout this chapter on North Korea’s cyber attacks and behavior in the digital realm align with some of the key theories on autocratic legitimation, with specific emphasis on personalist dictatorships. Overall, it should become clearer how the examples I have used from the empirical record support my needs-based theory on autocratic legitimation in the cyber domain.

North Korean cyber attacks and regime legitimation

According to existing literature, personalist autocracies depend heavily on economic performance and the acquisition and distribution of financial resources as a means of both regime legitimation, but also regime survival. This is not to suggest that personalist autocracies do not rely on a combination of legitimation strategies, or that they are not sensitive to a range of factors that could threaten the longevity of their regimes, but rather, relative to other regime types, they appear particularly vulnerable if access to money and material resources is scarce. To reiterate, as Tannenberg et al. (2020) suggest “personalistic regimes, because their rule relies upon the


neopatrimonial distribution of resources, delivering the goods to key constituencies is seen as a kind of performance on the basis of which legitimacy claims can be made.”\textsuperscript{347} Several other authors on autocratic regime legitimation argue this as well, including Geddes (1999) whose work has been foundational for a sizeable portion of all literature on this topic, and Kailitz (2013) who found that “as soon as the personalist autocrat cannot provide enough “booty” to his personal gang, they will start to look for an alternative.”\textsuperscript{348} Others, like Gerschewski (2018) expand on this idea in saying that “cronies remain loyal and do not revolt against the regime as long as they can be bought off via policy concessions, material spoils, or other revenues—or at least as long as the assurance that they benefit from the current regime is credible.”\textsuperscript{349}

Moreover, several works specifically explore North Korea, and how the Kim dynasty has continually convinced North Korea’s elite of their legitimacy and ‘right to rule’ through the provision of monetary and material assets. This further reinforces theories on personalist authoritarian legitimation strategies. For instance, Jina (2013) writes that in North Korea, “private goods are provided to the power elites in the form of state-granted monopolies and access to hard currency and bribes, legitimizing their pursuit of rent-seeking behaviors.”\textsuperscript{350} Likewise, Byman and Lind (2010) note that in North Korea “the health of the overall economy is less important than the regime’s ability to bribe elite supporters. The North Korean selectorate can be conceptualized as a key group of elites—somewhere between 200 and 5,000 people, depending on how wide the circle is drawn—that includes military leaders, party officials and bureaucrats.”\textsuperscript{351} Martin (2004) speaks to this dynamic as well, saying the Kim regime also

\textsuperscript{348} Geddes, 1999; Kailitz, 2013.
\textsuperscript{349} Gerschewski, 2018.
\textsuperscript{351} Byman and Lind, 2010.
bestows extravagant (by North Korean standards) gifts on the members of the selectorate, including luxury cars, high-end watches, stereo systems, and other electronics. Further, certain elites are rewarded with wives with sizeable pensions who have been given the opportunity to retire in their twenties from the “Happy Corps”: a group of attractive young women who serve Kim (Jong Il) as assistants and entertainers. Indeed, even during the great famine, Kim Il-song used North Korea’s class system to divert hardship away from his selectorate, and onto potential political opponents or lower classes of people in the country.  

Haggard and Nolan (2009) discuss this legitimation strategy as well, pointing out that the country’s highest and most strategically important classes – rewarded with homes in Pyongyang – were protected during the famine, with urban residents receiving the largest and highest quality food rations, sometimes double what poorer, rural, and strategically less important classes might receive from the regime. 

With this resource-based theory on personalist dictatorships in mind, I have suggested that we should expect to see these same strategies play out in the cyber domain. In other words, and using North Korea as a case study, the expectation is that personalist autocracies will find ways to acquire money to line the pockets of elites, maintain their reputation as a reliable source of money for those who matter most to regime survival, and for the broader population, appear as a sort of divine provider. In the case of North Korea, these theories appear to hold true, with the regime clearly prioritizing financially motivated cyber attacks. Interestingly, while North Korea’s behaviour in cyberspace appears consistent with the aforementioned theories on

personalist dictatorships and money, the North Korean government has less explicitly used
cyberattacks a way to bolster and preserve the image of its rulers - the exception being the
infamous Sony hack from 2014, which I briefly discuss below. That said, several of the country’s
early cyberattacks were designed to influence public perception and discourse in South Korea
and other nations abroad. By attacking critical infrastructure in rival nations, such as financial
institutions, telecommunications and media networks, transportation systems, and nuclear plants,
the Kim regime sought to cause social unrest and disorder in countries abroad – particularly in
South Korea – while also signalling the power and sophistication of Kim Jong-Il as a legitimate
leader to its adversaries.

Further, rather than controlling certain narratives about the Kim family online, and
targeting individuals or organizations that speak out against the regime in cyberspace, the North
Korean government has effectively ensured there is no online space or digital communication.
As Boynton (2011) notes, North Korea “… remains a stubborn holdout, a regime almost totally
in control of its national narrative.”354 With the exception of a small cadre of elites who can
access portions of the internet, absolutely zero freedom of the press, no access to outside media,
and no flow of external information into the country, the Kim regime has had to worry less about
their legitimacy being questioned online than countries like China or Russia. Fisher (2015) has
said, “If you went to North Korea and asked people about the internet, most of them would
probably have no idea what you were talking about.”355 Yet, for the handful of people who can
access North Korea’s state-run intranet known as “Kwangmyong” – the regime ensures

354 Robert S. Boynton, “North Korea’s Digital Underground.” The Atlantic, April, 2011:
355 Max Fisher, “Yes, North Korea has the internet. Here’s what it looks like.” VOX, March 19, 2015:
government propaganda is front and centre, with messages extolling the greatness of Kim, while stressing the evils of their foes, particularly the U.S. Likewise, in recent years, North Korea has increasingly focused on spreading propaganda abroad through online platforms like YouTube. While I do not consider these actions to be cyberattacks, the regime is clearly looking to influence the information environment by disseminating low-cost narratives about the country, and the merits of the Kim regime. As Sang-Hun (2021) notes, this new online content, designed for a global audience, aims to spread a simple message: “North Koreans, they’re just like everyone else. They play sports in their free time. They scream on roller coasters. They shop in malls and eat pizza.” Videos in support of this new modernized propaganda effort show children dancing and singing about their “dear General” (Kim), while the country’s Propaganda and Agitation Department work to “shore up the personality cult surrounding Mr. Kim.” From this perspective, Kim’s strategies in cyberspace do align with what we would expect to see from a personalist leader, but his tactics in this regard tend to be more offensive and concerned with pre-emptively shaping his image as opposed to responding in a reactionary way to attacks or criticisms his regime faces from individuals or organizations abroad. Ultimately, and as I stated in Chapter 1, while I cannot say definitively at this point that there is a direct correspondence between the behaviour of personalist dictatorships in cyberspace and the literature on authoritarian legitimation, I have illustrated new and novel correlations that warrant further examination, and which provide a first of its kind starting point for additional analysis on authoritarian behaviour in cyberspace.

---


357
First, the Kim regime has continued its long tradition of illicit criminal activities in cyberspace as a way of making money – something we do not see other countries like China and Russia doing, at least not nearly to the same extent. While the majority of observers and scholars writing about North Korea suggest this strategy is a way for the regime to fuel the country’s ballistic missile and nuclear weapons program, and to circumvent largescale international sanctions, I argue that the regime is pursuing criminal cyber activities for something more foundational: as a way to maintain status as a reliable and legitimate material provider to regime elites and the country’s highest class of people. For this research, I interviewed former Chief of the Central Intelligence Agency’s (CIA) Korea Branch, Bruce Klinger, whose insight supported my theory. Klinger told me “in North Korea, Kim is like the “Capo dei capi” – your welfare, your status, and your social power come from your loyalty and proximity to him, and in turn, your loyalty helps ensure regime survival. It is like Al Capone making money – it all goes into the hopper, and whether some of it is going towards machine guns or food is irrelevant. It all frees up resources that would otherwise have to go to the general population.” In addition, I also suggest that Kim Jong-un, in keeping with his grandfather’s ideology of juche – which roughly translates to “self reliance,” uses cyberspace to preserve one of the ideology’s key pillars: economic self-sufficiency. Jakhar (2020) echoes this in saying “Instead of seeking outside help or pursing economic liberalization to deal with the triple whammy of international sanctions, extreme weather and covid-19 border closures, [Kim Jong-un] has put the focus back on Juche.” By doing this, Kim Jong-un is able to maintain his veneer as the legitimate, chosen leader of the North Korean people and unifier of the Korean Peninsula. As Don Baker, Korea

---

358 Bruce Klinger was interviewed virtually for this dissertation on January 10, 2022.
scholar at the University of British Columbia has said, “Human beings [in North Korea] don’t need God. They now have the Kim family.”

Again, this connects to existing theories on personalist dictatorships and how, in part, they seek to legitimate themselves. Ultimately, what I have described here in this chapter, generating material wealth is best described in the literature as a type of performance legitimation strategy. To remind, legitimacy through performance and performance-related narratives refers to the abilities (real or perceived) of government in satisfying citizens’ needs. In this sense, a regime will either specifically highlight its achievements in fulfilling the demands of the population which, could include such things as material welfare and security from internal and extern threats or, alternately, it will rely on claims of achievements in the absence of any real and/or meaningful improvements. Rothstein (2009) explains this clearly by saying ‘legitimacy is created, maintained, and destroyed not by the input but by the output side of the political system.’ Von Soest and Grauvogel (2017) also find that ‘closed authoritarian regimes’ – which includes North Korea – rely especially heavily on output and performance – based claims to legitimacy, including their ability to provide material welfare and security. What I argue is that North Korea’s cyber attacks do indeed support these theories. The Kim regime continually uses the cyber domain to acquire money and perpetuate the idea he is a high performing guarantor of material goods and assets. Kim also uses this money to fuel his weapons programs as a way of signalling his prioritization of state security. In support of this chapter on North Korea, I interviewed Scott Snyder, Senior Fellow for Korea studies and Director of the program on U.S.-

---

360 Beauchamp, 2018.
363 Von Soest and Grauogel, 2017.
Korea policy at the Council on Foreign Relations. Snyder told me that the traditional form of reward for elites in North Korea has been bribery or rewards. However, since the 1990's as a result of extreme economic pressures, the leadership also began to require elites to go out and earn foreign money for the regime, which became a method of social and political advancement. Snyder told me that in terms of cyberspace “it is just another vehicle through which the regime can provide opportunities for upwardly mobile people.”

Snyder raised another point that contributed to my understanding of North Korea and which connects to theories on personalist autocracies and regime legitimation. Over the last several years, there has actually been a transition from complete totalitarianism in North Korea to an authoritarian regime with elements of performance-based legitimacy and incentives. However, in keeping with the idea of self-reliance and independence which I discussed earlier in this chapter, much of that performance is self-driven and self-realized by cyber criminals who act on behalf of the state. In other words, you have Kim who maintains the image of a material provider to his people (particularly those who matter most to him), but you also have cyber criminals who act on behalf of Kim, and who are incentivized to also perform as a way of improving their quality of life through loyalty and service to the regime.

Finally, as noted earlier in this chapter, North Korea does look to bolster the image of Kim online, but in a way that is slightly different from other autocracies like China and Russia. While personalist dictators like Chairman Xi and President Putin aggressively seek-out and punish individuals and organizations abroad who question the legitimacy and authority of their regimes, Kim – because the people of North Korea typically cannot access outside information – tends to disseminate pro-regime messaging online to convince outsiders of his credibility and

---

364 Scott Snyder was interviewed for this research virtually on January 14, 2022.
greatness. In other words, I suggest that more open authoritarian regimes will pursue more aggressive international cyberattacks to limit any dissent at home, whereas entirely closed regimes like North Korea are far less sensitive to destabilizing online content, and as a result, use digital tools to spread propaganda as opposed to punish opponents. That said, in November 2014, North Korea did carry out a cyber operation against Sony because of the company’s comedic movie “The Interview,” which depicted an assassination attempt against Kim. Pyongyang said the release of the film would be an “act of war.” In the end, and after hackers had destroyed the data of Sony Pictures Entertainment, released highly confidential and embarrassing company information, including salary lists, tens of thousands of Social Security numbers, and several unreleased films online, the company gave in, and cancelled the release of the film. Aside from this attack though, there is little data or publicly available information on North Korean cyber operations designed to attack or delegitimize dissidents or critics of Kim. Again, this is likely because the regime is much more insulated and technologically unplugged than most other nations in the world – including other authoritarian regimes. In fact, unlike countries like China and Russia where the Internet is highly controlled but still accessible to the masses, the Internet is largely prohibited in North Korea.

To conclude, for the North Korean government, cyberspace has become an invaluable tool that can and has been used for regime legitimation. Since taking power after the death of his father in 2011, Kim Jong-un has increasingly turned to his cyber army to advance his goals, including enriching his legitimacy, maintaining regional and global relevance, and most importantly, staving off any threats to the security of his kingship. As I have argued throughout this chapter, money has been the primary driver of Kim’s successes in achieving these goals. By connecting North Korea’s empirical record of cyber attacks with theories on how personalist
autocracies legitimize themselves and maintain the resiliency of their regimes, I have shed new light on how certain types of regimes may be expected to behave in the digital realm. However, similar to other chapters in this dissertation, this case study on North Korea and personalist dictatorships is only a first step in connecting these areas of study, and on linking the empirical with the theoretical. Additional analysis will be required to better understand such things as the relationship between access to financial resources and the legitimation strategies of personalist rulers, as well as why North Korea behaves the way it does in cyberspace. Having completed three case studies of three different regime types (two of which show some within-case variation) and how each regime varies in their use of cyberattacks, the next section will provide a more concise illustrative chapter where I will explore my null hypothesis and why military autocracies do not appear to use cyberspace to legitimize their rule.
CHAPTER SIX

GOITA, GUNS, AND GOVERNANCE: AN ANALYSIS OF MALI, COUPS, AND WHY MILITARY REGIMES DO NOT CARRY OUT CYBER ATTACKS

6.1 INTRODUCTION

In less than a decade, Mali, a landlocked country in West Africa, has endured three military coups – one in 2012, another in 2020, and the latest in 2021. Each scenario saw largescale civil unrest, violence, and even death. However, at no time did the country’s military leaders use cyberattacks to consolidate their power, ensure regime survival, or legitimize their rule. This finding, while puzzling, aligns with key theories on how military autocracies seek to legitimize themselves. Moreover, and based on these theories, the null hypothesis I raised earlier in this dissertation is also supported: if a regime does not face any significant threats in terms of its survival, or in terms of threats to the legitimacy of the regime, it will not engage in any significant cyber attacks. In this chapter, and using Mali as a case study, I will explore how military autocracies legitimize themselves, how they differ from the other regime types analyzed in this research, and why they appear less interested in using cyberspace for key strategic purposes. After analyzing several existing military autocracies, Mali was chosen given the fact it has experienced three distinct military coups throughout the last decade – a period where there has been a proliferation of cyber attacks and capabilities globally. In other words, because Mali has experienced so much volatility, and so many military regimes in such a short timeframe, I hoped there would be greater variation and data to work with. To note, while there are a handful of other military regimes I could have analyzed, like those in Thailand or Myanmar, they too are relatively new military governments, or countries that have experienced repeated coups in recent years. Indeed, as Jonathan Powell, Associate Professor at the University of Central Florida has
said, “When a country has one coup, that's often a harbinger of more coups.” Ultimately, to the best of my knowledge, other potential military regimes I could have studied have characteristics similar to Mali – particularly when it comes to the length and/or stability of their rule. As a final point, I also knew the study of cyber conflict and malicious cyber activities in Africa is a burgeoning subfield. Therefore, I believed I would find more material, and have greater access to those studying military regimes and cyber conflict in Africa, than in other regions.

Ultimately, and in keeping with seminal and widely agreed on theories from the literature, I argue that military autocracies are less interested in maintaining power and preserving their authority over the long-term, at least relative to other regime types. As a result, the benefits cyberspace and cyberattacks yield for other autocratic regime types are not as useful or appealing. Moreover, and complementary to this suggestion, military autocracies typically seek to legitimize themselves domestically by restoring order and increasing physical security – two performance based legitimacy claims that are achievable using traditional military power and authority in physical, rather than cyber, space.

The following chapter on Mali, military dictatorships, and regime legitimation – which is more illustrative and concise than previous chapters – is broken into several sections. The first provides some detail on what exactly a military autocracy is, how it is defined, and an overview of what the literature says in terms of how they look to convince populations of their right to rule. The second section provides an overview of how Mali’s military leaders have sought to legitimize themselves, and how their actions in the real world align with theories in the literature.

---

Finally, the third section of this chapter expands on how these theories, and the case of Mali, support my own needs-based theory on authoritarian legitimation in cyberspace.

6.2 BACKGROUND: MILITARY AUTOCRACIES, REGIME SURVIVAL, AND LEGITIMATION

As noted earlier in this dissertation, military autocracies are one of the foundational, commonly studied regime types throughout the literature on dictatorships and regime legitimation. Given the prevalence of military dictatorships throughout Africa, Latin America, the Middle East, and elsewhere over the last several decades, there is no shortage of material on juntas and oppressive rule. However, to the best of my knowledge, no scholarly work has sought to explain the disconnect between military autocracies and cyberspace, or why this particular regime type has, for the most part, neglected to use the digital domain to preserve or strengthen their rule. That being said, there are several theories throughout the literature that help explain why this might be the case. Before getting into those theories though, some detail is needed on how I define or conceptualize military autocracies.

My understanding of a military autocracy is rooted in Geddes’ definition which suggests military autocracies are those which are led by a group of officers who choose who will rule and who exercises influence on policy. However, Kailitz (2013) cautions that while we might have a generalizable understanding or perception of what a military autocracy is, the reality is that “there is no common procedural justification of military regimes,” and that “there is not even a clear pattern of how the military as an institution selects and controls the rulers.” For these reasons, as Kailitz notes, defining and classifying military autocracies is more challenging than it is with

other regime types such as personalist or single-party autocracies. Regardless, there are a variety of key elements that differentiate military regimes from other types, and which assist in identifying and classifying military autocracies. First, to appear as a legitimate, rational-legal military regime and not one run or controlled by armed rebels or vigilantes, the military as an organization or institution has to select the ruler in one way or another, and the military must also have a say in politics and policies. Essentially, the country is, as Kailitz notes “either ruled by a junta of high-ranking military officers – in which civilian bureaucrats may play a role or not – or by a high-ranking military officer, who is selected by the military as the ruler.”

Other authors, such as Geddes (1999), Linz (2000), and Ezrow and Franz (2011) have made similar statements as well.

In addition, the rational-legal ethos which is typically found in the military as an institution is another defining characteristic of a military regime which guides and informs much of its decision making. This is not something we see with other regime types throughout the literature, or within this dissertation. Finally, and as I will detail further in the following theory-focused section, military regimes tend to argue or present themselves – along with the bureaucracy – as the only rational apolitical arbiter of order – another element that separates it from other regime types.

In terms of theories found in the literature that help differentiate military autocracies from other regime types, there are at least two that are unique to military regimes, and which feed into and support my own theory and null hypothesis. First, a common theory throughout the literature suggests that military autocracies are not interested in maintaining power over the long term, as much as they are with other things. These include maintaining the integrity of the military as an

368 Kailitz, 2013.
institution, and on implementing and preserving a sense of order and security – regardless of how draconian or oppressive that order or sense of security might appear to outsiders. Indeed, Geddes writes that there is “a consensus in the literature that most professional soldiers place a higher value on the survival and efficacy of the military itself than on anything else.”

Geddes also notes that many officers will only join or support a coup if “they believe that the military institution itself is threatened.” Likewise, Nordlinger (1977) also notes that typically, soldiers begrudgingly or unenthusiastically transition from a strictly military role to one that also plays a government function – “most of them would probably have much preferred to remain in the barracks if their objectives, particularly the defense or enhancement of the military’s corporate interests, could have been realized from that vantage point.”

It may be Geddes who describes this point most clearly though when she writes that “because most officers value the unity and capacity of the military institution more than they value holding office, military regimes cling less tightly to power than do other kinds of authoritarianism and, in fact, often initiate transitions.”

In a similar vein, Kailitz and Stockemer (2015) write that military regimes “always lacks legitimacy to rule in the long run because the military is simply not designed to govern a country permanently.” Further, because military elites know and recognize this reality, they will usually act accordingly, and work to justify and legitimize only a temporary rule with a view to return governance back to civilians once the situation – whatever that may be – has improved. Indeed, unity among military elites is described as being more centered around returning power to civilian rule than anything else (e.g.

---

staying in power). This is unique amongst authoritarian regimes. Interestingly, Kailitz (2013) also points out that military elites are often concerned with and want to avoid the prospect of a civil war wherein soldiers are fighting soldiers, and in an attempt to avoid this, will often seek to return power to civilian authorities after a short time.

The second theory in the literature relevant to my own suggests military autocracies usually seek to legitimize themselves through a performance-based justification wherein their primary objective is to neutralize a threat to the country and restore order. I argue that because of this, and the fact that military autocracies do not typically look to remain in power over the long-term – at least relative to other regime types – external cyber attacks (and external physical attacks) have little to no utility. Tannenberg et al. (2020) discuss this, writing that “military regimes claim their right to rule or base their legitimacy on the need to restore order and physical security, which in turn becomes a sort of performance-based claim to legitimacy.”³⁷⁵ Similarly, Nordlinger (1977) and Perlmutter (1977) both note that military regimes usually justify their need to intervene and take over in domestic affairs as a means to restore political order, improve the economy, or and safeguard the nation.³⁷⁶ Others, such as Dukalskis and Gerschewski (2017) highlight this point as well: “the military’s right to rule is derived from being the guarantor of stability, order, and national interests.”³⁷⁷ In addition, other studies have shown that military autocracies are less conflict prone than other types of regimes (e.g. personalist autocracies). This is another finding that may support the aforementioned theories, and which also helps explain why military regimes do not appear to carry out cyber attacks. In the case of Mali, the two key theories I have discussed in this section

³⁷⁵ Tannenberg et al. (2020)
apply. In the following section, I offer a concise analysis of Mali’s military regimes since 2012 as a way of strengthening my null hypothesis and my broader needs-based theory on autocratic regime legitimation in cyberspace.

6.3 SOLDIERS IN THE PALACE: HOW MILITARY ELITES CONTINUE TO JUSTIFY COUPS AND CLAIM LEGITIMACY IN MALI

In 2012, on the heels of the Arab Spring, Mali – a tiny West African country often considered a beacon of democracy on the continent – experienced an unexpected military coup. For many observers, the 2012 coup – the country’s first since 1991 – was a downstream effect of Libyan leader Muammar al-Gaddafi’s death. With the downfall of Gaddafi following the NATO-led Libyan intervention, a disastrous regional insecurity vacuum developed, where nearby fragile states, unable to secure their borders, faced volatile situations fueled by the seepage of Libyan arms and rebels into their nations. What ensued was the proliferation of insurgency, extremism, and crime throughout many countries in the region – one of which was Mali. Indeed, as Time Magazine noted in 2013: “Within hours of Gaddafi’s death, many ethnic Tuareg fighters from northern Mali, who’d fought alongside Libyan forces as mercenaries, retreated across the Sahara, carrying as much weaponry as they could stuff into their pickup trucks. The patchwork of ethnic separatist groups and Islamist militias that seized Mali’s north this year cemented their control from the muzzles of these guns.” Well armed, these rebel militants began taking over large swaths of Mali, challenging the country’s military capabilities, and threatening to overrun the entire nation. It was the prospect of this threat, and an increasingly unstable domestic situation which officers from within Mali’s military based their coup.

Addressing the nation on state television after looting Mali’s Presidential Palace, arresting government Ministers, and declaring they had seized power, Mali’s new military government, led by junior officers and enlisted fighters claimed that change was needed in order to secure the country, and stave of a largescale, country-wide insurgency. In the eyes of the country’s 7,000 member military, President Amadou Touré was insufficiently challenging the rebels, he was not properly arming his military, and he was not demonstrating the leadership needed to safeguard the country. In a televised address, the junta – calling themselves the National Council for the Recovery of Democracy and the Restoration of the State – suggested the “incompetent regime” had shown an “incapacity to fight against the terrorists.”

According to the New York Times, the leader of the coup and Mali’s new head of government, Amadou Sanogo continually emphasized the deteriorating security situation in the country’s north, saying, “We should forget a little the Committee, the Parliament, the Constitution — that can wait. The serious topic, it’s the north. That’s the most important.” Further, and in line with theories detailed in the previous section, Sanogo also stated his plan of "holding a rapid process of normalisation, organizing free and transparent elections and a rapid restoration of the state.”

Ultimately, just over two weeks after taking power, and in response to crippling sanctions and border closures neighbouring countries had applied to Mali as a result of the coup, Sanogo agreed to cede power, returning the country to civilian control to interim President Dioncounda Traoré.

---

In August 2020, a similar event happened in Mali, with the country’s second coup in less than a decade. As was the case in 2012, the military once again overthrew the government – this time forcing President Ibrahim Boubacar Keita and his Ministers to resign. Unlike the situation in 2012, the 2020 coup was preceded by months of protests, where Malians voiced their opposition to the government's inability to counter the ongoing insurgency that had continued to plague the country, widespread government corruption, and a struggling economy. M5-RFP, a coalition of leaders from throughout Mali’s civil society, including religious figures and political opponents of Keita were a mobilizing force, uniting Malians in their demands for political accountability. After three months of unrest, a small group of senior officers in the military calling themselves the National Committee for the Salvation of the People (CNSP) arrested Keita, forcing him to step down on national television on August 18.382 Just as Sanogo had done in 2012, leaders of the new military regime signalled they had taken power to restore order in the country.

Speaking to reporters on the night of the coup, a military officer with the CNSP said, “Mali descends into chaos day by day [with] anarchy and insecurity because of the fault of the people in charge of its destiny. Real democracy doesn’t go with complacency, nor weakness of the state authority, which must guarantee freedom and security of the people.”383 Likewise, leader of the CNSP Assimi Goita based the 2020 coup on the country’s disorder saying “Mali is in a situation of socio-political crisis. There is no more room for mistakes.”384 In addition, and

similar to the 2012 coup, the CNSP also acknowledged they would look to return power to civilian rule as quickly as possible. Indeed, within hours of seizing power, the military said it would transition government back to civilian control in a “reasonable time.”\(^\text{385}\) Within a week, and primarily in response to economic sanctions and border closures implemented by neighbouring and regional countries, the military picked former Defence Minister Bah Ndaw to head a transitional government for 18 months until the country could organize an election.\(^\text{386}\) For many international observers, including leaders of the M5-RFP, the selection of a former military officer to head the provisional government was concerning, with some expressing skepticism about the prospect of a democratic future. Within eight months, these concerns became a reality.

In May 2021, Mali experienced its third coup in less than a decade, and its second in less than a year. Upset that interim President Ndaw selected a new Cabinet, and formed a new government without consulting Goita (then acting as Vice President), the country’s soldiers arrested Ndaw and his Prime Minister, Moctar Ouane on May 24.\(^\text{387}\) Two days later, Ndaw and Ouane resigned. Described by some, including French President Emmanuel Macron as a “coup within a coup,” Goita once again claimed his seat as leader of Mali – a position he continues to hold some eight months later. While Goita originally promised to hold elections in February


2022, his military regime has now proposed pushing that date back to December 2025 – a move his regime claims is necessary in order to focus on the country’s Islamic insurgency crisis.\(^{388}\)

I interviewed Dr. Dennis Tull, an expert on the Sahel and Central Africa working at the German Institute for International and Security Affairs about Goita and his legitimacy claims. While Dr. Tull confirmed to me that each military regime since 2012 has relied on pursuing “a robust and effective armed response to the mixed Islamo-separatist insurgency in the north,” as their rationale for seizing power, he notes the actual performance of the regime in this space has been questionable.\(^{389}\) More specifically, Dr. Tull told me that despite Goita and his regime claiming “spectacular successes” against the jihadists, their record of actually achieving things is not backed by “much evidence.” Interestingly, Dr. Tull raised a point I had not come across through my research on Mali. According to Dr. Tull, “…the current junta has brought an altogether different tool to build domestic legitimacy: attacking its foreign partners and especially the former colonial power France, with all kinds of declarations and provocations.” Apparently, this sort of nationalistic push has worked “spectacularly well” – giving the regime an opportunity to maintain some type of legitimacy, despite not delivering on their claims to restore order throughout the country. The concern now is whether Goita and his military elites will look to maintain power over the long-term, or if they will cave to regional and international pressure to form a transitional government as they did in 2020. To note, Geddes has suggested that “it is common for military interventions to lead to short periods of military rule followed by the consolidation of power by a single officer and the political marginalization of much of the


\(^{389}\) Dr. Denis Tull was interviewed for this dissertation via email on February 2, 2022.
rest of the officer corps.” Indeed, a transition from a military autocracy to a personalist dictatorship is exactly what could be happening in Mali, though at this point it is too soon to say so definitively.

What does the situation in Mali tell us?

Used as a typical case study, the situation in Mali over the last decade confirms two key theories from the literature on military regimes and how they seek to legitimize their rule, and by extension, my own needs-based theory, hypothesis on military regimes and cyber attacks, as well as my null hypothesis. To remind, my fourth hypothesis states “because military regimes are less interested in maintaining power over the long-term, and because they base their legitimacy on addressing specific internal issues which can be achieved using traditional methods such as applying military force or threatening the population, they are less likely to carry out cyber attacks.” Further, my null hypothesis states “if a regime does not face any significant threats in terms of its survival, or in terms of threats to the legitimacy of the regime, it will not engage in any significant cyber attacks.” I argue that at least two existing, and widely supported theories from the literature explain why military regimes – including Mali – do not typically carry out cyber attacks.

First, as discussed earlier in this chapter, it is often suggested that military regimes are less interested in maintaining power over the long term, and more interested in things such as the resiliency and integrity of the military in and of itself as an institution. In all three cases with Mali – the coup in 2012, the coup in 2020, and the coup in 2021 – the juntas have either transitioned control of government into the hands of civilians, or they have signalled their intent

\[390\] Geddes, 1999.
to within a set timeframe. This finding is in line with data collected by Geddes, which suggests that on average, military autocracies last shorter periods than other types of regimes, with personalist regimes lasting nearly twice as long and single-party regimes lasting nearly three times as long. This is not only attributed to their lack of interest in holding on to power, but to other things as well, including splits within the ruling military elites.

Second, military regimes typically base their takeover and control on some type of performance-based rationale, which also serves as the main basis of their legitimacy. Internal disorder of some type, civilian government corruption, and poor economic performance are three examples of common things military regimes will use to legitimize themselves. Indeed, in the case of Mali, the country’s continued insurgency issue and the need to restore order has been a pillar of the military regime’s legitimation strategy throughout every coup. I argue that much of this can be achieved without the use of cyberspace. Rather, Mali’s military regimes, and other military regimes we have seen throughout history in places like Latin America, Africa, the Middle East, and elsewhere, have effectively relied on other, more traditional forms of oppression and control, such as the use of force, threats of imprisonment, or worse.

I interviewed Dr. William Akoto from Fordham University in New York about military regimes, how they control people, and why they do not use cyberspace in the same way other regimes do. Dr. Akoto studies both cyber conflict, and military regimes, making him an ideal interviewee for my dissertation. Dr. Akoto told me “in the case of military regimes, they have other more effective tools that can achieve the same purpose of intimidating the opposition and censuring the media (e.g. they can deploy state security agencies like the police, army, or intelligence operatives etc.). These conventional repression tools are much more effective than
cyber can be on its best day, so they use those instead.” Moreover, Dr. Akoto discussed another dynamic that is important to note in terms of military regimes and their aversion to using cyberspace: lack of resources and expertise.

Dr. Akoto told me “the costs [of carrying out cyber operations] include the time, computer, and human resources needed to successfully conduct such operations. The problem is that many countries do not possess the computer and human resource skill base needed to stage successful cyber operations. They can hire proxies outside the country to do it but that comes with its own set of challenges. For many regimes, the capabilities are a major obstacle.”

Likewise, when I interviewed Dr. James Lewis he told me “the use [of cyberspace] is determined by capabilities…so in that context, you need to balance your actual abilities in cyberspace with how they can help you achieve your national objectives.” Similarly, when I interviewed Dr. Bilyana Lilly about the Kremlin’s behaviour in cyberspace, she suggested much of what we see in terms of Russia’s cyber attacks are determined by their resources. Dr. Lilly told me “Russia has the math background, they have the physics background, they have the schools to pull people from…they have the means and the resources in the country to achieve their objectives in cyberspace.” From this perspective, it could be argued that military regimes have more efficient and effective tools at their disposal, but they also face challenges in acquiring and applying more technologically advanced tools such as cyber capabilities. That being said, I disagree with this assertion for a variety of reasons.

In the case of Mali, and indeed throughout much of Africa, there has been a surge in cyber capabilities over the last several years – even “cyber mercenaries” have become a

---

391 Dr. William Akoto was interviewed for this dissertation via email on January 28, 2022.
noteworthy issue in multiple African nations. These developments challenge the suggestion that Mali and other military regimes cannot undertake cyberattacks – even if they want to. In Mali for instance, the country has ramped up its Information and Communication Technologies (ICT) capabilities, infrastructure, and strategic planning, having implemented a national policy and strategic plan for ICT, administered through the Information and Communications Technology Agency. Further, the country established a Cybercrime Section within the Judicial Intervention Unit of Bamako, and the General Department of Scientific Police has a cyber-specific unit, as well. In 2011, the government also created the Digital Complex of Bamako to serve as a research and innovation center for new technologies throughout the country, and in 2019 Mali implemented a new suppression of cybercrime law – all measures that signal the country has at least a rudimentary understanding of, and abilities in, cyberspace.392

Indeed, online disinformation videos described as “technologically advanced” have been circulating widely in Mali – some of which include “deepfakes” and computer-generated voices designed to influence public perception of domestic politics. It has been suggested these videos are being produced by the government, or by pro-government actors. 393 Moreover, it was reported that during violent protests in 2020, the military response was “accompanied by an internet disruption” that prevented Malians from accessing social media and certain websites.394 Mali – like all other nations – also has the ability to contract hackers for hire to carry out operations on their behalf. Several recent reports have suggested this is a growing trend

throughout Africa. For example, in 2020, Kaspersky warned about hackers for hire in Kenya, while Amnesty International released a report in 2021 detailing a hackers for hire campaign in Togo. In another case, the University of Toronto’s Citizen Lab found that in 2020 Nigeria had hired an online surveillance company to “spy on the communications of opposition figures, journalists, and protesters.” Speaking to this point, Dr. Nathaniel Allen at the Africa Center for Strategic Studies at the National Defense University raised another perspective that challenges the suggestion military regimes might lack the ability to carry out cyber operations. Dr. Allen told me it could be the case that “regimes which face more significant internal political instability, coups, or unrest, are less likely to sponsor cyber operations against other states.”

Because of this, Dr. Allen explained, military regimes in Africa might be “more likely to invest in surveillance and disinformation capabilities” as opposed to other cyber capabilities that are more external in nature. This supports the theory that military regimes are typically more focused on internal threats and security, whereas other regime types studied in this dissertation appear more concerned with external threats, vulnerabilities, and adversaries.

These and other examples point to the fact that countries which are less technologically advanced – at least relative to nations like China, Russia, and North Korea – have the ability and the resources to hire hackers or buy the technology needed to carry out online operations. As for Mali, the country possesses both the basic cyber proficiencies needed to carry out rudimentary cyber operations, as well as the resources to hire cyber mercenaries. All told, while expertise and


397
resources should be taken into account when considering why countries may or may not use cyberspace to achieve strategic objectives, I argue the decision comes down to choice – not ability. It is not that the military regimes in Mali cannot carry out cyber attacks beyond its border, it is because they have no need to.

To conclude, military regimes do not use cyberattacks because unlike other regime types studied in this work, they are not as interested in ensuring long-term regime survival. Furthermore, they typically base their legitimation on some type of performance-based metric, such as restoring order within the country – something that is achievable through other means, such as the use of force and intimidation. Other issues, such as limited financial resources and human talent in the digital domain may be other factors that contribute to their lacking use of cyberspace. By highlighting key theories from the literature, and briefly addressing some of the main elements of Mali’s history with military regimes over the last decade, I have shed new light on why military regimes do not usually use cyberspace to achieve their goals. Doing this supports my own needs-based theory in terms of how certain regimes behave in cyberspace, while also reinforcing my null hypothesis. However, as I note in the core chapters of this dissertation, this chapter on military regimes and Mali is only a first step in addressing an important issue which is almost missing entirely from cyber-related literature: why do certain countries and certain authoritarian regimes not carry out cyberattacks? Exploring this issue more broadly will be important if we are to better understand variation in the use of cyber tools. That said, having addressed the core hypothesis that underpin this dissertation, I will now provide some concluding thoughts on where additional research is warranted in terms of theory and policy, while also covering the main findings from this dissertation.
CHAPTER SEVEN

CONCLUDING THOUGHTS AND FUTURE AVENUES OF RESEARCH

7.1 CONCLUSION

While the majority of scholarly work on cyber conflict explores how states and various hostile actors behave in cyberspace, few have sought to analyze variation in the use of cyberspace as an instrument of power. My dissertation is one of the first to address this gap and shed light on why certain countries – specifically ones under authoritarian rule – behave so differently in the digital realm. Overall, I have identified new and novel affinities suggesting that authoritarian behaviour in cyberspace may depend on the type of regime carrying out the attack. By honing in on four different regime types and four different authoritarian countries, two of which (China and Russia) displayed within-case variation, I have illuminated new theoretical connections which contribute to the field, and which set the stage for additional research and analysis on the determinants of state and potentially non-state behavioural variance in cyberspace.

In addition, to the best of my knowledge, my dissertation is the first attempt to connect key political science theories on authoritarian regime legitimation to real-world cyber patterns and events. Throughout each chapter on China, Russia, and North Korea, as well as a more concise chapter on military regimes and Mali, I have found that when extended to authoritarian behaviour in cyberspace, many of the core theories from the literature remain valid. Through this exercise, I have developed an initial needs-based theory on authoritarian cyber strategy, where I suggest that different types of authoritarian regimes will use cyberspace to obtain or achieve whatever it is that particular type of regime needs most to legitimize their ‘right to rule’ and
stave of collapse. Relatedly, my theory also shows that military regimes – a type of regime that does not typically seek to maintain power over the long-term and which legitimates its rule by addressing clearly identifiable internal threats – do not carry out cyber attacks, because as I have suggested, they do not need cyberspace to achieve their goals.

Current, mainstream explanations of state behaviour in cyberspace typically revolve around ideas such as China’s goal of re-emerging as a global superpower, Russia’s aim at eroding the U.S.-led international order, and North Korea’s objective of funding the country’s nuclear weapons program. Although these explanations help us better understand high-level state objectives in cyberspace, they offer little insight as to why countries operate so differently online. My theory helps address this puzzle, while also contributing to other important theoretical considerations throughout the literature, including those related to regionalism, rivalry, and restraint. While I recognize that the case studies I have undertaken in this dissertation need to be read with the understanding they are not definitive analyses on cyber behaviour, and that different types of autocratic regimes can pursue a mixture of legitimation strategies, they provide insightful, theoretically innovative, and policy-relevant connections between different regime types, and different cyber strategies. Indeed, all of the hypotheses in this dissertation proved correct, while other interesting and unintended findings were observed.

Key Takeaways

Before providing some thoughts on areas of future research, a concise recap of the key findings from this dissertation is detailed below. My rationale for re-iterating these findings is twofold. First, doing so will remind the reader of the most noteworthy takeaways from this dissertation. Second, highlighting what we now know through this dissertation will position me
to discuss what we still do not know about cyber conflict and authoritarian behaviour in cyberspace, and where future research and analysis is needed.

**Hypothesis 1**: If an authoritarian regime is personalist, then the cyber attacks that country carries out are more likely to be characterized by obtaining access to financial resources.

While all the hypotheses in this set were proven correct, none was proven more clearly than this one. In the case of North Korea, a personalist regime, financially motivated attacks are clearly the Kim regime’s priority in cyberspace – much more so than any other regime analyzed in this research, and likely more so than any other country in the world. Throughout the literature, we are told that personalist regimes are particularly sensitive to poor economic performance, and that they often seek to legitimate their authority through financial cooptation, ensuring the country’s “selectorate” are convinced, or at least coerced, into supporting and maintaining the legitimacy of the ruler. In North Korea, this appears to be the case.

This does not mean that Kim Jong-un does not pursue other legitimation strategies, or that he does not apply other and much harsher tools to control the population and preserve his power, but rather, relative to other regimes analyzed in this research, he relies more heavily on financial resources – particularly unearned income – to maintain power. As Geddes notes, “personalist regimes are relatively immune to internal splits except when calamitous economic conditions disrupt the material underpinnings of regime loyalty.”

**Hypothesis 2**: If an authoritarian regime is a single-party, then the cyber attacks that country carries out are more likely to be characterized by cyber activities that target entities which challenge that narrative, or which are critical to the continuation of the regime’s messaging.

---

My case study on China supports the prominent argument that single-party regimes rely particularly heavily on ideological claims and narratives to legitimize their rule – claims and narratives that are often characterized by developmentalist and welfarist goals. When it comes to China, I have shown that the CCP has used cyberspace as a tool to deliver on these goals, while simultaneously eroding the abilities of individuals and organizations to criticize the regime or present alternative perspectives to party messaging. As King, Pan, and Roberts (2013) note, while online measures designed to safeguard the legitimacy of autocracies is widespread “the global trendsetter is China, which has developed a highly elaborate online infrastructure that censors only certain types of messages.”

With communist ideology serving as the foundation of all CCP rhetoric and decision-making, I argue that the regime’s core source of legitimation lies in the future, and the prospect of a return to greatness. Using cyberspace, the regime disseminates messages related to this vision while silencing all those who oppose it. Further, I argue that the regime is in the process of actively stealing its way back to global superpower status. In this sense, the regime’s prioritization of cyber espionage is not exclusively about economic performance, it is about ensuring the regime proves to the people of China, and regime loyalists, that the process is working, and that the party’s long-term strategies are coming to fruition.

Throughout this study on China, I also found that as the regime has become increasingly personalist under Xi Jinping, the country’s cyberattacks have become more focused on safeguarding his image as the saviour of the nation. This finding is consistent with theories from the literature that suggest personalist autocracies often basis their legitimacy claims on the notion

---

that they have been chosen ‘from above’ to fulfil a certain mission. In the case of China, Xi Jinping has taken on a God-like status, and cyberspace has become an invaluable tool his regime uses to ensure that image is preserved and even increased. As Zhao (2019) notes, “personality cults are hallmarks of autocracy, and the presence of a new “cult of Xi” in China could signal a return to personalistic rule.”

**Hypothesis 3**: If an authoritarian regime is an electoral autocracy, then the cyber attacks that country carries out should be characterized by output-based claims to legitimacy, such as targeting external threats or enemies, whether they be real or imagined.

Like China, Russia is another complex case, characterized by a range of legitimation strategies, and variation in the use of cyberspace as a means to exert power, influence the information domain, and legitimize the government’s rule. When it comes to the Kremlin’s use of cyber attacks, I argued that because the regime is an electoral autocracy, we should expect their behaviour in cyberspace to be focused on defending the country from external threats and enemies – something that not only ties into the legitimacy claims of electoral autocracies, but something that is intertwined with Russia’s longstanding siege mentality. By exploring the Russian government’s history of cyber attacks, it is clear the regime has used their cyber capabilities to counter what they perceive to be expansionist actors (e.g., the U.S. and NATO), to erode other forms of government as a means of highlighting the superiority of their own, and to maintain conflict with their rivals below the threshold of armed conflict.

---

On this latter point, I argue that for the Kremlin, the ability to provoke their rivals in cyberspace has been a valuable tool the regime has used to preserve the adversarial relationship the Kremlin relies on to legitimize itself, while exercising plausible deniability at home. This allows the Kremlin to maintain the narrative that Russia is always on the defensive, and that President Putin is a protector of the nation. Further, I also provided an analysis illustrating that as President Putin has become more of a personalist autocratic, particularly since 2012, Russia’s cyber attacks have become increasingly focused on perpetuating pro-Putin narratives, and attacks individuals and organizations who challenge his ‘right to rule’ and authority.

**Hypothesis 4:** Because military regimes are less interested in maintaining power over the long-term, and because they base their legitimacy on addressing specific internal issues which can be achieved using traditional methods such as applying military force or threatening the population, they are less likely to carry out cyber attacks.

Focusing on two key theories related to how military regimes differ from other autocracies or types of government, I have shown that this hypothesis is true. Specifically, we know that military regimes are typically less interested in maintaining power over the long-term than other types of regimes. Rather, they are generally preoccupied or concerned with preserving the integrity of the military as an institution, ensuring the armed forces are well funded and equipped, and that the underlying cohesion and ethos of the armed forces is maintained. From this perspective, they do not need to carry out cyber attacks to achieve these things – especially given the fact that the military lacks legitimate claims to govern over long periods.

Further, and in terms of their actual legitimation strategies, restoring order, or addressing a specific domestic issue is often what they base their ‘right to rule’ on. Again, achieving these things, whether they be countering a type of armed insurgency, rooting out government
corruption, or improving economic performance, are not generally things that would benefit from external cyber attacks. This is not to say that military regimes will not use cyber attacks in the future, or that they are not currently trying to control the online flow of information within their countries right now. Rather, I argue that generally speaking, and for at least two key reasons, military regimes will continue to rely on other, more traditional forms of control and coercion.

**Future Research**

Although this research project is a meaningful first step towards exploring authoritarian variance in cyberspace, there is significant room for additional study in this space. There are several areas that warrant further exploration and analysis which would dramatically move the needle in terms of understanding cyber conflict and adversarial behaviour in cyberspace.

To start, when I interviewed Dr. Max Smeets for this project, he pointed out that there is a “general bias in the field” in terms of “explaining the behaviour of a few” while overlooking inactivity of the many. Indeed, when we look at authoritarian countries like Venezuela, Tajikistan, or Turkmenistan for instance, why is it that they are so inactive when it comes to carrying out cyberattacks or at least malicious cyber activity beyond their own borders? More theorizing, research, and analysis is needed to understand this phenomenon. Relatedly, other theories from political science, strategic studies, and international relations could be applied to the cyber domain with a view to better understand why state and non-state actors pursue certain types of cyber activities (or not) over others. For instance, there is a vast body of work on the causes of war, which could be extended or tested against real-world cyber behaviour. Some have argued that war is more likely when a state is in decline (Levy, 1987), while others (e.g. Jervis,

---

Dr. Max Smeets was interviewed virtually for this dissertation on October 11, 2021.
1976) have hypothesized that war is more likely if defensive and offensive weapons are indistinguishable from one another or if there is a security dilemma driven by misperceptions. Others, like Mansfield and Snyder (1995), argue that democratizing states are more war-prone and aggressive than countries that are not going through a governance change. Van Evera (1998) takes a different approach, arguing that shifts in the offense-defense balance have a considerable effect on the likelihood of war, while Klare (2002) argues that following the end of the Cold War, wars will be primarily fought over natural resources, as opposed to ideology. Even widely discussed theories related to greed and grievances could be applied to cyberspace. For example, Fearon and Laitin (2003) find that the feasibility of insurgency is what makes war more likely, while Collier (2007) argues that grievances do not determine the risk of conflict, but rather, the risk of conflict is determined by the feasibility of predation. Collier also notes that grievances may be enough to generate political conflicts, but that conflict will only escalate into violence if belligerents have the necessary economic resources. Literature related to potential economic considerations could also be tested against cyber behavior. Variables such as feasibility, inequality levels, and resource endowments would lead to interesting and novel analyses of cyber conflict and cyber strategies, regardless of regime type.\footnote{\textsuperscript{402} Jack S. Levy, “Declining Power and the Preventive Motivation for War.” World Politics, Vol. 40, No. 1, pp. 82-107, 1987; Robert Jervis, “Perception and Misperception in International Politics.” Princeton University Press, 1976; Edward D. Mansfield and Jack Snyder, “Democratization and the Danger of War.” International Security Vol. 20, No. 1, pp. 5-38, 1995; Stephen Van Evera, “Offense, defense, and the causes of war.” International Security Vol. 22, pp. 5-43, 1998; Michael Klare, “Resource Wars: The New Landscape of Global Conflict.” Henry Holt and Company, 2002; James D. Fearon and David D. Laitin, “Ethnicity, Insurgency, and Civil War.” The American Political Science Review, Vol. 97, No. 1, pp. 75-90, 2003; Paul Collier, “The Bottom Billion: Why the Poorest Countries Are Failing and What Can Be Done About It.” Oxford University Press, 2007.}

Further, this research, and the overwhelming majority of material on cyber conflict and cyber strategy is focused on individual state and non-state actors. A meaningful stream of future
research that would make a significant contribution to the field would be an examination of cooperation and coalitions in terms of cyber behavior. For example, an analysis of how coalitions of states collaborate, respond, and react to events in cyberspace would shed light on an important emerging topic. Throughout the last decade, the international community has stressed the need to develop and advance an international rules-based order to guide state action and behavior in cyberspace. Indeed, several United Nations member states have worked to ensure a framework is in place which supports the global rules-based order in cyberspace, and which reinforces and affirms international law and adherence to voluntary norms in terms of state behaviour in the digital realm. To this point, a statement released by the White House in July 2021 stated “… the President is putting forward a common cyber approach with our allies and laying down clear expectations and markers on how responsible nations behave in cyberspace.” Additionally, with ongoing events like Russia’s most recent invasion of Ukraine, which started in February 2022, discussions and concerns regarding collective action and cooperative partnerships in cyberspace are only increasing. As recently as February 28, 2022, the North Atlantic Treaty Organization (NATO) suggested, “a cyberattack on a NATO member state could trigger Article 5, its collective defence clause.” yet, despite these and other major developments and initiatives, when it comes to coalitions and collective action in cyberspace, there is little research exploring what the future of cyber partnerships might look like, and whether key theories of cyber behaviour from state level analysis would mimic or differ from the behaviour of coalitions,


whether they be democracies or autocracies. As Healy (2011) wrote over a decade ago, cooperation and coalitions in cyberspace as a future conflict domain “…will require grounding in the norms and regimes that have helped to tame conflicts in other domains; transparency, confidence-building measures, formal and informal treaties, and laws of armed conflict.” Still, in the time since, there has been little research or substantive policy development in these areas. An exploration of these issues as part of an analysis on collective state-level behaviour in cyberspace would go a long way.

Future scholarly research should also examine what variables, if any, produce distinctive national approaches to cyber strategy and statecraft. For example, as Valeriano, Jensen, and Maness (2018) ask – are clear differences established in country-specific case studies a function of politics, power, or culture? Further, “…do domestic influences, such as log-rolling coalitions and how states translate cyber capacity into coercive power, produce distinct strategies?” An exploration of whether national approaches to cyber operations are a function and reflection of state ascension or decline would be a significant contribution to the field – one that my research could feed into and support. The concept of strategic culture and long-standing preferences that shape or influence state behaviour is another avenue of cyber research that warrants greater attention. Indeed, I expect that each of these research clusters would provide important insight into the variables and factors that contribute to state (and perhaps non-state) behaviour in cyberspace – something both scholars and policymakers need a better understanding of.

---

Even relatively well-established streams of cyber research would benefit from a greater analysis of regime-type and behaviour. For example, many of the most influential works on cyber deterrence point to cyber attacks being opaque instances of belligerent activity that are part of a broader coercive strategy aimed at augmenting larger geo-strategic and military efforts. In this sense, a substantial portion of the cyber literature tries to frame enemy behaviour in cyberspace in terms of whether or not it can be deterred – not why it occurs the way it does or why countries prefer certain types of attacks over others. Further, to the best of my knowledge, the majority of material on cyber deterrence fails to examine whether certain types of regimes are more easily deterred in cyberspace. Substantial research has been produced which analyses the utility of relying on the logic of deterrence and coercion to counter contemporary terrorism (Wilner, 2015) however, we have not seem the same types of research applied to the cyber domain. Using my research as a starting point may prove to be useful when it comes to assessing the motivations and strategies of certain cyber actors, and whether and how their behavior in cyberspace could be altered.

In addition, the overwhelming majority of research and material on cyber conflict revolves around a small handful of autocracies, despite the fact that the world’s most powerful democratic countries (e.g. the U.S. and U.K.) carry out their own cyber attacks. For example, Dorfman, Zetter, McLaughlin and Naylor (2020) reported that in 2018, President Trump signed a “sweeping authorization” for the CIA to carry out covert cyber operations against countries like China, Russia, and North Korea. Likewise, it was reported in 2021 that the U.S. and U.K. have

---


agreed to “join forces” to carry out “combined cyber operations” against their adversaries.\textsuperscript{409} It has also been reported that France for instance, has put in motion a plan to create an army of “cyber spies,” while Germany has gone ahead and formed its Cyber and Information Domain Service charged with carrying out “…offensive cyber operations,” among other things.\textsuperscript{410} Even the Government of Canada has taken steps to enhance its abilities to conduct a range of cyber operations. As Carvin (2018) notes – “Canada is going on the attack—at least in cyberspace.”\textsuperscript{411} We also know that Canada’s Communications Security Establishment used offensive cyber operations several times in 2021 to “disrupt foreign extremists trying to recruit Canadians to their causes or cripple cybercriminals targeting Canadians.”\textsuperscript{412} Yet, we still know very little about how democratic governments behave in cyberspace – let alone how they vary in their use of cyber attacks to achieve key strategic objectives. This is another stream of study that requires more research and analysis.

Finally, while I have focused on a relatively small sample size for this dissertation, researchers could improve the generalizability of my theory by testing it on out-of-sample or emerging cases. Doing this would make a significant contribution to the field, while enhancing external validity. Further, exploring potential correlation between other variables (e.g. natural resource wealth, trade relations, and institutional constraints) and authoritarian cyber behaviour

\begin{thebibliography}{999}
\item \textsuperscript{409} Gordon Corera, “UK and US join forces to strike back in cyber-space,” BBC News, November 18, 2021: https://www.bbc.com/news/technology-59335332
\end{thebibliography}
would greatly improve our understanding of authoritarian behaviour in cyberspace, and the impact certain factors may or may not have when it comes to their digital strategies.

Bridging the Gap

For several years, there has been a concerted effort to bridge the gap between scholars studying cyber conflict, and policymakers working in cyber and national security. Unfortunately, for a variety of reasons, little progress has been made in addressing this disconnect. I argue that much of this is attributable to the fact that policymakers and practitioners working in cyberspace are continually in a responsive whack-a-mole posture, where their main priority is preventing and responding to threats and hostile activities – not understanding why those attacks or activities take place. Further, policymakers have been grappling with the speed in which this domain has matured and become a priority area for government decision makers. For example, in the 2006 U.S. National Security Strategy, the word “cyber” was mentioned once.\(^{413}\) By 2021, the U.S. Interim National Security Strategic Guidance document identified cyber as a domain that poses “existential danger” while identifying cybersecurity as a “top priority.”\(^{414}\) This rapid rise of cyber has left policymakers with little time to develop comprehensive, interdisciplinary understandings of cyberspace and cyber conflict. As a scholar-practitioner working in Canada’s national and cybersecurity space, I have repeatedly tried to address this issue through several projects and initiatives. This dissertation is no exception.

This chapter and my dissertation as a whole, does not provide concrete steps to counter hostile or adversarial behaviour in cyberspace, such as pursuing more aggressive offensive cyber
operations, or taking steps that potentially increase the likelihood of regime change or democratization in countries like China. Offering suggestions or providing policy solutions that require significant and rigorous analysis or strategic foresight is beyond the scope of this dissertation. Rather, what I have set out to do is contribute to the understanding and appreciation policymakers have for certain considerations and variables that may contribute to or determine how our enemies behave and attack in cyberspace. Indeed, understanding the determinants of state behavior in cyberspace is a key component policymakers currently lack in terms of understanding the broader puzzle around variance in the use of cyberspace as an instrument of power and coercion.

In 2017, a report for the Hewlett Foundation’s Cyber Initiative suggested “…few cyber researchers and policy experts outside of government understand either the specific needs and priorities of government officials, or the pathways to effectively communicate new information or ideas to them. As such, government officials’ needs are not being fully met by the broader cyber policy community. In economic terms, the supply of cyber policy resources is not meeting the demand for such resources.”415 From my perspective, this remains the case in 2022. The report goes on to say, that government officials want “…more work that aims to connect basic, conceptual, and theoretical research to practical applications, through additional analysis and clearer communication.”416 Having straddled the line between scholarly cyber research and work as a policymaker in the national security and intelligence space, I can confidently say that this dissertation is a useful contribution in helping address some of these strategic pitfalls.

416 Ibid.
foreign-sponsored election interference, to online disinformation and radicalization seeping into the physical world, to privacy violations, online threats and intimidation, commercial espionage, and ransomware, this dissertation sheds light on a variety of cyber-related issues policymakers are struggling to understand, let alone quell.

Yet, there are several potential steps the Government of Canada and other countries could pursue to help facilitate better academic/policy knowledge dissemination. In the following sections and in response to the continued divide between scholarly cyber research and policymaking, I moot a number of potential initiatives the government could pursue to address this issue.

- In light of the role cyber now has in conflict and political warfare, the government could develop a distinct cyber portfolio, with a standalone Minister responsible for cyber strategy, research, and policy development. At present, cyber responsibilities remain spread across several departments and agencies, where many of the country’s most crucial cyber files are addressed in silos. With a new department responsible specifically for cyber strategy, the Government of Canada could bring cyber into clearer focus, while simultaneously creating an environment where policy discussions could be discussed more openly and hopefully – more realistically. As Valeriano, Jensen, and Maness (2018) have stated: “we need to move the discourse toward the reality of what cyber tools are good for, how they work, and how they achieve effects. We need to talk about coercion, not war. Policy makers would be wise to stop offering cyber bombs and start focusing on the more mundane task of building network defenses and resiliency.” A new cyber portfolio in Canada would be a meaningful

---

first step towards refining the focus of policymakers, tempering the conjecture that persists, and creating an environment more conducive to collaboration with scholars.

- Similarly, Canada, along with key international allies and partners should develop a Centre of Excellence and Expertise for cyber. Staffed by military personnel, civilian government employees, and academics, a centre of this nature would not only serve as a pathway for increased international cooperation and collaboration on addressing cyber threats, and developing cyber policies, it would also strengthen Canada’s internal awareness and expertise by tapping into world-class policy and research bases around the world – something Canada’s cyber policy community sorely lacks.

- Given the plethora of cyber threats and vulnerabilities Canada’s policy community is struggling to address, the creation of a Blue Ribbon Cyber Strategy Advisory Panel could be another useful initiative. Ideally, the panel – comprised of international scholars and practitioners – would explore ways the government could strengthen its approach to understanding and addressing cyber threats. Ultimately, the Panel would facilitate enhanced collaboration between Canada’s policy community, domestic and international scholars, and the private sector.

- Adversaries such as China and Russia are investing heavily in new bleeding edge, breakthrough cyber technologies, in fields such as artificial intelligence, with advancements in subfields like machine, and deep learning. These technologies are being militarized by belligerent nations at a dauntingly unprecedented pace, to the detriment of Canada and our allies. Should Canada and other allied nations not keep pace, countries such as China and Russia may have the technological upper hand in future conflicts, particularly in areas such as cyberspace. Therefore, the government would be wise to develop new and innovative
ways to leverage Canadian and allied expertise in these critically important leap-ahead fields, acquire new technologies, and introduce them into Canada’s military and security toolkits.

- Finally, and perhaps most importantly, Canada should look to create new opportunities for academics to work with, and conduct research in support of, cyber policy development. Just as Charron and Fergusson (2019) have suggested that the North American Aerospace Defense Command (NORAD) needs a “summer school” to “understand and critique the full scope of NORAD challenges,” something similar in the cyber domain would also be valuable. Whether it be a standalone conference or symposium on cyberspace, more fellowships, internships, grants and scholarships, or something akin to the aforementioned summer program, there are world class experts in Canada and abroad, whose insights, knowledge and research abilities could be leveraged in support of Canada bridging the gap.

To conclude, from a broader geo-political perspective, this dissertation may prove to be useful in terms of understanding ongoing and future cyber competition among governance regimes. As countries like the U.S. and China seek to assert themselves as the arbiters of rules and norms on the internet, policymakers must become more attune with the underlying reasons certain authoritarian regimes are looking to write the rules of the road online. If global democracies want a fighting chance against the rise of the digital dictators analyzed in this research – an understanding of their ideologies, their emotions, their aspirations, and their vulnerabilities is required. Going forward, my hope is that future policymakers and scholars can explore related puzzles and questions that flow from my work, develop new and innovative

---

418 Andrea Charron and James Fergusson, “NORAD: Beyond Modernization,” Centre for Defence and Security Studies, University of Manitoba, January 31, 2019
research programs, and identify novel insights that explain why autocracies behave the way they do in cyberspace.
REFERENCES


Chan, Tara-Francis. “A $100 counterfeit 'supernote' found in South Korea could have been made in North Korea.” Business Insider, December 13, 2017: https://www.businessinsider.com/counterfeit-supernote-found-in-south-korea-2017-12.


Chekinov, Sergey and Sergey Bogdanov, “Prognozirovanie kharaktera i soderzhaniia voin budushchego: problemy i suzhdenia [Predicting the character and content of a future warrior: challenges and judgments].” Voennaya Mysl’, no. 10 (October), 2015, pp. 41-49.


Giles, Keir. “Russia’s ‘New’ Tools for Confronting the West Continuity and Innovation in Moscow’s Exercise of Power.” Chatham House, Russia and Eurasia Programme, March 2016,


Lockie, Alex. “Russia has a grand plan to undermine the West's democracies — and it's working.” *Business Insider*, October 30, 2016: https://www.businessinsider.com/russia-undermine-west-democracies-2016-10.


Malka, Ariel, Yphtach Lelkes, Bert N. Bakker and Eliyahu Spivack. “Who Is Open to Authoritarian Governance within Western Democracies?” Cambridge University Press, September 8, 2020, https://www.cambridge.org/core/journals/perspectives-on-

Marczak, Bill John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert, “Running in Circles


Pennington, Matthew. “NKorea said to have stolen a fortune in online bank heists.” Associated Press, October 3, 2018: https://nationalpost.com/pmn/news-pmn/nkorea-said-to-have-stolen-a-fortune-in-online-bank-heists/wcm/ff41750b-ece3-4e2a-b04c-7ca34d18c537/.


Roy Choudhury, Saheli. “South Korean cryptocurrency exchange Bithumb says it was hacked and $30 million in coins was stolen.” CNBC, June 20, 2018: https://www.cnbc.com/2018/06/19/south-korea-crypto-exchange-bithumb-says-it-was-hacked-coins-stolen.html.


